Лучшая книга для подготовки к экзамену

РЕКОМЕНДОВАНО
ПРЕДСТАВИТЕЛЬСТВОМ КОРПОРАЦИИ
Microsoft®
В МОСКВЕ

TCP/IP

Экзамен 70-059

Microsoft
Certified
Systems
Engineer

Эд Титтел, Курт Хадсон
и Джеймс Майкл Стюарт

ПИТЕР®

Certification
Insider Press

COROLUS

TCP/IP

Экзамен 70-059

Эд Титтел
Курт Хадсон
Дж. Майкл Стюарт

Санкт-Петербург
Москва • Харьков • Минск
1999

Эд Титтел, Курт Хадсон, Джеймс Майкл Стюарт

TCP/IP
Сертификационный экзамен — экстерном (экзамен 70-059)

Перевел с английского А. Выскубов

Главный редактор	*В. Усманов*
Заведующий редакцией	*А. Пасечник*
Научный редактор	*К. Иншутин*
Литературный редактор	*Л. Филиппов*
Художественный редактор	*И. Половодов*
Художник	*Н. Биржаков*
Корректор	*В. Листова*
Верстка	*Р. Гришанов*

ББК 32.988я7

УДК 681.326(075)

Титтел Э., Хадсон К., Стюарт Дж. М.

Т45 TCP/IP. Сертификационный экзамен — экстерном (экзамен 70-059) — СПб: Издательство «Питер», 1999. — 416 с.: ил.

ISBN 5-8046-0025-7

Книги серии «Сертификационный экзамен — экстерном» представляют собой удобные, сжатые, хорошо структурированные конспекты для подготовки к сдаче сертификационных экзаменов на звание Microsoft Certified Systems Engineer. Книга «TCP/IP (экзамен 70-059)» не содержит ничего лишнего, только то, что действительно необходимо: фактический материал, типовые экзаменационные вопросы с разбором ответов и тестовый экзамен для самопроверки. Кроме того, вы найдете в ней советы по стратегии и тактике сдачи экзамена.

Серия «Сертификационный экзамен — экстерном» — настоящая находка для преподавателей, которые смогут рекомендовать ее слушателям в качестве пособия для самостоятельной работы и тренировки. Книга не потеряет актуальности и после успешной сдачи экзамена: она поможет в нужный момент освежить в памяти необходимые сведения.

Книги серии «Сертификационный экзамен — экстерном» рекомендованы представительством корпорации «Майкрософт» в Москве в качестве учебного пособия для подготовки к экзаменам на звание MCSE.

ISBN 5-8046-0025-7
ISBN 1-57610-195-9 (англ.)

Издательство «Питер». 196105, Санкт-Петербург, ул. Благодатная. 67. Лицензия ЛР № 066333 от 23.02.99.

Подписано к печати 10.06.99. Формат 60×90 $^{1}/_{16}$. Усл. п. л. 27. Доп. тираж 6000. Заказ 4169

Отпечатано с диапозитивов в АООТ «Типография "Правда"».

191119, С.-Петербург, Социалистическая ул., 14.

Отзывы

Серия книг «Сертификационный экзамен — экстерном» станет хорошим дополнением к учебникам, входящим в стандартный комплект литературы для подготовки к тестам на звание Microsoft Certified Professional и Microsoft Certified System Engineer. Она удачно вписывается в учебный план Microsoft и содержит материал, знание которого необходимо для успешной сдачи экзаменов. Статус сертифицированного специалиста по продуктам и технологиям Microsoft высоко ценится во всем мире, и можно только приветствовать появление новой учебной литературы, помогающей специалистам повысить уровень своей квалификации и самостоятельно подготовиться к сдаче тестов, требующих глубоких технических знаний.

Ольга Дергунова, глава представительства корпорации «Майкрософт» в Москве

Обучение и сертификация специалистов в области информационных технологий в нашей стране пользуются все большей популярностью. В связи с этим хотелось бы особо отметить серию «Сертификационный экзамен — экстерном». Материал в этих книгах изложен доступным языком, четко структурирован и пригодится не только для подготовки к тестам, но и в качестве справочника для дальнейшей работы. Как преподаватель я рекомендую эту серию всем студентам и кандидатам на получение статуса MCSE. Удачи вам!

А. В. Горбунов, MCT, MCSE, Учебный центр Microsoft
Академия народного хозяйства при Правительстве Российской Федерации

Мы рады, что с выходом книг серии «Сертификационный экзамен — экстерном» российские специалисты смогут при помощи учебных пособий на родном языке подготовиться к экзаменам и стать Сертифицированным системным инженером Microsoft. Наша газета много внимания уделяет тематике обучения и сертификации. Среди поступающих в редакцию образцов книги серии «Сертификационный экзамен — экстерном» отличаются полнотой содержания при конспективном характере изложения. Они претендуют на то, чтобы стать лучшими учебными пособиями на русском языке. Мы рекомендуем всем своим читателям использовать при подготовке книги серии «Сертификационный экзамен — экстерном».

О. О. Андронова, главный редактор газеты «Компьютер-Информ», Санкт-Петербург

Слушатели наших курсов часто испытывают потребность в учебных пособиях, которые могли бы помочь им закрепить знания и навыки, получаемые в процессе обучения, подготовиться к сдаче экзаменов по программам сертификации Microsoft. В настоящее время подобных книг, в которых сжато изложена информация для подготовки к сертификационным экзаменам на русском языке и стоимость которых невысока, практически нет. Поэтому мы приветствуем выпуск серии «Сертификационный экзамен — экстерном», это удачное решение проблемы. Мы будем рекомендовать эти учебные пособия своим слушателям.

А. В. Речинский, директор Авторизованного учебного центра Microsoft
при Факультете переподготовки специалистов
Санкт-Петербургского государственного технического университета

Желаю всем читателям, купившим книгу из серии «Сертификационный экзамен — экстерном», успешной подготовки и сдачи экзаменов на звание MCSE. Издание книг этой серии чрезвычайно своевременно. Думаю, что популярность им обеспечена.

А. С. Иванов, руководитель Центра тестирования Sylvan Prometric
при Санкт-Петербургском электротехническом университете

Изучать курс MCSE по книгам серии «Сертификационный экзамен — экстерном» — одно удовольствие. Безусловно, такая форма обучения очень эффективна, тем более что в дальнейшем, после сдачи экзамена, любая из этих книг становится прекрасным справочным пособием профессионала. Хочу порекомендовать эту серию книг всем специалистам в области информационных технологий.

Леонид Николаев, главный редактор журнала BYTE/Россия

Еще в процессе работы над серией «Сертификационный экзамен — экстерном» я успешно сдал весь курс MCSE. Думаю, вы уже поняли, какие книги я использовал для подготовки.

Кирилл Иншутин, редактор

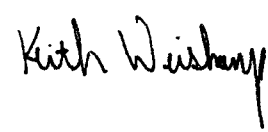
Готовы ли вы пройти сертификацию?

Я думаю, вы неоднократно задавали себе этот вопрос. Возможно, у вас уже есть неудачный опыт сдачи экзамена или вы расстроены сложностью программы и путаницей в доступных учебных материалах? Мы создали нашу тренировочную программу, чтобы помочь вам безукоризненно сдать экзамены на степень сертифицированного системного инженера Microsoft (MCSE), не потратив остаток жизни на подготовку к ним.

Каждая книга серии направлена на то, чтобы помочь вам не только подготовиться к экзамену, но и понять, в чем же заключается экзамен. В этих книгах содержатся сотни советов по сдаче тестов, которые просто невозможно найти где-нибудь еще. Для составления наших руководств мы собрали самую лучшую команду сертифицированных преподавателей, профессионалов MCSE и разработчиков сетевых курсов.

Наша задача состоит в том, чтобы предложить вам испытанные приемы тренировки и активного обучения, отсутствующие в других руководствах. Мы предлагаем уникальные советы по подготовке, приемы, узелки на память, комментарии к хитрым вопросам, тренировочный тест и многое другое. Каждое руководство по своему построению максимально приближено к тому экзамену, которому оно посвящено.

Удачи вам в сдаче сертификационных экзаменов и спасибо за то, что позволили нам помочь вам в достижении ваших целей.



Кейт Вейскамп,
издатель Certification Insider Press

Обратите внимание, что во «Введении» мы рассказали о ситуации со сдачей сертификационных экзаменов в России.

Вы можете помочь нам продолжить издание самых лучших материалов для подготовки к экзаменам. Присылайте свои отзывы и пожелания по электронной почте (comp@piter-press.ru). Нам будет интересно знать, как руководства помогли вам при подготовке или какую новую информацию вы бы хотели еще получить.

Кроме книги «TCP/IP (экзамен 70-059)», в состав серии «Сертификационный экзамен — экстерном» входят также учебные пособия «Networking Essentials (экзамен 70-058)», «NT Workstation 4 (экзамен 70-073)», «NT Server 4 (экзамен 70-067)» и «NT Server 4 in the Enterprise (экзамен 70-068)». Мы желаем вам успехов в сдаче тестов и получении звания MCSE!

Издательство «Питер»

Краткое содержание

Содержание

Об авторах

Эд Титтел

Эд Титтел (Ed Tittel) работал в качестве инструктора и разработчика курсов для American Research Group и имел дело со множеством материалов, касающихся Windows NT 4, как Workstation, так и Server. Эд также регулярно пишет статьи для журнала «Windows NT» и работает инструктором Softbank Forums на его Interop и NT Intranet торговых шоу. До начала самостоятельной работы в 1994 году Эд в течение шести лет работал в компании Novell, пройдя путь от рядового инженера до директора отдела технического маркетинга.

Эд написал более 40 книг на компьютерную тематику, включая «HTML for Dummies», «Networking Windows NT 4.0 for Dummies» и множество книг по Windows NT, NetWare, сетям и Всемирной паутине.

Эд написал более 20 статей для таких журналов, как «Byte», «Infoworld», «LAN Magazine», «LAN Times», «The NetWare Advisor», «PC Magazine» и «WindowsUser». В настоящее время Эд также является автором публикаций в сети для Interop Online. Вы можете связаться с Эдом по электронной почте (etittel@lanw.com) или через Web-страницу http://www.lanw.com/etbio.htm.

Курт Хадсон

Курт Хадсон (Kurt Hudson) — автор, инструктор и консультант в области сетевых и компьютерных технологий. Последние шесть лет он специализируется на обучении и преподавательской работе. Он написал несколько тренировочных руководств и книг на различные темы для правительственных и частных учреждений.

Как бывший инструктор Военно-воздушных сил США Курт работал над высокосекретными проектами, использующими технологии, которые многие люди видели только в кино. В течение шести лет работы в

вооруженных силах Курт получил три медали за улучшение эффективности систем, отличное преподавание и улучшение национальной безопасности. После того как Курт ушел из Военно-воздушных сил, он работал на различные частные корпорации, включая Unisys и Productivity Point International, где занимался изучением и преподаванием технических тем.

После получения статуса MCSE и MCT, Курт занялся написанием книг и разработкой тренировочных курсов для тех людей, которые хотят сдать сертификационные экзамены Microsoft. Вы можете связаться с Куртом по электронной почте (kurt@hudlogic.com) или через Web-страницу (www.hudlogic.com).

Джеймс Майкл Стюарт

Джеймс Майкл Стюарт (James Michael Stewart) — писатель, специализирующийся на Windows NT и Интернете. Он был соавтором книг «Intranet Bible» и «Hip Pocket Guide to HTML 3.2». Он также внес вклад в написание книг «Windows NT Networking for Dummies», «Building Windows NT Web Servers» и «Windows NT, Step by Step».

Майкл пишет статьи для многочисленных печатных и сетевых изданий, включая «C|Net», «Infoworld», журналы «Windows NT» и «Datamation». Он является модератором конференции Softbank, посвященной NT (http://forums.sbexpos.com/forums-interop/get/HOS_3.html). А также был лидером группы изучения NT в Central Texas LAN Association. В настоящий момент он является MCP для Windows NT Server 4, Workstation и Windows 95.

Майкл в 1992 году окончил Техасский университет в Остене. Однако его компьютерные знания были приобретены самостоятельно, на основе практически 14-летнего опыта. Вы можете связаться с Майклом по электронной почте (michael@lanw.com) или через Web-страницу (http://www.alnw.com/jmsbio.htm или http://www.impactonline.com/).

Благодарности

Эд Титтел

С самого начала я хотел бы поблагодарить команду Coriolis, которая смогла достать удивительно много кроликов из одной маленькой запачканной шляпы. Кейт Вейскамп (Keith Weiskamp) — человек с предвидением и волей, позволившей превратить голую идею в настоящий феномен. Шари Джо Хайджр (Shari Jo Hejr) — леди, которая работала над магическим контрактом, собравшим все вместе. Мы особенно признательны производственной команде под умелым управлением Сандры Ласистер (Sandra Lassister): управляющему редактору Пауле Кмерц (Paula Kmertz), редактору проекта Джеффу Келлуму (Jeff Kellum), координатору Киму Эофф (Kim Eoff). Спасибо также выдающемуся отделу продаж, включая Тома Майера (Tom Mayaer), Джоша Миллса (Josh Mills) и Энн Талл (Anne Tull). Конечно, мы также благодарны дизайнерам: Эйприл Нильсен (April Nielsen), Джимми Янгу (Jimmie Young) и Энтони Стоку (Anthony Stock).

Я очень признателен за эту книгу моим соавторам: Джеймсу Майклу Стюарту и Курту Хадсону. Без их потрясающего знания Microsoft, тестирования и богатого мира сетевых технологий эта книга никогда бы не появилась. Мы никогда бы не создали наше детище без нашего генерального менеджера Дэвида Джонсона (David (DJ) Johnson) и Мэри Бурмейстер (Mary Burmeister). Спасибо вам всем, вы были великолепной командой! Я также хочу поблагодарить гремлинов[1] из Microsoft, особенно тех, кто составил экзамены MCSE, за предоставленный нам шанс поучаствовать в таком восхитительном приключении.

Курт Хадсон

Я хотел бы поблагодарить Шеннона Джонсона (Shannon Johnson), MCSE, за его вклад в эту книгу. Шеннон — настоящий специалист по IP. Я также хочу поблагодарить за ее вклад Джулию Хадсон (Julie Hudson), CNA и MCP.

Джеймс Майкл Стюарт

Спасибо моему начальнику и соавтору, Эду Титтелу, за предоставленную мне возможность участвовать в написании этой книги. Спасибо DJ за его громадные усилия по завершению этой книги. Спасибо моим родителям, Дэйву и Лауре, за веру в меня. Спасибо Марку: я представил мир, в котором мы не были бы друзьями, и он получился унылым, грустным и печальным. К счастью, мы живем не в нем. Спасибо, Герберт, — я действительно завидую тебе и твоей пушистой шерсти. Пусть твои девять жизней никогда не кончаются. И, наконец, как всегда, спасибо, Элвис, — твоя преданность, непоколебимость и определенность вдохновили целое поколение на еду и одновременный просмотр трех телепрограмм.

[1] В современном американском фольклоре — злые гномы, портящие технику. — *Примеч. перев.*

экзамены, касающиеся компонентов BackOffice. В их числе экзамены по SQL Server, SNA Server, Exchange, Systems Management Server, и т. п. Однако экзаменом по выбору может быть и экзамен по сетевым технологиям, например «Internetworking with Microsoft TCP/IP» (опять же, рассматриваемая версия NT должна совпадать с версией в основном экзамене).

Итак, для того чтобы стать MCSE, необходимо сдать шесть экзаменов. Часто бывает, что весь процесс занимает год или больше и многим приходится сдавать экзамены по нескольку раз, чтобы все же сдать их. Цель нашей книги — предоставить в ваше распоряжение материал, достаточный для сдачи экзамена с первой попытки.

Наконец, сертификация — развивающийся процесс. Когда продукты Microsoft устаревают, MCSE обычно имеют от 12 до 18 месяцев для того, чтобы обновить свой статус, сдав экзамены по текущим версиям программных продуктов. Если этого не сделать, статус MCSE будет утерян. Поскольку технологии развиваются и новые продукты вытесняют старые, это не удивительно.

Наиболее подробную информацию о сертификационной программе Microsoft вы сможете найти на Web-узле Microsoft. На момент написания этой книги страница, посвященная программе MCP, находилась по адресу www.microsoft.com/Train_Cert/mcp/default.htm. Однако Web-узел Microsoft часто изменяется, так что вам, возможно, придется провести поиск на узле по ключевому слову «MCP» или строке «Microsoft Certified Professional Program».

Сдача сертификационного экзамена

Увы, экзамен не бесплатен. Вы заплатите за каждую попытку, вне зависимости от того, сдадите вы экзамен или нет.

Стоимость каждого теста индивидуальна и определяется ценовой политикой фирмы — «хозяина» теста. В Европе один тест стоит $100–$300, и эти цены одинаковы во всех центрах Европы, Америки, Африки и Австралии. Однако фирмы, заинтересованные в активном развитии сертификации в отдельных регионах, устанавливают в этих регионах специальные цены, способствующие повышению интереса к их сертификациям. В России один тест Microsoft российскому специалисту обходится в $23. Так что сдавать тесты Microsoft в России очень выгодно!

Организационно сдать тест сейчас достаточно просто: сеть центров тестирования достаточно широка. Сегодня в 10 городах России работают 16 центров Sylvan Prometric (из них два в Санкт-Петербурге — ЛЭТИ, ЛИМТУ) и несколько центров VUE (Virtual University Enterprises) (один из них — УТЦ АйТи в Санкт-Петербурге). Детальную

информацию о российских центрах Sylvan Prometric можно найти на Web-сервере www.prometric.ru, о VUE — www.it.spb.ru/vue.

В день экзамена придите хотя бы на 15 минут раньше назначенного вам времени. Вы должны иметь удостоверение личности с фотографией.

Вам не будет позволено взять с собой что-либо на экзамен, кроме чистого листа бумаги и авторучки. Мы советуем вам сразу же после этого записать на листе важную информацию по теме экзамена. В эту книгу включена краткая справка, которая включает выжимку из наиболее важных фактов и понятий. Мы советуем вам «сдать» пример экзамена перед вашим первым экзаменом; вряд ли вам понадобится делать это в дальнейшем.

После того как экзамен будет завершен, программное обеспечение сообщит вам, сдали ли вы экзамен. Все экзамены оцениваются из расчета 1000 баллов, и результаты разделены на диапазоны по смыслу. Даже если вы не сдали экзамен, мы предлагаем вам попросить — и сохранить в дальнейшем — отчет об экзамене, который администратор экзамена может напечатать для вас. Вы сможете использовать этот отчет при подготовке к переэкзаменовке, если она будет необходима.

Изменение вашего статуса

Что касается преимуществ, которые получает специалист, имеющий сертификацию той или иной фирмы, то прежде всего это регулярные приглашения на ежегодные конференции (с предоставлением небольшой скидки), проводимые Microsoft в самых живописных углах земного шара.

Каждый сертифицированный специалист Microsoft получает доступ к «закрытой» части Web-сервера Microsoft, где можно найти много интересных и полезных в реальной жизни вещей.

Но самое главное — во многих фирмах без такого сертификата вас просто не допустят к работе с информационными системами, и это все больше становится нормой и у нас в России.

Дополнение о программах сертификации

Область информационных технологий — одна из самых динамичных областей человеческой деятельности. Фирма Microsoft постоянно обновляет не только список сертификаций, но и содержание каждой из текущих сертификаций.

Сегодня кроме названных в данной книге сертификаций Microsoft предлагает еще три:

- **Вопросы для подготовки к экзамену.** В конце каждой главы приведен набор вопросов, позволяющих вам проверить, как вы усвоили материал. Особо сложные вопросы выделены значком

Эти вопросы либо содержат коварную ловушку, либо просто очень трудны. Вы должны читать их очень внимательно, и не один раз. Имейте в виду — такие вопросы регулярно встречаются в экзаменах Microsoft.

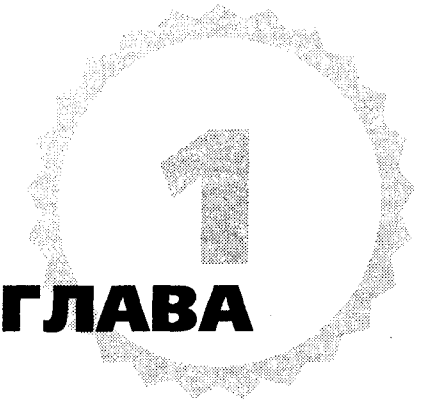
- **Дополнительная информация.** В конце каждой главы приведен список ресурсов, из которых вы можете получить дополнительную информацию. Это ресурсы Microsoft и сторонних компаний, предлагающие более подробную информацию по материалу главы. Если вы найдете какой-либо из них полезным — используйте его, но имейте в виду, что вовсе не обязательно изучать все указанное. С другой стороны, мы рекомендовали только то, что используем сами — и ни один из этих ресурсов не окажется пустой тратой времени или денег. Для обозначения

ресурсов на компакт-дисках мы используем значок 

ресурсов в Интернете мы используем значок 

Как использовать эту книгу

Если вы сдаете свой первый сертификационный экзамен, имейте в виду, что эту книгу нужно читать последовательно. Последующие главы используют материал предыдущих. Если после первого прочтения книги вы захотите повторить какие-либо темы, используйте алфавитный указатель или содержание книги, чтобы перейти сразу к интересующим вас вопросам. Эта книга может служить не только учебным пособием для подготовки к экзамену, но и справочником по реализации TCP/IP в Windows NT 4.



Сертификационные экзамены Microsoft

Термины, необходимые для понимания материала:

- Переключатель
- Флажок
- Экспонат
- Вопрос с набором ответов
- Внимательное прочтение
- Процесс исключения

Приемы и знания, которыми вы должны овладеть:

- Подготовка к сдаче сертификационного экзамена
- Тренировка (для улучшения результатов)
- Использование экзаменационного программного обеспечения наилучшим образом
- Распределение времени
- Откладывание наиболее сложных вопросов на потом
- Угадывание (в качестве последней надежды)

Как показывает опыт, люди не любят сдавать экзамены, вне зависимости от того, насколько хорошо они к ним готовы. Однако в большинстве случаев представление о том, что придется делать, позволяет меньше беспокоиться. Проще говоря, вы, вероятно, не будете так нервничать при сдаче четвертого или пятого сертификационного экзамена Microsoft, как при сдаче первого.

Сдаете вы первый экзамен или десятый, знание различных связанных с экзаменом мелочей (количества времени, отведенного на вопросы, обстановки, в которой вы окажетесь, и прочего), а также знакомство с экзаменационным программным обеспечением поможет вам сконцентрироваться непосредственно на вопросах экзамена, а не на том, что происходит вокруг. Аналогично, простейшие умения помогут вам распознать ловушки в некоторых экзаменационных вопросах Microsoft и, возможно, даже обратить их себе на пользу.

В этой главе мы расскажем вам про обстановку на экзамене и используемое программное обеспечение, а также предложим вашему вниманию несколько испытанных стратегий сдачи экзамена, которые вы сможете использовать для улучшения результатов. Мы собрали эту информацию на материале более чем 40 экзаменов, которые мы сдавали сами, а также учли советы наших друзей и коллег — некоторые из них сдавали более чем по 30 экзаменов!

Обстановка на экзамене

После того как вы прибываете в экзаменационный центр, в котором записаны на сдачу экзамена, вы должны зарегистрироваться у координатора экзамена. Вас попросят предъявить удостоверение личности, с фотографией. После того как вы зарегистрируетесь и подойдет ваше время, вас попросят оставить все книги, сумки и прочие вещи, которые вы могли принести с собой, после чего проводят в закрытую комнату. Как правило, в этой комнате находится от одного до шести компьютеров.

Вам будет выдана авторучка или карандаш и лист бумаги или, в некоторых случаях, пластиковая доска и специальный стираемый карандаш. Вы можете записать на этом листе бумаги все, что хотите, и можете писать на обеих сторонах листа. Мы советуем вам запомнить так много, как вы сможете, из информации, приведенной на вкладке к этой книге, и записать все, что вы помните, на листе бумаги сразу же после того, как вы получите бумагу и карандаш. Вы сможете обратиться к своим записям в любой момент в течение экзамена, но вы должны сдать лист, когда будете покидать комнату.

Большинство комнат, в которых проходит экзамен, имеют большое окно в стене. Это позволяет координатору экзамена наблюдать за комнатой и следить, чтобы экзаменуемые не общались друг с другом.

Он может также вмешаться, если произойдет что-либо непредвиденное. Координатор экзамена загрузит к вашему приходу сертификационный экзамен Microsoft, на который вы записались — в нашем случае это экзамен 70-059, — и вы сможете начать сразу же, как займете место перед компьютером.

Для каждого из сертификационных экзаменов Microsoft установлено определенное время, которое отводится на обдумывание ответов. Это время сообщит вам экзаменационная программа. Она также выводит на экран часы, по которым вы можете ориентироваться. Экзамен 70-059 состоит из 58 вопросов, случайно выбранных из большого набора. На его выполнение отводится 90 минут. Кроме того, если вы сдаете экзамен на иностранном языке, вам дается дополнительно 30 минут.

Все сертификационные экзамены Microsoft проводятся непосредственно на компьютере и состоят из вопросов, к которым предлагается набор ответов, из которых следует выбрать один или несколько правильных. Хотя это может показаться слишком простым, вопросы составлены так, чтобы проверить не только знание вами основных принципов и сведений о Microsoft TCP/IP в Windows NT 4, но и способность принимать решение в непредвиденных обстоятельствах и при разных ограничениях. Достаточно часто вам потребуется выбрать не один, а несколько ответов; может потребоваться выбрать лучшее или наиболее эффективное решение из нескольких правильных, что не так уж просто и заставляет задуматься.

Эта книга покажет вам, чего можно ожидать, и объяснит, как справляться с проблемами, подвохами и прочими трудностями, с которыми вы, вероятно, встретитесь на экзамене.

Построение экзамена

Типичный экзаменационный вопрос приведен ниже (см. Вопрос 1). Предложено несколько ответов на этот вопрос, из которых вы должны выбрать единственный правильный. После вопроса приведен краткий обзор всех ответов и объяснение, почему они верны или нет.

Question 1

Which of the following correctly describes the function of ARP?

- A. Maps IP addresses to NetBIOS names.
- B. Puts frames on the wire.
- C. Converts bits into bytes.
- D. Maps IP addresses to MAC addresses.

Вопрос 1

Какое из следующих предложений правильно описывает функции ARP?

- A. Определение имен NetBIOS по IP-адресам.
- B. Помещение фреймов в сеть.
- C. Преобразование битов в байты.
- D. Определение MAC-адреса по IP-адресу.

Правильный ответ — D. ARP (Address Resolution Protocol) является протоколом межсетевого уровня, отвечающим за определение аппаратного адреса (также называемого MAC-адресом), соответствующего данному IP-адресу. ARP не определяет имена NetBIOS, не помещает фреймы в сеть и не преобразует биты в байты. Следовательно, ответы A, B и C неверны.

Приведенный пример аналогичен тем вопросам, которые можно встретить на сертификационных экзаменах Microsoft. На экзамене вам потребовалось бы навести указатель на переключатель рядом с ответом D и щелкнуть левой кнопкой мыши, чтобы выбрать правильный ответ. Единственное различие между приведенным выше примером и вопросами экзамена заключается в том, что на экзамене вы не увидите объяснения того, какой ответ правилен.

Теперь рассмотрим вопрос, в котором вам требуется выбрать несколько ответов. Этот тип вопросов использует флажки, а не переключатели, что позволяет вам выбрать несколько ответов.

Question 2

Which two programming interfaces provide Windows applications with access to the TCP/IP transport protocols? (Chose two.)

- A. NetBIOS
- B. NDIS
- C. BSD Sockets
- D. Windows Sockets

Вопрос 2

Какие два программных интерфейса обеспечивают приложениям Microsoft доступ к транспортным протоколам TCP/IP? (Выберите два ответа.)

- A. NetBIOS
- B. NDIS
- C. Сокеты BSD
- D. Сокеты Windows

Правильные ответы — A и D. NetBIOS и сокеты Windows являются программными интерфейсами, обеспечивающими приложениям доступ к протоколам TCP/IP транспортного уровня. Ответ B неверен, поскольку NDIS (Network Device Interface Specification) является программным интерфейсом, обеспечивающим взаимодействие между драйверами транспортного протокола и соответствующими драйверами сетевого интерфейса. Ответ C неверен, поскольку сокеты BSD используются для обеспечения доступа приложений к транспортным протоколам TCP/IP в UNIX-системах.

В подобных вопросах вы должны выбрать несколько ответов, чтобы ответить правильно на весь вопрос. Мы можем сказать (хотя Microsoft и не хочет это комментировать), что такой вопрос не засчитывается, если выбраны не все нужные ответы. Другими словами, ответив на вопрос частично правильно, вы не получите за него ни балла. Например, чтобы ответ на вопрос 2 был зачтен как верный, вы должны установить флажки рядом с ответами A и D.

Эти два основных типа вопросов могут появляться во множестве форм, однако именно они образуют основу, на которой построены сертификационные экзамены Microsoft. Более сложные вопросы могут включать в себя так называемые «экспонаты», которые обычно являются изображением окна одной из TCP/IP-утилит Windows NT. В некоторых из этих вопросов вам потребуется сделать выбор, установив флажок или переключатель непосредственно на изображении окна диалога; в других случаях вы просто должны использовать информацию в окне программы для того, чтобы определить правильный ответ. Знакомство с соответствующей утилитой — ключ к правильному ответу.

Другие вопросы, включающие в себя экспонаты, могут предлагать вашему вниманию схемы или сетевые диаграммы для лучшего описания ситуации, в которой вам требуется произвести устранение неисправностей или настройку. Внимательное рассмотрение таких экспонатов — путь к успеху. Приготовьтесь работать как с вопросом, так и с картинкой. Зачастую они достаточно сложны, чтобы вы могли запомнить все сразу.

Эффективное использование экзаменационного программного обеспечения Microsoft

Хорошо известный принцип сдачи экзаменов гласит, что вы должны сначала прочитать все вопросы с начала до конца, но отмечать только те ответы, в которых вы абсолютно уверены с первого раза. Далее вы можете заняться более сложными вопросами, точно зная, сколько времени остается на них.

К счастью, экзаменационное программное обеспечение Microsoft позволят вам легко придерживаться этого принципа. В нижней части каждого вопроса вы найдете флажок, позволяющий вам пометить вопрос для повторного рассмотрения. (Замечание: Пометка вопросов поможет легко найти те из них, к которым нужно вернуться, но вы *можете перейти к любому вопросу и просто используя кнопки* Вперед (Forward) и Назад (Back).) После прочтения всех вопросов, если вы отвечали только тогда, когда абсолютно уверены, и помечали остальные вопросы, вы можете продолжить последовательный просмотр вопросов, уменьшая список тех, на которые еще нужно ответить, и оставляя наиболее сложные вопросы на потом.

Совет

Имеется еще одна потенциальная выгода от прочтения всех вопросов до того, как вы начнете отвечать на наиболее сложные из них. Иногда вы можете найти в формулировках последующих вопросов какую-либо информацию, проливающую свет на предыдущие вопросы. Или же информация, заключенная в формулировках последующих вопросов, может освежить в вашей памяти факты, схемы или прочие данные о Microsoft TCP/IP, которые могут помочь вам в ответе на предыдущие вопросы. В любом случае вы продвинетесь вперед, если пропустите вопросы, в ответах на которые вы не уверены.

Продолжайте работать над вопросами до тех пор, пока вы не будете абсолютно уверены во всех ответах или пока не закончится отведенное на экзамен время. Если время подходит к концу, а вы ответили еще не на все вопросы, попробуйте быстро угадать ответы на них. Отсутствие ответа на вопрос гарантирует, что за него вам не будет *начислено баллов, в то время как ответ наугад может оказаться правильным*. Такая стратегия может быть использована только потому, что Microsoft одинаково оценивает вопросы, ответ на которые отсутствует, и вопросы, на которые дан неверный ответ.

Совет

Когда отведенное время подходит к концу, лучше расставить ответы *наугад, чем оставить вопросы без ответа*.

Относитесь к экзамену серьезно

Самый важный совет о сдаче экзамена Microsoft, который мы можем вам дать, звучит так:

Внимательно читайте текст вопроса!

Некоторые вопросы намеренно сформулированы двусмысленно, в некоторых используется двойное отрицание, в других крайне важна

терминология. Мы сдавали множество как тестовых, так и «настоящих» экзаменов, и практически в каждом тесте мы неверно отвечали по крайней мере на один вопрос из-за того, что мы не прочитали его достаточно внимательно.

Чтобы удержаться от искушения слишком быстро перескакивать с вопроса на вопрос, мы предлагаем вам придерживаться следующих правил:

- Прочитайте каждое слово в формулировке вопроса. Если вы поймаете себя на том, что перескакиваете вперед, вернитесь к началу вопроса и перечитайте его заново.
- После прочтения попытайтесь переформулировать вопрос вашими собственными словами. Если вы сможете это сделать, вам будет проще выбрать правильный ответ.
- Возвращаясь к вопросу после того, как вы прочитаете все вопросы экзамена, заново перечитайте каждое слово. В противном случае ваши мысли могут «попасть в колею». Иногда, перечитав вопрос после того, как вы отвлеклись на другой, вы обнаруживаете, что в первый раз вы что-то пропустили. Имейте виду, если вы чего-то не заметили, то и во второй раз не заметите этого, если не будете читать внимательно. Постарайтесь избежать такой ситуации.
- Если вы возвращаетесь к вопросу более двух раз, попытайтесь четко определить, чего вы не понимаете в вопросе, почему приведенные ответы кажутся бессмысленными или почему кажется, что правильный ответ отсутствует. Если вы будете сосредоточенно обдумывать вопрос некоторое время, из глубины вашей памяти могут всплыть детали, которых вам не хватало, или вы можете заметить «ловушку»», и это укажет на правильный ответ.

Кроме того, при поиске ответа на каждый вопрос попытайтесь вспомнить, что вы знаете о TCP/IP утилитах NT, их поведении и характеристиках; какие помните факты и схемы, имеющие отношение к вопросу. Обдумав то, что вы знаете (а также то, что вы записали на выданном вам листе бумаги) вы, скорее всего, сможете успешно определить правильный ответ на вопрос.

Стратегии работы с вопросами

Судя по тем экзаменам, которые мы сдавали, в структуре ответов просматривается пара интересных тенденций. В тех вопросах, которые требуют единственного ответа, обычно два или три из приведенных ответов очевидно неверны, и два ответа выглядят подходящими. Но, конечно, только один из них правилен. Если только ответ не очевиден (а если он кажется очевидным, перечитайте вопрос в поисках

ловушки — зачастую именно в таких вопросах люди делают ошибки), начните процесс поиска правильного ответа с исключения очевидно неверных ответов.

Очевидно неверные ответы можно определить по несуществующим названиям меню или утилит, несуществующим параметрам программ, а также по терминам, которых вы ранее никогда не встречали. Если вы готовились к экзамену, в экзаменационных вопросах не может встретиться ничего такого, что было бы для вас совершенно новым. Незнакомые или странные термины означают, что, скорее всего, ответ абсолютно неверен. Эти соображения помогут вам определить правильный ответ и исключить неправильные.

Во многих вопросах предполагается, что TCP/IP утилиты NT используют настройки по умолчанию. Поэтому важно знать и понимать, как ведет себя TCP/IP в Windows NT по умолчанию. Если вы знакомы с настройками по умолчанию и понимаете, что они значат, это поможет вам разрубить множество гордиевых узлов.

В тех случаях, когда предлагается выбрать несколько ответов, вы должны отметить все правильные ответы, чтобы вопрос был вам зачтен. Рассматривайте это как еще один аргумент в пользу внимательного прочтения.

При работе над вопросами экзамена очень удобен предоставляемый программным обеспечением Microsoft счетчик вопросов, показывающий, на сколько вопросов вы ответили и сколько еще осталось. Планируйте ваше время так, чтобы сделать четверть вопросов за четверть отведенного времени (13 вопросов за 22 минуты). Также проверьте скорость вашей работы, когда пройдет три четверти времени (39 вопросов за первые 66 минут).

Если вы не успели ответить на все вопросы за 85 минут, используйте оставшиеся пять минут на то, чтобы попытаться угадать ответы на остальные вопросы. Запомните, что ответ наугад потенциально лучше отсутствия ответа, поскольку вопросы без ответов никогда не засчитываются, а угадать ответ вы можете и правильно. Если у вас нет никаких идей по поводу оставшихся вопросов, выбирайте ответы наугад или выберите во всех таких вопросах ответ «a» или «b» и т. д. Важно, чтобы к концу экзамена у вас был бы хоть какой-то ответ на каждый вопрос.

Подготовка к экзамену

В конце концов, знания перерастают в уверенность, а уверенность — в успех. Если вы внимательно изучите материал книги и вопросы для подготовки к экзамену в конце каждой главы, вы поймете, в каких областях вам требуется дополнительная информация.

После этого прочитайте некоторые дополнительные материалы из числа указанных в соответствующем разделе — в конце каждой главы. Если вы будете знакомы с понятиями, используемыми в приведенных вопросах, вы сможете эффективно действовать в аналогичных ситуациях на экзамене. Если вы знаете материал, вы можете быть уверены, что вы сдадите экзамен.

После того как вы проработаете всю книгу, попробуйте сдать примерный экзамен, приведенный в главе 17. Это позволит вам почувствовать стиль настоящего экзамена и определить, в каких областях вам нужно изучить что-то дополнительно. Перед тем как сдавать настоящий экзамен, обязательно изучите материал, связанный с вопросами, на которые вы не ответили. Только после того, как вы почувствуете почву под ногами и уверенность во всем материале примерного экзамена, вы можете сдавать настоящий экзамен.

Совет

Если при сдаче репетиционного экзамена, который приведен в конце этой книги, вы набрали менее 75% правильных ответов, вам следует заниматься дальше. Как минимум скопируйте тесты для подготовки к экзамену (Personal Exam Prep, PEP) и тесты для самопроверки с Web-узла Microsoft Training And Certification (его адрес приведен в следующем разделе). Если вы более честолюбивы или хорошо обеспечены, вы можете приобрести тренировочный тест у одного из предлагающих их сторонних производителей. Нам нравятся тесты компании Transcender Corporation и компании Self Test Software (это производители тестов PEP).

Вооружившись информацией из этой книги и решимостью подтвердить свои знания, вы должны сдать сертификационный экзамен. Но если вы не работали над подготовкой к экзамену, вам придется сдавать экзамен несколько раз, пока вы его наконец не сдадите. Если вы отнеслись к подготовке серьезно, экзамен пройдет как по маслу. Удачи!

Дополнительные ресурсы

Естественно, лучший источник информации о сертификационных экзаменах Microsoft — сама Microsoft. Поскольку ее продукты и технологии — а экзамены посвящены именно им — изменяются достаточно часто, лучший источник информации об экзаменах — Интернет.

Если вы еще не посетили Web-узел Microsoft Training And Certification, сделайте это сейчас. В момент написания этой главы основная страница узла была расположена по адресу www.microsoft.com/Train_Cert/ (рис. 1.1).

Примечание

Возможно, когда вы читаете эту главу, адрес или вид указанной страницы изменился — подобное регулярно происходит на Web-узле Microsoft. Если это так, то прочитайте внимательно раздел «Борьба с изменениями в Web».

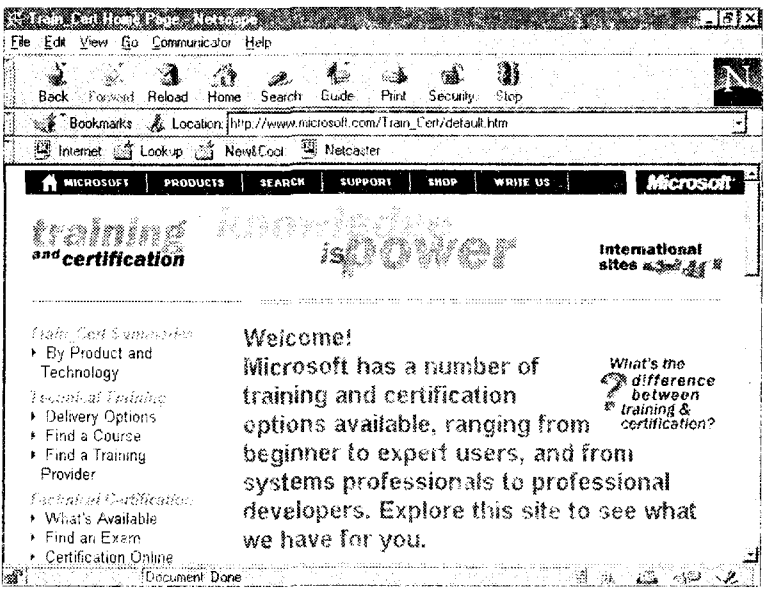


Рис. 1.1. Web-узел Training And Certification — хорошая отправная точка для дальнейшего поиска информации, относящейся к последним экзаменам и подготовке к ним

Меню в левом столбце страницы позволит вам найти наиболее важные источники информации о сертификационных экзаменах. Проверьте следующие ссылки:

- **Train_Cern Summaries/By Product and Technology.** Используйте эту ссылку для перехода к сгруппированным согласно программному продукту образовательным, тренировочным и прочим материалам. Под заголовком Microsoft Windows/Windows NT вы найдете целую страницу информации о сертификационных экзаменах, связанных с Windows NT. Вы получите множество информации о тренировке и подготовке к экзаменам, а также полный список экзаменов, относящихся к Windows NT.
- **Technical Certification/Find an Exam.** Эта ссылка перенесет вас на страницу, которая позволит получить полный список экзаменов Microsoft, а также найти все экзамены, подходящие для получения

определенного статуса (MCPS, MCSE, MCT и т. д.) или же экзамены, касающиеся определенного продукта. Эта страница очень полезна также для получения информации о конкретном экзамене, поскольку для каждого экзамена существует свое специальное руководство по подготовке. Для сдачи экзамена по TCP/IP возьмите на странице руководство для экзамена 70-059.

- **Site Tools/Downloads.** Здесь вы найдете список файлов и тестов, которые Microsoft распространяет свободно. Вы можете найти на странице информацию, заслуживающую того, чтобы вы ее скопировали, например, Certification Update, Personal Exam Prep (PEP) тесты, различные экзамены для самопроверки и общее руководство по подготовке к экзамену (Exam Study Guide). Найдите время изучить эти материалы до того, как сдавать экзамен.

Конечно, это только часть информации, доступной на Web-узле Microsoft Training And Certification. Когда вы будете просматривать этот узел — а мы настоятельно рекомендуем вам это сделать, — вы, скорее всего, найдете массу интереснейшей информации, о которой мы даже не упомянули.

Борьба с изменениями в Web

Раньше или позже вся информация о Web-узле Microsoft Training And Certification и о других ресурсах Сети, которые мы будем упоминать в этой книге, совершенно устареет. В некоторых случаях URL будут содержать страницу, указывающую, где теперь можно найти нужную вам информацию; в других случаях адреса будут указывать в пустоту и вы получите сообщение об ошибке «404 File not found».

Если это произойдет, не сдавайтесь! Всегда существует способ найти во Всемирной паутине то, что вы ищете, — если вы можете потратить некоторое время и энергию. Для начала отметим, что большинство крупных Web-узлов — в том числе и Microsoft — предлагают вам инструменты для поиска. Вернитесь к рис. 1.1 и обратите внимание на надпись «SEARCH» в верхней части страницы. Если вы только в состоянии найти этот Web-узел (а мы уверены, что он достаточно долго будет располагаться по адресу www.microsoft.com), вы можете использовать соответствующую ссылку для поиска нужной вам информации.

Чем более точно вы сформулируете ваш запрос, тем вероятнее, что найденная информация будет именно тем, что вы ищете. Например, вы можете провести поиск строки «training and certification», получив в ответ огромное количество ссылок на страницы о подготовке и сертификации вообще, но если вы ищете руководство по подготовке к экзамену 70-059 «Internetworking with Microsoft TCP/IP on

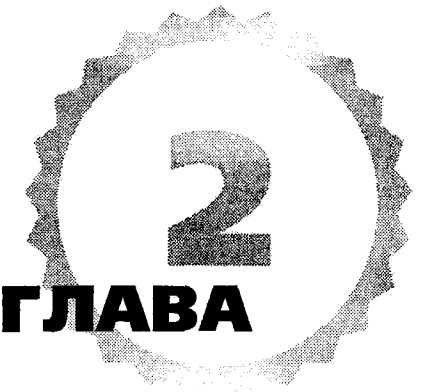
Windows NT 4.0», вам лучше использовать для поиска примерно такую строку:

```
Exam 70-059 AND preparation guide
```

Точно так же, если вы хотите найти материалы по подготовке и сертификационным экзаменам, которые можно было бы скопировать, примените примерно следующую строку для поиска:

```
training and certification AND download page
```

Наконец, не бойтесь использовать поисковые инструменты общего назначения, наподобие расположенных по адресам www.search.com, www.altavista.digital.com, www.excite.com для поиска нужной вам информации. Несмотря на то что Microsoft предоставляет лучшую в Интернете информацию о сертификационных экзаменах, существует масса источников информации от третьих фирм, не следующих «партийной линии» Microsoft. Резюме этого раздела таково: если вы не можете найти в Сети какую-либо страницу, на которую ссылается эта книга, посмотрите рядом. Если и это не поможет, вы всегда можете отправить нам письмо по электронной почте — мы постараемся помочь.



Концепции и планирование: TCP/IP и Windows NT

Термины, необходимые для понимания материала:

- ARPANet
- RFC (Запрос комментариев)
- IAB (Совет по архитектуре Интернета)
- OSI (Взаимодействие открытых систем)
- Порты
- Сокеты
- Скользящие окна TCP/IP
- Уровень приложения
- Уровень транспорта
- Межсетевой уровень
- Уровень сетевого интерфейса
- NetBIOS
- Сокеты Windows

Приемы и знания, которыми вы должны овладеть:

- Объяснение назначения уровней IP
- Сравнение уровней IP и уровней OSI
- Описание интерфейсов IP

В этой главе объясняются основные концепции реализации TCP/IP Microsoft — это обеспечит основу для дальнейшего изучения материала. Возможно, некоторые из обсуждаемых здесь концепций и не встретятся вам на экзамене, однако их знание необходимо для твердого понимания пакета протоколов TCP/IP Microsoft. Мы опишем основные компоненты пакета протоколов TCP/IP и объясним, как работает каждый из них в отдельности. Мы также обсудим, какую роль играет каждый компонент в общей архитектуре пакета протоколов TCP/IP в Windows NT.

TCP/IP: исследованный и объясненный

TCP/IP — это не один протокол и не пара протоколов, как может показаться при взгляде на название. TCP/IP на самом деле является пакетом протоколов. Иными словами, это большая группа протоколов, работающих вместе. Основной идеей разработчиков TCP/IP было создание протокола, который мог бы использоваться в различных смешанных вариантах сетевого окружения, а также иметь возможность выбирать различные маршруты для достижения пункта назначения. Это требование гибкости было решающим. TCP/IP, изначально названный NCP[1] (Network Control Protocol, сетевой управляющий протокол), появился как экспериментальный протокол, используемый для связи между сетями с коммутацией пакетов. Это результат действия эксперимента, предпринятого Министерством обороны США — ARPANet (Advanced Research Project Agency Network, сеть агентства по перспективным научным проектам). Основной задачей этого проекта было обеспечение работоспособности сети даже в случае отказа или повреждения какой-либо ее части — путем реализации возможности выбора альтернативных маршрутов для передачи данных.

Несмотря на то что истоки TCP/IP — в Министерстве обороны, создание и развитие этого пакета не может быть приписано какой-либо одной группе разработчиков. TCP/IP не является чьей-либо собственностью, это — основной протокол Интернета. Как и многие другие стандарты, связанные с Интернетом, стандарты TCP/IP свободно распространяются и публикуются как RFC (Request for Comments, запрос комментариев — см. следующий раздел) и поддерживаются IAB (Internet Architecture Board, Совет по архитектуре Интернета).

IAB позволяет любому частному лицу или компании предоставить на рассмотрение или испытать RFC. RFC может содержать различную

[1] Это не совсем правильно. Протокол NCP использовался в ARPANet с 1970 года; TCP/IP был создан на основе NCP группой разработчиков под руководством Винтона Серфа (Vinton Cerf) лишь в 1972 году. — *Примеч. перев.*

информацию; это — возможность публикации предложений или новых идей, относящихся к стандартам, которые могут так или иначе изменять или дополнять функциональность семейства протоколов TCP/IP. RFC при помощи Интернета выносятся на публичное обсуждение и затем рассматриваются IETF (Internet Engineering Task Force) — подразделением IAB. После того как пройдет достаточное для обсуждения и критики время, предложенный черновой стандарт может стать стандартом, который будет выполнять все Интернет-сообщество. Поскольку TCP/IP основан на открытых стандартах, не являющихся чьей-либо собственностью, он обсуждался и проверялся множеством людей по всему миру, и, таким образом, он непрерывно развивается и совершенствуется с момента своего возникновения.

TCP/IP основан на модели открытой системы. С точки зрения системной архитектуры TCP/IP соответствует эталонной модели OSI (Open Systems Interconnection, взаимодействие открытых систем) — основной модели системной архитектуры, предлагающей программистам основу для разработки сетевых протоколов. Используя модель OSI, программисты могут быть уверены, что разрабатываемые ими протоколы обладают базовой функциональностью, а также в том, что есть стандартизация, общая для их собственной реализации протокола и чьей-либо еще. Microsoft TCP/IP соответствует TCP/IP-стандартам, содержащимся в RFC. Однако реализация Microsoft TCP/IP включает в себя и поддержку возможностей, не входящих в другие версии TCP/IP.

Запрос комментариев (RFC)

Как мы упоминали выше, RFC используются для документирования стандартов Интернета. Имейте в виду, что RFC, описывающие существующие стандарты, являются лишь небольшой частью всего множества RFC. Другими словами, каждый стандарт Интернета документирован как минимум одним RFC, но не каждый RFC становится стандартом.

Существует множество различных типов RFC, в частности FYI (For Your Information, к вашему сведению), Drafts (черновики) и STD (Standards, стандарты). Любой человек имеет право представить на рассмотрение RFC или же прокомментировать существующий, одобрив его или, наоборот, подвергнув критике. Затем IETF публикует информацию в Интернете. Если RFC является предложением нового протокола или службы Интернета, IETF рассматривает его и вносит свои комментарии. Для того чтобы на рассмотрение и изменения RFC было достаточно времени, предлагаемый стандарт становится черновым стандартом не ранее чем через шесть месяцев после публи-

кации, а черновой стандарт, в свою очередь, становится стандартом не ранее чем через четыре месяца.

RFC обозначаются при помощи присвоенных им номеров, например RFC 1880 «Internet Official Protocol Standards». Эти номера присваиваются последовательно и никогда не используются повторно. Если стандарт пересматривается, то он получает новый номер, а предыдущая версия становится устаревшей. Всегда проверяйте, используете ли вы последний RFC по изучаемой теме. RFC 1880, например, содержит список последних RFC по стандартам Интернета. Чтобы найти определенный RFC или узнать больше о RFC в целом, вы можете посетить Internic (http://www.internic.net) или воспользоваться одним из множества имеющихся в Сети поисковых серверов, таких как Search.Com (http://www.search.com), и произвести поиск по ключевому слову «RFC».

Модель OSI и TCP/IP

Хотя для обмена данными между компьютерами используются различные протоколы, все сетевые коммуникационные протоколы должны обеспечивать выполнение определенного набора основных функций. Эти функции могут быть по-разному реализованы различными разработчиками, но они все должны иметь несколько общих основных характеристик. Справочная модель OSI была создана международной организацией по стандартизации (International Organization for Standartization, ISO) для того, чтобы обеспечить основу, на которой будут строиться все протоколы. Модель OSI использовалась на практике, но на сегодня она обычно используется в качестве теоретического прототипа для определения блоков, из которых должна состоять хорошая система, реализующая сетевой протокол. Большинство используемых в настоящее время сетевых протоколов, например TCP/IP или разработанные Novell IPX/SPX, содержат все основные функции, заданные в модели OSI, или часть их.

Такая стандартная модель архитектуры имеет несколько преимуществ при использовании ее программистами. Она определяет рамки для разработки семейства протоколов. Она позволяет всем членам компьютерного сетевого сообщества — как профессионалам, так и любителям, — совместно обсуждать общие уровни функциональности, присущие всем системам протоколов. Также, в идеальной ситуации, обеспечиваемая многоуровневой концепцией протоколов модульность позволяет заменить устаревший функциональный блок кода улучшенной его версией — без необходимости переработки всего семейства протоколов. Эта взаимозаменяемость упрощает взаимодействие меж-

ду вариантами сетевого программного обеспечения различных производителей.

До того как модель OSI была признана в качестве подходящей для разработки протоколов, большинство разработчиков создавало свои собственные протоколы, мало заботясь о возможности взаимодействия с программными продуктами других производителей. Однако поскольку все большее и большее количество покупателей принимали идею открытых стандартов, то стандарты, являющиеся чьей-либо собственностью, стали проигрывать на рынке. Возможность взаимодействия становилась все более важной, и необходимость стандартной модели, такой как OSI, стала очевидна. Например, если два производителя программного обеспечения решали разработать свои собственные версии протокола и оба из них при этом руководствовались моделью OSI, то по крайней мере оба протокола были основаны на модульном принципе, и определенные функциональные блоки этих протоколов выполняли схожие задачи. Хотя модель OSI не гарантирует возможности взаимодействия между двумя различными реализациями одного протокола, она предоставляет для разрабатываемого протокола хорошую схему.

Уровень за уровнем

Модель OSI состоит из семи уровней, и каждый уровень отвечает за выполнение определенных задач. Это не означает, что протокол, основанный на модели OSI, состоит из семи различных частей или имеет ровно семь определенных функций. Как мы упоминали выше, эти уровни просто представляют типы функций, которые протокол должен поддерживать, и они организуют функциональные блоки в определенную логическую иерархию. Обратите внимание, что блоки, находящиеся наверху этой иерархии, отвечают за функции, наиболее «близкие» к пользователю или приложению, в то время как нижние блоки выполняют функции, «близкие» к физической сети или сетевым интерфейсам.

Давайте подробнее разберем роли и задачи, выполняемые различными уровнями модели OSI, показанной на рис. 2.1.

- **Уровень 7: уровень приложения.** Это верхний уровень модели OSI. Он отвечает за обеспечение доступа приложений к сети. Пользовательские приложения и системные службы обычно общаются с сетью при помощи взаимодействия с процессами, работающими на этом уровне модели OSI.
- **Уровень 6: уровень представления данных.** Этот уровень модели OSI близко связан с прикладным уровнем. Его основная задача — следить за тем, чтобы данные, передаваемые на прикладной уровень, были в нужном формате, и конвертировать их при необходимости.

- **Уровень 5: уровень сеанса.** Уровень сеанса отвечает за установление, поддержку и прекращение связи между приложениями или процессами, работающими в разных частях сети.

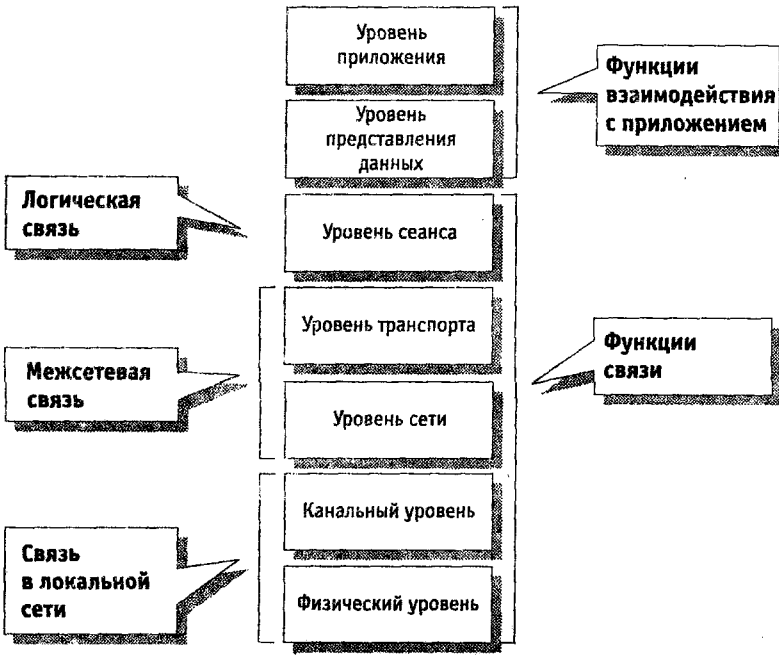


Рис. 2.1. Семь уровней модели OSI и связанные с ними функции

- **Уровень 4: уровень транспорта.** Транспортный уровень отвечает за передачу сообщений от узла-отправителя к узлу-получателю. Он отвечает за создание виртуального канала между двумя точками сети, а также за проверку целостности данных (если ее не обеспечивают нижние уровни протокола).
- **Уровень 3: уровень сети.** Этот уровень отвечает за маршрутизацию пакетов между несколькими сетями. Сетевой уровень работает вне зависимости от нижележащих протоколов и, как следствие, от устройств, таких как маршрутизаторы. Этот уровень позволяет взаимодействовать сетям, использующим различные реализации канального и физического уровней.
- **Уровень 2: канальный уровень.** Это уровень исходно был создан как единый функциональный уровень. Однако стала ясна необходимость разделения канального уровня на два подуровня — уровень управления логической связью (Logical Link Control, LLC) и уровень

управления доступом к устройствам (Media Access Control, MAC). Подуровень MAC обеспечивает доступ к сети в соответствующее время, например когда другие компьютеры не передают информацию или когда появляются права доступа к сети. На этом уровне биты и байты преобразуются в кадры или наоборот. Подуровень LLC преобразует биты и байты, полученные с подуровня MAC, в формат, требуемый сетевым уровнем.

- **Уровень 1: физический уровень.** Физический уровень связан с физическим доступом к сети — с методом, которым биты и байты отправляются и принимаются. Это уровень, на котором определяются спецификации на оборудование, соединители, длину кабеля и сигналы.

Чтобы стало понятнее, как работает модель OSI, рассмотрим следующий пример. Когда прикладной уровень получает пакет данных от приложения или службы, он обрабатывает эту информацию тем или иным образом, добавляет к ней заголовок и передает следующему уровню модели OSI — уровню представления данных. Уровень представления данных обрабатывает полученные данные, добавляет свой собственный заголовок и передает информацию вниз по иерархии. Данные в конце концов проходят все уровни вплоть до физического, причем на каждом уровне они обрабатываются и к ним добавляется заголовок. Затем данные передаются по сети на другой компьютер. Прибыв на машину-получатель, данные проходят через все уровни в обратном порядке. Каждый уровень обрабатывает их и удаляет соответствующий заголовок, перед тем как отправить данные вверх по иерархии, как показано на рис. 2.2.

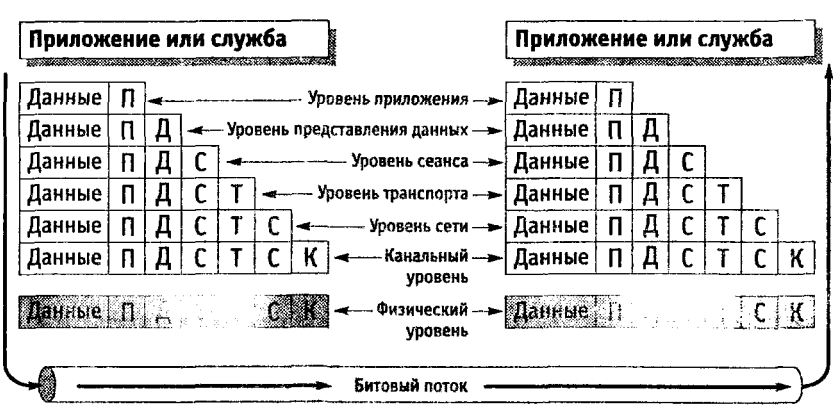


Рис. 2.2. Взаимодействие между аналогичными уровнями модели OSI при передаче данных между различными узлами сети

Каждый уровень модели OSI взаимодействует только с уровнями, находящимися непосредственно над и под ним. Также каждый уровень взаимодействует только с аналогичным уровнем на другом компьютере и не заботится о том, как протекают процессы, выполняемые другими уровнями.

Коммуникации, реализуемые в нижней части модели OSI, являются просто потоком битов. Данные в нижней части модели обрабатываются просто как набор битов или как пакет битов. Однако при перемещении данных вверх по уровням модели они структурируются. Биты группируются в байты, байты — в слова и более сложные структуры, слова и данные наконец становятся цельными идеями, предложениями или даже документами, прежде чем они будут обрабатываться приложением или пользователем.

Функциональность модели OSI

Как мы упоминали выше в этой главе, многоуровневое построение позволяет протоколы, основанные на модели OSI, организовать как модульные, причем в высокой степени. Функции таких протоколов четко разделены на отдельные группы, поэтому программист, вместо того чтобы писать один монолитный кусок кода, имеет возможность создать несколько отдельных, небольших частей (функциональных блоков), каждый из которых обеспечивает выполнение определенной группы функций. Еще раз повторим, что модульность построения протокола позволяет просто обновлять или заменять отдельные куски кода.

Например, рассмотрим случай, в котором программист разработал набор протоколов TCP/IP с использованием модели OSI. Представим, что через год этому программисту пришел в голову более эффективный способ отправки данных через сеть. Поскольку он придерживался модульной концепции при реализации набора протоколов, он может переписать и перекомпилировать только тот кусок кода, который обеспечивает выполнение функций канального и физического уровня (обычно это функции сетевого драйвера). Однако, если бы он не использовал модель OSI, обновить реализацию протокола было бы намного сложнее; возможно, ему бы даже понадобилось полностью переписать весь код.

Программное обеспечение, реализующее какой-либо протокол и построенное на основе модели OSI, содержит широкий набор различных по функциональности компонентов, от драйвера сетевой карты и программного обеспечения, передающего данные по сети и проверяющего их целостность, до программы, взаимодействующей с приложениями пользователя.

Не все программное обеспечение, созданное для реализации сетевых протоколов, включает все функции, определенные в модели OSI. Например, компания может производить только сетевые карты. Если это так, то данную компанию не волнует, как одно приложение будет взаимодействовать с другим. Структура модели OSI позволяет такой компании заниматься разработкой только аппаратного и программного обеспечения, работающего на нижних уровнях модели OSI, а программное обеспечение, работающее на верхних уровнях, может разработать кто-либо другой.

Аналогия между OSI и почтой

Модель OSI работает подобно современной почтовой службе. Представим на минуту, что вы — приложение, работающее на компьютере, и желаете поговорить с другим приложением на другом компьютере сети (в этом случае мы можем провести аналогию между сетью и транспортными линиями, используемыми почтой). Первым шагом при отправке информации будет написание письма; затем оно должно быть помещено в конверт с именем, адресом и правильным почтовым индексом; затем письмо должно быть опущено в почтовый ящик. После этого уже не ваша забота, как именно письмо дойдет до получателя, — вы исходите из того, что оно как-нибудь да дойдет.

После этого письмо забирает почтальон и помещает его в сумку, которую он приносит в местное почтовое отделение. Оттуда письма переправляются в другое почтовое отделение на автомобиле, грузовике, фургоне, поезде или самолете — в зависимости от их срочности — и по получении сортируются. В получившем письмо почтовом отделении письмо попадает в сумку другого почтальона, который и приносит его получателю. Еще раз повторим — вас не заботило то, как именно письмо дойдет до получателя. Все, что вы должны были сделать, — это использовать правильный «протокол» и поместить письмо в почтовый ящик. Как правило, этого достаточно для того, чтобы письмо дошло до адресата.

Таким образом, только те лица, которые отвечают за определенный участок пути, должны знать, как информация попадет из пункта А в пункт Б. Если часть процесса должна быть изменена, чтобы применить новую технологию или лучшую реализацию процесса, изменения должны быть произведены только на непосредственно касающемся изменения участке. (В нашем примере это может быть замена поезда на самолет.) Все другие процессы и протоколы не нуждаются в модификации и могут работать как обычно.

К счастью, Microsoft разработала свою собственную реализацию TCP/IP в соответствии со стандартами. Поскольку TCP/IP следу-

ет модульной модели, близкой OSI, реализация TCP/IP Microsoft (MS TCP/IP) также является модульной. Однако Microsoft включила в свою версию TCP/IP некоторые новые возможности и пару дополнительных интерфейсов. Добавления включают в себя расширенную поддержку NetBIOS (используемую только приложениями и службами Windows), интерфейсы TDI (Transport Driver Interface, интерфейс транспортного драйвера) и NDIS (Network Device Interface Specification, спецификация драйвера сетевого интерфейса). Эти добавления упрощают процесс создания приложений и драйверов для MS TCP/IP независимыми производителями программного и аппаратного обеспечения.

Обзор архитектуры Microsoft TCP/IP

Реализация TCP/IP фирмы Microsoft на самом деле соответствует четырехуровневой модели TCP/IP вместо семиуровневой модели наподобие OSI. Это показано на рис. 2.3.

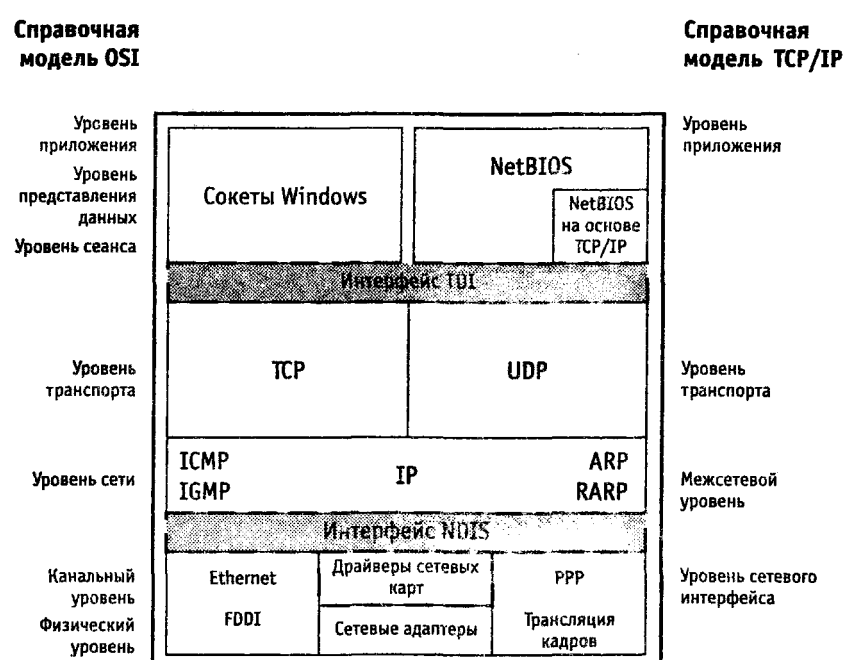


Рис. 2.3. Соответствие модели OSI и четырехуровневой модели TCP/IP реализации TCP/IP фирмой Microsoft

Эта четырехуровневая модель имеет ту же функциональность, что и ее семиуровневая сестра, модель OSI. Она просто включает больше число функций в один уровень, что приводит к уменьшению количества уровней. На рис. 2.3 вы можете видеть, что уровень приложения модели TCP/IP соответствует уровню приложения, уровню представления данных и уровню сеанса модели OSI. Уровень транспорта модели TCP/IP соответствует аналогичному уровню модели OSI. Межсетевой уровень модели TCP/IP и уровень сети модели OSI выполняют одни и те же функции. Уровень сетевого интерфейса модели TCP/IP соответствует канальному и физическому уровням модели OSI.

Уровень приложения

При помощи уровня приложения модели TCP/IP приложения и службы получают доступ к сети. Это их окно в мир. Два различных программных интерфейса (Application Programming Interface, API), обеспечивающие доступ к транспортным протоколам TCP/IP, — сокеты Windows и NetBIOS — мы обсудим в следующих разделах. Мы также обсудим интерфейс транспортного драйвера (Transport Driver Interface, TDI), который позволяет разработчикам приложений создавать компоненты сеансового уровня без необходимости знания строения компонентов транспортного уровня.

Совет

Все программные интерфейсы (API) обеспечивают стандартизированный интерфейс, который программист может использовать при создании приложений. Например, если один программист разрабатывает протокол, использующий интерфейс сокетов Windows, а другой — приложение, работающее с интерфейсом сокетов Windows, протокол и приложение могут взаимодействовать через общий интерфейс, которым в данном случае являются сокеты Windows.

Интерфейс сокетов Windows

Интерфейс сокетов Windows, или, как это часто называется, WinSock, является сетевым программным интерфейсом, предназначенным для облегчения взаимодействия между различными TCP/IP-приложениями и семействами протоколов. Как мы упоминали выше, многие разрабатывают приложения, предназначенные для работы с TCP/IP или их собственными реализациями TCP/IP. Сокеты Windows ведут свое происхождение от программного интерфейса сокетов, реализованного в операционной системе BSD Unix. Он был создан с целью предоставления общей базы приложениям и протоколам, работающим с верхним уровнем модели TCP/IP.

Интерфейс NetBIOS

Большинство служб и приложений, работающих под управлением операционной системы Windows, используют для связи между процессами (Interprocess Communications, IPC) интерфейс NetBIOS, позволяющий использование имен NetBIOS. Например, если вы хотите подключиться к разделяемому каталогу Accounts на машине SALES1 вы используете имя \\SALES1\Accounts. Эта схема именования известна как UNC (Universal Naming Convention, универсальное соглашение об именовании), и она использует имена NetBIOS, в отличие от доменных имен Интернета и DNS (Domain Name Service, служба формирования имен узлов – см. главу 9).

NetBIOS выполняет три основные роли:

- Определение имен NetBIOS.
- Служба датаграмм NetBIOS.
- Служба сеанса NetBIOS.

Имена NetBIOS определяются либо при помощи широковещательных запросов в локальной сети, либо при помощи сервера имен NetBIOS (NetBIOS Name Server, NBNS). Более крупные сети для определения имен NetBIOS используют WINS (Windows Internet Name Service, служба определения имен Интернета) – реализацию NBNS фирмой Microsoft. Это позволяет однозначно определять имена NetBIOS и уменьшить число широковещательных запросов в локальной сети. Если сервер WINS недоступен или конкретный компьютер не настроен на использование WINS для определения имен, то широковещательный запрос отправляется в сегмент локальной сети. WINS подробно обсуждается в главе 12, «Служба определения имен Интернета WINS».

Службы датаграмм NetBIOS отвечают за отправку и прием информации при помощи широковещательных датаграмм и датаграмм, не требующих установки соединения. Поскольку такая передача данных производится без установки соединения, она считается ненадежной. Нет никакой гарантии, что информация дойдет до узла-получателя. Узел-отправитель не ожидает подтверждения получения информации и не пытается отправить информацию повторно.

Службы сеанса NetBIOS отвечают за отправку и получение информации при помощи надежного двустороннего соединения, называемого *сеансом*. При создании сеанса оба устанавливающих его узла подтверждают друг другу свою готовность к коммуникациям и определяют, какой порт или сокет будет использоваться для того, чтобы убедиться в надежности соединения.

Интерфейс транспортного драйвера (TDI)

Интерфейс транспортного драйвера фактически является программным интерфейсом, работающим на границе между компонентами

уровня сеанса и уровня транспорта. Он позволяет программисту создавать компоненты сеансового уровня, не задумываясь о структуре связанных с ними компонентов транспортного уровня, и наоборот. Этот интерфейс встречается только в реализации TCP/IP фирмы Microsoft.

Уровень транспорта

Уровень транспорта модели TCP/IP отвечает за установление и поддержание соединения между двумя узлами. Его основными задачами являются подтверждение получения информации, управление потоком данных, а также упорядочение и ретрансляция пакетов.

В зависимости от типа службы, которая нужна приложению, могут быть использованы TCP (Transmission Control Protocol, протокол управления передачей) или UDP (User Datagram Protocol, пользовательский протокол датаграмм). TCP обычно используется в тех случаях, когда приложению требуется передать большой объем информации и убедиться, что данные своевременно получены адресатом. Приложения и службы, отправляющие небольшие объемы данных и не нуждающиеся в получении подтверждения, используют UDP, который является протоколом без установления соединения.

Протокол управления передачей (TCP)

TCP отвечает за надежную передачу данных от одного узла сети к другому. Он создает сеанс с установленным соединением, иначе говоря *виртуальный канал, между двумя машинами*. При установлении соединения TCP создает и отправляет запрос на соединение удаленному компьютеру и затем ожидает ответа. Если удаленная машина работает и подключена к сети, она отвечает пакетом, говорящим: «Я доступна для диалога и ожидаю дальнейшей информации». После этого машина, инициировавшая соединение, отвечает: «Отлично, вот остаток информации». Такой процесс установления коммуникационного сеанса называется трехступенчатым открытием соединения (three-way handshaking – поскольку установление соединения происходит в три шага:

1. Клиент, запрашивающий соединение, отправляет серверу пакет, указывающий номер порта, который клиент желает использовать, а также определенное число – ISN (Initial Sequence number).
2. Сервер отвечает пакетом, содержащим ISN сервера, а также ISN клиента, увеличенное на 1.
3. Клиент должен подтвердить установление соединения, вернув ISN сервера, увеличенное на 1.

Трехступенчатое открытие соединения устанавливает номер порта, который должен использоваться, а также ISN клиента и сервера.

Машины, которые устанавливают и поддерживают соединение, должны обмениваться определенной важной информацией. Каждый отправляемый TCP-пакет содержит номера TCP-портов отправителя и получателя, номер фрагмента для сообщений, разбитых на меньшие части, а также контрольную сумму, позволяющую убедиться, что при передаче не произошло ошибок. Кроме того, каждый пакет содержит подтверждающий номер, по которому отправляющая машина может определить, какие части сообщения уже достигли получателя. Пакет также содержит размер скользящего окна TCP, позволяющий управлять потоком данных между двумя компьютерами.

Порты, сокеты и скользящие окна

Каждый процесс, использующий TCP, должен иметь номер порта, указывающий расположение определенного приложения или процесса на каждой машине. Приложение может быть настроено на использование практически любого из 65535 доступных портов. Однако наиболее употребительные TCP/IP-приложения и службы используют первые 1023 из всех доступных портов. Эти применяемые по умолчанию, или «хорошо известные», порты распределены между протоколами, работающими на сервере, стандартами IANA (Internet Assigned Numbers Authority), в то время как порты, используемые на стороне клиента, выделяются приложению динамически при открытии соединения.

Например, при установлении Telnet-сеанса с удаленным узлом вы обычно соединяетесь с «хорошо известным» TCP-портом 23, а ваш Telnet-клиент получает динамически выделенный номер порта, который будет использоваться сервером при передаче сообщений на ваш компьютер.

Порт фактически является подмножеством сокета. Сокеты используются службами и приложениями, которые нуждаются в установлении соединения с удаленной системой (или с несколькими системами). Сокет состоит из IP-адреса и номера порта.

Приложение создает сокет, комбинируя IP-адрес и номер порта. Если приложению нужна гарантия того, что информация дойдет до получателя, оно использует службу с установлением соединения (TCP); в противном случае используется служба, не требующая установления соединения (UDP). Затем информация передается вниз по уровням модели TCP/IP и отправляется по сети как широковещательное или направленное (определенному узлу) сообщение. Если компьютер устанавливает соединение, соединение будет сформировано с использованием указанного сокета.

«Скользящее окно» — это термин, используемый для описания переменного размера буферов передачи и приема TCP, а также механиз-

ма управления заполненностью этих буферов. Размер скользящего окна может быть использован для регулировки количества информации, которая будет отправлена через TCP-соединение до получения подтверждения о приеме.

Внимание

Если ваша сеть используется для передачи больших объемов данных, таких как цифровой звук или изображение, вы можете увеличить производительность, увеличив размер TCP-окна. Однако, если TCP/IP работает через медленную линию связи между двумя сетями, вам, возможно, лучше уменьшить размер TCP-окна. Дальнейшую информацию вы можете найти в документе Microsoft Technet Article Q140552 или же произведите поиск словосочетания «TCP Window Size» («Размер TCP-окна»).

Пользовательский протокол датаграмм (UDP)

UDP — другой протокол уровня транспорта, предназначенный для передачи данных по сети. В отличие от TCP UDP не устанавливает соединение. Сеанс не создается, UDP просто предпринимает попытку отправки данных. UDP не проверяет, дошла ли информация до адресата.

UDP используется приложениями, которые отправляют небольшие объемы данных и не нуждаются в подтверждении адресатом их получения. Служба имен NetBIOS и служба датаграмм NetBIOS пересылают крайне небольшие объемы информации и используют этот протокол.

UDP также использует номера портов для определения конкретного процесса по указанному IP-адресу. Однако UDP-порты отличаются от TCP-портов и, следовательно, могут использовать те же номера портов, что и TCP, без конфликтов между службами.

Межсетевой уровень

Межсетевой уровень отвечает за маршрутизацию данных внутри сети и между различными сетями. Маршрутизаторы, которые зависят от используемого протокола, работают на этом уровне модели и используются для отправки пакетов из одной сети (или ее сегмента) в другую сеть (или в сегмент сети).

Протокол Интернета (IP)

IP является протоколом, не устанавливающим соединение и использующим датаграммы для отправки данных из одной сети в другую. IP не ожидает получения подтверждения (ACK, Acknowledgment)

получения отправленных пакетов от узла-адресата. Подтверждения, а также повторные отправки пакетов осуществляются протоколами и процессами, работающими на верхних уровнях модели.

Например, если приложение использует UDP на основе IP (ни один из этих протоколов не использует подтверждение получения данных), проверка того, достигли ли пакеты адресата и в правильном ли порядке они получены, должна производиться самим приложением. Это позволяет ускорить передачу данных и уменьшить нагрузку на сеть, но вызывает дополнительную нагрузку на приложение.

Каждый IP-пакет содержит адреса узла-отправителя и узла-получателя, идентификатор протокола (который позволяет IP передать пакет соответствующему транспортному протоколу), контрольную сумму и TTL (Time To Live, время жизни). TTL — это число, которое говорит каждому маршрутизатору между узлом-отправителем и узлом-получателем, через который проходит пакет, сколько времени пакет может находиться в сети. Каждый раз при прохождении через маршрутизатор TTL уменьшается на одну единицу или на время, которое пакет ждал на маршрутизаторе отправки (на большее из этих чисел).

Такая система предотвращает бесконечное странствие по сети некорректных или поврежденных пакетов. Если таким пакетам позволить свободно распространяться, это может в конце концов привести к значительному падению производительности сети.

IP использует операцию логического «И» для определения того, является ли IP-пакет локальным или удаленным. Если адрес узла-получателя локальный, то IP запрашивает при помощи ARP (Address Resolution Protocol, протокол сопоставления адреса) аппаратный адрес узла-получателя. Этот адрес затем используется для непосредственной отправки пакета адресату (вместо отправки широковещательного пакета).

Если IP-адрес был определен как удаленный, IP производит в локальной таблице маршрутизации поиск пути для пакета. Если путь не найден в локальной таблице маршрутизации, пакет отправляется на используемый по умолчанию шлюз. IP-маршрутизация подробно обсуждается в главе 6, «Реализация IP-маршрутизации».

Используемый по умолчанию шлюз проверяет адрес узла-получателя. Если адрес локален для одного из интерфейсов маршрутизатора, маршрутизатор использует ARP для отправки пакета адресату. Если адрес узла-получателя определен как удаленный, маршрутизатор уменьшает значение TTL как минимум на единицу, вычисляет новую контрольную сумму и переправляет пакет своему собственному шлюзу, используемому по умолчанию. Весь процесс повторяется заново, пока пакет не достигнет адресата или пока TTL не сравняется с нулем.

Протокол сопоставления адреса (ARP)

Протокол сопоставления адреса является протоколом межсетевого уровня, ответственным за определение аппаратного адреса (также называемого MAC-адресом), соответствующего указанному IP-адресу. На этот протокол ссылаются как на «определение IP-адресов».

Прежде чем IP-пакет сможет быть отправлен на другой узел, должен быть известен аппаратный адрес этого узла. ARP сначала производит поиск аппаратного адреса, соответствующего данному IP-адресу, в своем кэше. Если аппаратный адрес найден, то пакет отправляется адресату. Все другие машины в локальной сети «увидят» пакет, но не будут его обрабатывать, поскольку он предназначен не им.

Если соответствия не найдено в кэше, производится широковещательный ARP-запрос. Аппаратные адреса записываются в шестнадцатеричном формате; в широковещательном запросе используется аппаратный адрес FF-FF-FF-FF-FF-FF. Сообщение в широковещательном ARP-запросе выглядит примерно так: «Эй, кто-нибудь использует IP-адрес W.X.Y.Z? Если да, отправьте ваш аппаратный адрес мне на аппаратный адрес A-B-C-D-E-F». Каждая машина в локальной сети обрабатывает этот запрос и определяет, использует ли она IP-адрес, указанный узлом, отправившим широковещательный ARP-запрос. Если одна из машин локальной сети обнаруживает, что она использует данный IP-адрес, она создает и отправляет ответный пакет, включающий в себя ее аппаратный адрес. Эта информация затем используется запрашивавшим узлом для передачи пакета данных непосредственно адресату.

Если отправлявший широковещательный запрос узел получает ответ, он помещает его в ARP-кэш для дальнейшего использования и отправляет пакет данных адресату. Если ответ на широковещательный запрос не был получен, весь процесс повторяется для определения аппаратного адреса шлюза по умолчанию, и пакет пересылается ему для отправки в другую сеть. ARP подробно обсуждается в главе 7, «Определение IP-адресов».

Протокол управления сообщениями Интернета (ICMP)

Протокол ICMP используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации. Этот протокол обычно используется между двумя маршрутизаторами для контроля за тем, насколько быстро информация передается между двумя системами. Если маршрутизатор перегружен трафиком с других узлов, он может отправить специальное сообщение — ICMP-ошибку, генерируемую системой, получающей датаграммы с более высокой скоростью, чем она может их обрабатывать, — маршрутизатору, с которого приходят данные. Это сообщение просит узел-отправитель отправлять пакеты с меньшей частотой.

Протокол управления группами Интернета (IGMP)

Узлы локальной сети используют IGMP для того, чтобы зарегистрировать себя в группе. Информация о группах содержится на маршрутизаторах локальной сети. Маршрутизаторы используют эту информацию для отправки групповых сообщений всем членам указанной группы.

Групповые сообщение аналогично широковещательным, являются методом отправки данных одновременно нескольким узлам. Этот метод используется такими приложениями, как Microsoft NetShow — программой, используемой для отправки звукового и видеопотока приложению-клиенту. Эта программа может быть использована для организации встреч и совещаний по Интернету.

Уровень сетевого интерфейса

Этот уровень модели TCP/IP отвечает за распределение IP-датаграмм. Он работает с ARP для определения информации, которая должна быть помещена в заголовок каждого кадра. Затем на этом уровне создается кадр, подходящий для используемого типа сети, такого как Ethernet, Token Ring или ATM, затем IP-датаграмма помещается в область данных этого кадра, и он отправляется в сеть.

Вопросы для подготовки к экзамену

Question 1

Choose the option that best defines TCP/IP.

- ○ A. A protocol designed by Microsoft to allow information to be routed among heterogeneous network environments.
- ○ B. A protocol designed by the IAB to allow many different hardware and software vendors to access the Internet.
- ○ C. A suite of protocols that allows for communication among different types of applications running on various platforms and in various network environments.
- ○ D. A suite of protocols designed by Microsoft to allow everyday people to access resources on the Internet.

Вопрос 1

Выберите предложение, лучше других определяющее TCP/IP.

- ○ A. Протокол, разработанный Microsoft для того, чтобы позволить маршрутизацию информации между смешанными сетями.
- ○ B. Протокол, разработанный IAB для того, чтобы предоставить доступ к Интернету различным производителям программного и аппаратного обеспечения.

- C. Семейство протоколов, организовывающих обмен информацией между разными типами приложений, которые работают на различных платформах и в различных сетевых окружениях.
- D. Семейство протоколов, разработанных Microsoft и позволяющее обычным пользователям получать доступ к ресурсам Интернета.

Правильный ответ — C. TCP/IP позволяет обмениваться данными по сети приложениям и службам, работающим практически на любой платформе, включая Unix, Windows, Macintosh и другие. TCP/IP не был разработан Microsoft, хотя Microsoft и создала свою собственную реализацию TCP/IP. Таким образом, ответы A и D неверны. И хотя IAB и его подкомитет IETF участвуют в процессе стандартизации TCP/IP, не они — разработчики TCP/IP. Поэтому ответ B также неверен.

Question 2

Which of tne following statements about RFCs are correct? (Check all correct answers.)

- ❑ A. RFCs are referenced by a specific number, such as RFC 1880.
- ❑ B. RFC numbers are assigned sequentially and are never reused.
- ❑ C. RFC stands for «Requested Format of Comments».
- ❑ D. When a standard outlined in an RFC is revised, a new number is issued.

Вопрос 2

Какие из следующих утверждений о RFC верны? (Отметьте все правильные ответы.)

- ❑ A. RFC указываются при помощи своего номера, например RFC 1880.
- ❑ B. Номера RFC присваиваются последовательно и никогда не используются повторно.
- ❑ C. RFC — это сокращение от «Requested Format of Comments».
- ❑ D. Когда стандарт, описываемый RFC, пересматривается, он получает новый номер.

Правильные ответы — A, B и D. Каждый RFC имеет свой собственный уникальный номер. Эти номера присваиваются последовательно независимой организацией и никогда не используются повторно. Когда существующий RFC пересматривается, он получает новый номер, а предыдущие документы, описывающие этот стандарт, считаются устаревшими. RFC является сокращением от «Request For Comments». Поэтому ответ C неверен.

Question 3

Each of the following statements list layers of the OSI Reference Model and the respective layers of the TCP/IP Reference Model. Which of the following statements incorrectly maps corresponding layers?

- A. OSI Application, Presentation, Session, and TCP/IP Application.
- B. OSI Transport and TCP/IP Transport.
- C. OSI Network and TCP/IP Network Interface.
- D. OSI Data Link, Physical and TCP/IP Network Interface.

Вопрос 3

В каждом из ответов перечислены уровни справочной модели OSI и соответствующие им уровни справочной модели TCP/IP. В каком из ответов соответствие указано неправильно?

- A. OSI: уровень приложния, уровень представления данных, уровень сеанса; TCP/IP: уровень приложения.
- B. OSI: уровень транспорта; TCP/IP: уровень транспорта.
- C. OSI: уровень сети; TCP/IP: уровень сетевого интерфейса.
- D. OSI: канальный и физический уровни; TCP/IP: уровень сетевого интерфейса

Ответ на этот вопрос — C. Сетевой уровень модели OSI соответствует межсетевому уровню модели TCP/IP. Все другие ответы правильно указывают соответствие. Схема соответствия уровней OSI уровням TCP/IP была приведена выше на рис. 2.3.

Question 4

Which two programming interfaces provide Windows applications with access to the TCP/IP transport protocols? (Check two.)

- A. NetBIOS
- B. NDIS
- C. BSD Sockets
- D. Windows Sockets

Вопрос 4

Какие два программных интерфейса обеспечивают приложениям Windows доступ к транспортным протоколам TCP/IP? (Выберите два ответа.)

- A. NetBIOS
- B. NDIS
- C. Сокеты BSD
- D. Сокеты Windows

Правильный ответ — A и D. NetBIOS и сокеты Windows являются программными интерфейсами, обеспечивающими приложению доступ к протоколам транспортного уровня TCP/IP. Ответ B неверен, поскольку NDIS (Network Device Interface Specification, спецификация интерфейса сетевого устройства) является программным интерфейсом, предназначенным для обеспечения взаимодействия между драйверами транспортных протоколов и соответствующими драйверами сетевых интерфейсов. Ответ C является неверным, поскольку сокеты BSD Unix были разработаны для доступа к транспортным протоколам TCP/IP приложений Unix.

Question 5

You are thinking about creating an application that will require a constant end-to-end connection with another machine that is running a corresponding service. You do not want to include code in your program to ensure that data is arriving at its destination in an orderly and timely fashion. With these requirements in mind, which of the following protocols is most appropriate for use with your application?

- A. TCP
- B. UDP
- C. ARP
- D. ICMP

Вопрос 5

Вам предстоит разработать приложение, требующее постоянного соединения с другим компьютером, на котором работает соответствующая служба. Вы не хотите включать в вашу программу код, проверяющий, вовремя ли и в правильном ли порядке данные были получены удаленной машиной. Имея в виду эти требования, какой из следующих протоколов вам кажется наиболее подходящим для использования с вашим приложением?

- A. TCP
- B. UDP
- C. ARP
- D. ICMP

Правильный ответ — A. Протокол TCP обеспечивает «надежный» сеанс с установкой соединения с другим клиентом или сервером в сети на основе IP. Ответ B неверен, поскольку протокол UDP «ненадежен» и просто предпринимает попытку отправки информации, не проверяя, получена ли она адресатом. Ответы C и D также неверны. ARP используется IP для разрешения IP-адресов в аппаратные адреса и не обеспечивает «надежной» передачи данных. Протокол ICMP также используется IP. Он предназначен для отправки сообщений управления потоком данных и сообщений об ошибках клиенту и не обеспечивает «надежной» передачи данных.

Question 6

Which of the following statements best describes a socket?

- A. A number used to identify the location of a process on a remote host.
- B. A port number used to identify the location of a process on a remote host.
- C. A random number generated by a server that provides an application with access to a process on a remote host.
- D. The combination of a port number and an IP address used to provide an application or service with access to a process on a remote host.

Вопрос 6

Какое из следующих утверждений наилучшим образом описывает сокет?

- A. Число, используемое для указания расположения процесса на удаленном узле.
- B. Номер порта, используемый для указания расположения процесса на удаленном узле.
- C. Случайное число, генерируемое сервером, позволяющее приложению получить доступ к процессу на удаленном узле.
- D. Комбинация номера порта и IP-адреса, используемая для того, чтобы обеспечить приложению или службе доступ к процессу на удаленном узле.

Правильный ответ — D. Сокет создается локальным процессом или приложением для установления соединения с удаленным приложением. Этот сокет является комбинацией IP-адреса машины, на которой работает удаленное приложение, номера порта и типа используемой службы. Следовательно, D — лучший ответ. Ответ A неверен, поскольку сокет — это не просто число, используемое для идентификации удаленного процесса. Ответ B частично правилен, поскольку сокет включает в себя номер порта, но этот ответ недостаточно точен. И наконец, клиент (а не сервер!) выбирает «на лету» номер порта при установлении соединения с удаленным процессом. Следовательно, ответ C также не является правильным описанием сокета.

Question 7

The following statements describe individual parts of the threeway handshake used to establish a session. Which of these statements is incorrect?

- A. «I have information for you. Can we establish communication?»
- B. «No, I am busy right now and don't have time for you. Try back in few minutes.»
- C. «Yes, I am available for communication. Continue with your transmission.»
- D. «Great, I received your responsce. Here is the rest of the information.»

Вопрос 7

Следующие утверждения описывают отдельные стадии трехступенчатого открытия соединения. Какое из утверждений неверно?

- A. «У меня есть информация для тебя. Можем мы установить соединение?»
- B. «Нет, я сейчас занят и у меня нет времени на тебя. Попытайся еще раз через несколько минут.»
- C. «Да, я готов к открытию соединения. Продолжай передачу.»
- D. «Отлично, я получил твой ответ. Вот остаток информации.»

Ответ на этот вопрос — B. Трехступенчатое открытие соединения не допускает ответа «Нет» от удаленной системы. Если машина недоступна, она просто не отвечает. Если она доступна, но перегружена другими передачами, она использует механизм управления потоком данных, отправляя ICMP-сообщение с просьбой замедлить передачу данных. Ответы A, C и D корректно описывают возможные сообщения при открытии соединения и расположены в правильном порядке.

Question 8

Which of the following reside at the Internet layer of the TCP/IP Reference Model? (Check all correct answers.)

- ❑ A. PING
- ❑ B. ARP
- ❑ C. ICMP
- ❑ D. IGMP

Вопрос 8

Что из перечисленного ниже находится на межсетевом уровне эталонной модели TCP/IP?

- ❑ A. PING
- ❑ B. ARP
- ❑ C. ICMP
- ❑ D. IGMP

Правильные ответы — B, C и D. PING не является частью межсетевого уровня (поскольку работает в качестве приложения), хотя и использует ICMP-сообщения. Остальные перечисленные протоколы расположены на уровне Интернета эталонной модели TCP/IP. Протоколы, находящиеся на уровне Интернета, показаны выше на рис. 2.3.

Question 9

IP resides at which layer of the TCP/IP protocol stack? (Choose the best answer.)

- A. Network Interface
- B. Internet
- C. Transport
- D. Application

Вопрос 9

На каком уровне семейства протоколов TCP/IP находится IP? (Выберите лучший ответ.)

- A. Уровень сетевого интерфейса.
- B. Межсетевой уровень.
- C. Уровень транспорта.
- D. Уровень приложения.

Правильный ответ – B. Протокол IP расположен на уровне Интернета семейства протоколов TCP/IP. IP является протоколом, использующим датаграммы для пересылки данных без открытия соединения, IP не ожидает подтверждения получения данных (ACK) от узла-адресата. Подтверждение получения данных и повторная отправка пакетов осуществляются протоколами и процессами, работающими на верхних уровнях модели.

Question 10

Which of the following correctly describes the function of ARP?

- A. Maps IP addresses to NetBIOS names.
- B. Puts frames on the wire.
- C. Converts bits into bytes.
- D. Maps IP addresses to MAC addresses.

Вопрос 10

Какой из следующих ответов правильно описывает функции ARP?

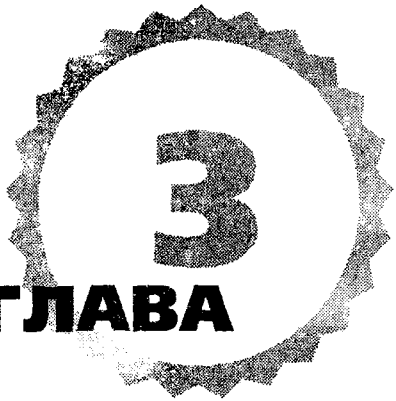
- A. Определение соответствующих IP-адресам имен NetBIOS.
- B. Отправка пакетов в сеть.
- C. Преобразование битов в байты.
- D. Определение соответствующих IP-адресам MAC-адресов.

Правильный ответ – D. ARP, протокол определения адресов, является протоколом уровня Интернета, отвечающим за определение аппаратных адресов (также называемых MAC-адресами), соответствующих данным IP-адресам.

Дополнительная информация

Произведите поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft. com), используя ключевые слова «TCP», «NetBIOS», «Reference Model», «Windows Sockets» и родственные им.

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы можете произвести поиск на компакт-диске, используя ключевые слова «TCP», «NetBIOS», «Reference Model», «Windows Sockets». Полезные материалы о TCP/IP могут быть найдены в томе «Networking Guide» *Resource Kit.*



Установка и настройка

Термины, необходимые для понимания материала:

- DNS (Служба формирования имен узлов)
- WINS (Служба определения имен Интернета)
- DHCP (Протокол динамической конфигурации узла)
- IPCONFIG
- PPTP (Туннельный протокол типа «точка-точка»)
- Шлюз по умолчанию
- IP-адрес
- DHCP-ретрансляция

Приемы и знания, которыми вы должны овладеть:

- Установка поддержки TCP/IP в Windows NT
- Понимание основ настройки IP

В этой главе мы изучим процесс установки и настройки семейства протоколов TCP/IP на компьютере, работающем под управлением Microsoft Windows NT 4. Мы расскажем как о процессе установки TCP/IP, так и о требуемых и дополнительных настройках. Также будет объяснена настройка службы определения имен Интериста (WINS) и службы формирования имен узлов (DNS).

Установка поддержки TCP/IP в Windows NT 4

Когда вы устанавливаете поддержку TCP/IP на компьютере, работающем под управлением Windows NT, вы устанавливаете основные компоненты, необходимые для работы TCP/IP, а также некоторое количество полезных утилит для работы с сетью. На Windows NT Server вы также устанавливаете и настраиваете службы сервера WINS, DNS и DHCP. Эти службы позволяют вашему Windows NT Server предоставлять другим узлам сети возможность определения имен Интернета и получения настроек TCP/IP по сети.

При установке TCP/IP также устанавливается несколько клиентских утилит, таких как FTP-клиент и Telnet. Эти утилиты позволяют подключаться к другим TCP/IP-узлам в вашей сети или в Интернете. FTP-клиент позволяет установить соединение с FTP-сервером, после чего копировать файлы с сервера и на сервер. Telnet — это утилита, которая может быть использована для работы с интерпретатором командной строки удаленной системы. Эти и другие утилиты подробно обсуждаются в главе 13, «Коммуникации».

Процесс установки

Прежде чем вы начнете установку и настройку TCP/IP (или любого другого протокола) на компьютере, работающем под управлением Windows NT, вы должны войти в систему в качестве члена локальной группы администраторов. Политика безопасности Windows NT позволяет только тем, кто входит в такую группу, производить изменения в настройках системы.

Внимание

Вы должны войти в систему как член локальной группы администраторов, чтобы иметь возможность произвести изменения в настройках Windows NT.

Вам также следует убедиться, что исходный дистрибутив Windows NT будет доступен вам при установке. Он может находиться на компакт-

диске или быть скопированным в разделяемый каталог одной из машин сети. Для установки или обновления сетевых компонентов достаточно скопировать содержимое соответствующего каталога (для процессоров Intel это каталог I386) с компакт-диска в один из разделяемых каталогов сети.

Совет

Если вы собираетесь устанавливать или копировать файлы из разделяемого сетевого каталога, какой-либо вид транспортного протокола (такой, как NetBEUI или NWLink IPX/SPX-совместимый транспорт) уже должен быть установлен. Убедитесь, что по крайней мере один протокол, используемый в вашей сети, уже установлен.

В следующих разделах описан процесс установки TCP/IP для Windows NT. В этом разделе мы обсудим концепции, сложности и возможные экзаменационные вопросы, имеющие отношение к этому процессу.

Для того чтобы установить или удалить сетевые компоненты, а также внести изменения в настройки сети вы должны сначала открыть Network Control Panel. Для этого в меню Start выберите команду Settings ➤ Control Panel, затем дважды щелкните на значк Network; вы также можете щелкнуть правой кнопкой на значке Network Neighbourhood на рабочем столе и выбрать Properties из контекстного меню. После того как вы это сделаете, откройте вкладку Protocols и нажмите кнопку Add.

Затем найдите и выберите протокол TCP/IP в списке доступных протоколов и нажмите кнопку OK. После этого начнется процесс установки. Вы увидите окно диалога, показанное на рис. 3.1. Вы должны указать, хотите ли вы использовать DHCP (протокол динамической конфигурации узла). Сервер DHCP может автоматически производить настройку TCP/IP на вашем компьютере. Если служба удаленного доступа (Remote Access Service, RAS) установлена, вам также будет задан вопрос, хотите ли вы сконфигурировать RAS для использования протокола TCP/IP.

DHCP обеспечивает автоматическую настройку конфигурации TCP/IP-узлов. На каждой машине, на которой вы хотите использовать DHCP, клиентское программное обеспечение должно быть настроено на использование DHCP (см. рис. 3.1). Сервер DHCP передает клиенту IP-адрес, маску подсети и адрес шлюза по умолчанию, а также многие другие параметры TCP/IP. За дополнительной информацией о DHCP обратитесь к главе 11, «Протокол динамической конфигурации узла».

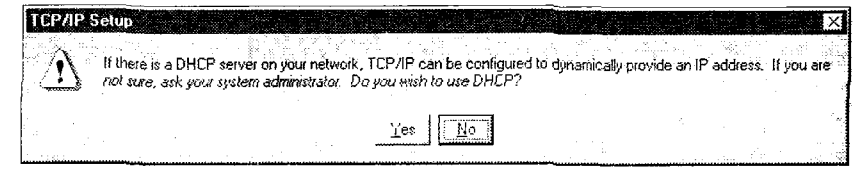


Рис. 3.1. Окно диалога установки TCP/IP, предлагающее разрешить или запретить использование DHCP

Windows NT должна произвести копирование необходимых файлов из каталога I386 компакт-диска с дистрибутивом Windows NT Server, поэтому в процессе установки у вас будет запрошено расположение этих файлов. Введите в окне диалога File Location путь к файлам на компакт-диске (например, D:\I386) или путь к файлам в сети (например, \\APPS\I386).

После того как Windows NT закончит копирование основных файлов TCP/IP и устанавливаемых по умолчанию сетевых утилит, нажмите кнопку OK. После этого вам будет предложено установить необходимые параметры TCP/IP.

Настройка TCP/IP в Windows NT 4

Если вы решили не использовать DHCP, то вы должны произвести настройку TCP/IP вручную. Этот процесс включает в себя установку IP-адреса, маски подсети и адреса шлюза по умолчанию (если требуется взаимодействие с удаленными сегментами сети). Кроме того, вы можете установить адреса серверов WINS и DNS, имеющихся в вашей сети. Вы также можете произвести более сложную настройку — например, установить несколько IP-адресов или поддержку нескольких сетевых карт.

Вкладка свойств IP-адреса

Для того чтобы TCP/IP-узел правильно работал в сети, он должен быть настроен на использование правильного IP-адреса и маски подсети. Если вы не используете DHCP, эта информация должны быть введена вручную.

Для того чтобы выполнить настройку TCP/IP вручную, выберите в меню Start команду Settings ➤ Control Panel, затем дважды щелкните значок Network и откройте вкладку Protocols в появившемся окне. Затем нажмите кнопку Properties, откройте вкладку IP Address и измените требуемые настройки. Ниже приведен список, поясняющий функции элементов управления на этой вкладке.

Внимание

Если вы установите неверный IP-адрес, можете получить сообщение об ошибке Это говорит о том, что в сети возник конфликт адресов. Такое происходит, когда два или более компьютеров в сети используют один и тот же IP-адрес. Вы должны убедиться, что устанавливаемый адрес правилен, до того, как начать настройку TCP/IP на любом компьютере.

Адрес шлюза по умолчанию (маршрутизатора) также должен быть установлен на узле, использующем TCP/IP, если он будет взаимодействовать с компьютерами вне локального сегмента сети.

- **Adapter.** Вы можете установить IP-адреса для всех установленных адаптеров (рис. 3.2). Вы можете использовать список Adapter для выбора адаптера, который вы хотите настраивать.

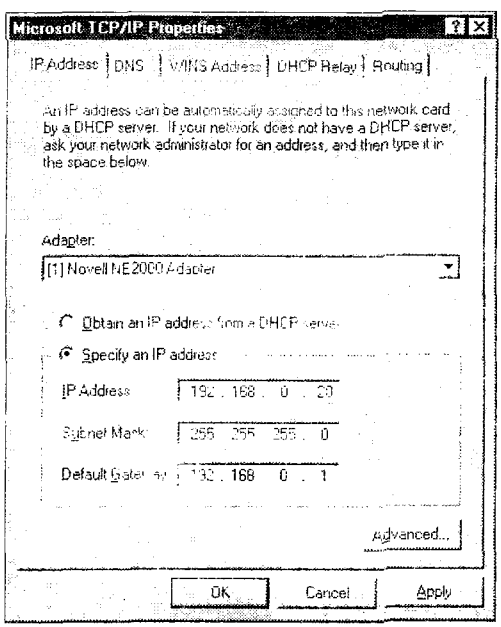


Рис. 3.2. Вкладка IP Address окна диалога настройки свойств TCP/IP

- **Obtain An IP Address From A DHCP Server.** Если в вашей сети имеется сервер DHCP, установите этот переключатель. После этого ваш компьютер сможет подключиться к локальному серверу DHCP и получить необходимую информацию о настройках IP. Если сервер DHCP недоступен, вы должны установить переключатель Specify An IP Address и ввести правильные IP-адреса, маску подсети и адрес шлюза по умолчанию для вашей сети (см. рис. 3.2).

Дополнительная настройка IP-адресации в Windows NT 4

Кнопка Advanced на вкладке IP Address окна диалога открывает окно диалога Advanced IP Addressing, показанное на рис 3.3. В нем вы можете настроить использование нескольких IP-адресов, а также нескольких шлюзов по умолчанию для каждого из установленных сетевых адаптеров. Кроме того, вы можете разрешить PPTP-фильтрацию или дополнительную политику безопасности для каждого из адаптеров в отдельности. PPTP-фильтрация запрещает обработку сетевыми интерфейсами Windows NT всех пакетов, кроме PPTP-пакетов.

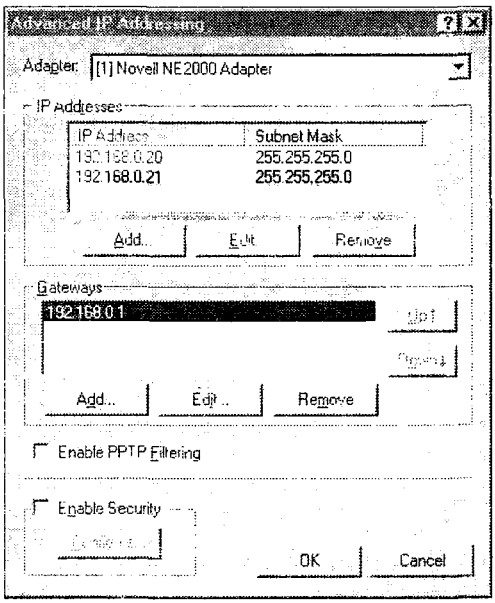


Рис. 3.3. Окно диалога Advanced IP Addressing

Совет

Вы можете использовать выпадающий список Adapter для выбора адаптера, который вы хотите настраивать. Это позволяет вам управлять несколькими сетевыми картами. Настройки каждого конкретного адаптера отображаются сразу же после его выбора из списка.

Ниже приведен список, поясняющий функции элементов управления в этом окне диалога.

- **IP Addresses.** Вы можете установить несколько IP-адресов для использования одним сетевым адаптером (рис. 3.3). Используя

это окошко, можно установить до четырех дополнительных адресов. Если вы хотите установить пять или более дополнительных IP-адресов для сетевой карты, вы можете сделать это, отредактировав реестр Windows NT. Нужная информация есть в документе TechNet article Q149426 «Adding More Than Five IP Addresses to NIC in Windows NT».

Совет

Установка нескольких IP-адресов для одного сетевого адаптера позволяет вам поддерживать несколько виртуальных Web-узлов на одном компьютере.

- **Gateways.** В окошке Gateways вы можете указать до пяти шлюзов. Шлюз, находящийся наверху списка, всегда используется первым. Если он почему-либо недоступен, TCP/IP попытается использовать все остальные шлюзы по порядку, пока один из них не примет информацию для дальнейшей передачи.
- **Enable PPTP Filtering.** Флажок Enable PPTP Filtering запрещает сетевому адаптеру обрабатывать любые пакеты, кроме PPTP-пакетов. Эта возможность обычно используется на компьютерах сети, предназначенных для использования исключительно в качестве PPTP-шлюза. Поскольку такие машины имеют как минимум один сетевой адаптер, соединенный с внешним миром, эта PPTP-фильтрация предотвращает несанкционированный доступ к серверу или локальной сети, соединенной с сервером через другие интерфейсы.

Совет

Поддержка PPTP (Point-To-Point Tunelling Protocol, туннельный протокол «точка-точка») — новая возможность Windows NT 4. PPTP является как клиентским, так и серверным компонентом, позволяющим безопасную передачу данных от клиента в частную сеть при помощи TCP/IP-сети, такой как Интернет. При помощи шифрования данных перед отправкой создается виртуальная частная сеть (VPN, Virtual Private Network), позволяя клиенту отправлять и получать данные при помощи потенциально небезопасного соединения. PPTP поддерживает NetBEUI, IPX и IP и может быть использован как в локальных и глобальных сетях, так и при коммутируемом подключении.

Дополнительную информацию о PPTP вы можете найти в главе 11 «PPTP» документа «Windows NT Server Networking Guide» в *Windows NT Server Resource Kit* (для NT версии 4) или в Microsoft Knowledge Base, документе Q161410 (который может быть найден на компакт-диске TechNet или во Всемирной паутине).

- **TCP/IP Security.** Эта возможность на самом деле является фильтром TCP/IP-пакетов (рис. 3.4). Этот фильтр позволяет вам управлять потоком входящих TCP/IP-пакетов, основываясь на номерах TCP/UDP-портов или IP-протоколе, с которыми связаны пакеты. К исходящему трафику фильтрация не применяется. Вы можете настроить отдельный фильтр для каждого используемого сетевого адаптера. Установите переключатель Permit Only, чтобы запретить обработку всего сетевого трафика для данного адаптера. Затем добавьте порты или протоколы, обработку которых вы хотите разрешить.

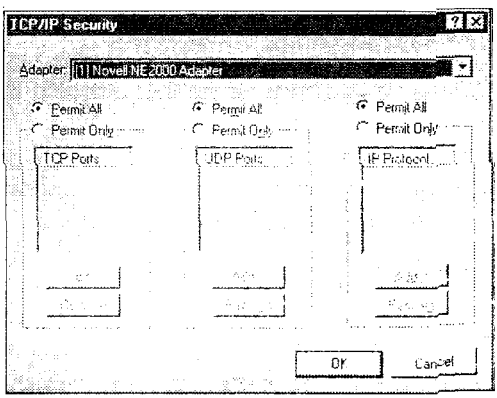


Рис. 3.4. Окно диалога TCP/IP Security

Вкладка настроек DNS

Microsoft TCP/IP в Windows NT 4 позволяет вам настроить использование сервера DNS (Domain Name Service, служба формирования имен узлов) для определения имен TCP/IP-узлов. Сервер DNS преобразует удобные в использовании имена узлов в их IP-адреса. Это позволяет вам не запоминать какой-либо запутанный набор цифр (например, 131.107.2.12), чтобы иметь возможность подключиться к удаленному компьютеру. Это похоже на возможности, предоставляемые сервером WINS (упомянутому выше в главе 2, «Концепции и планирование: TCP/IP и Windows NT»), — определение IP-адресов по именам NetBIOS.

Как DNS, так и WINS обеспечивают дружественное к пользователю определение IP-адресов по именам узлов (например, пользователь может вводить www.microsoft.com, а не запоминать адрес 207.68.156.61). Однако WINS обеспечивает динамическую регистрацию и определение имен NetBIOS, в то время как DNS использует статическую базу

данных, настройка и обновление которой должны производиться вручную. DNS и WINS также отличаются пространством имен (методом, используемым для именования компьютеров в локальной сети или в Интернете).

Соглашение об именовании, применяемое WINS, использует однородное пространство имен, в то время как соглашение об именовании, применяемое DNS, использует пространство имен с иерархической структурой. Пространство имен NetBIOS однородно, поскольку имена NetBIOS состоят только из одной части.

Администрирование такого пространства имен несложно, когда вы имеете дело с небольшой организацией, но, как только сеть становится больше, все труднее и труднее избегать использования повторяющихся имен. WINS упрощает работу администратора, позволяя каждому компьютеру в процессе загрузки операционной системы автоматически зарегистрировать свое имя и IP-адрес в базе данных WINS. Если запрошенное имя NetBIOS уже используется, NetBIOS не будет инициализирована правильным образом на запрашивающей машине.

Пространство имен DNS имеет иерархическую структуру: каждое имя состоит из имени узла и имени домена. Например, имя www.xerox.com состоит из имени узла — www и имени домена — xerox.com. Такое разделение позволяет осуществлять децентрализованное администрирование пространства имен. Целая организация определяется определенным именем домена, таким, как xerox.com, и этот домен может содержать поддомены, например, server5.xerox.com. Локальный администратор может назначать компьютерам внутри таких поддоменов имена узлов, не заботясь о том, чтобы имена внутри организации не повторялись. Сочетание имен узла, поддомена и домена образует полное доменное имя (FQDN, Fully Qualified Domain Name), такое как www.server5.xerox.com.

В отличие от WINS DNS не позволяет динамическую регистрацию и определение имен DNS. Это означает, что каждый раз, как DNS-имя узла изменяется или узел перемещается в другую подсеть (что влечет изменение IP-адреса), администратор должен вручную обновить базу данных DNS. Дополнительную информацию о DNS вы можете найти в главе 8, «Определение имен узлов», и в главе 9, «Служба формирования имен узлов (DNS)».

Ниже приведен список, поясняющий функции элементов управления на вкладке DNS окна диалога настройки TCP/IP (рис. 3.5):

- **Host Name.** По умолчанию имя узла, задаваемое в поле Host Name, должно совпадать с текущим именем NetBIOS данного компьютера. Не следует изменять его без особых на то причин.

- **Domain.** Для того чтобы узел мог корректно работать в IP-сети, вы должны ввести правильное имя домена для вашей организации (если вы не знаете его, обратитесь к администратору сети). Сочетание имени узла и имени домена образует FQDN. FQDN становится именем, под которым машина будет известна серверу DNS.

Совет

В Windows NT 4, DNS и WINS интегрированы друг с другом. Тесные связи между этими двумя службами обеспечивают некоторую форму динамической DNS (предлагаемого стандарта, который позволит узлам динамически регистрировать свое имя и IP-адрес на сервере DNS). Хотя эти связи и не обеспечивают истинную динамическую DNS, они позволяют серверу DNS на основе Microsoft Windows NT 4 обращаться с серверу WINS в том случае, когда он не может самостоятельно определить адрес, соответствующий имени узла.

- **DNS Service Search Order.** Введите IP-адрес сервера DNS (или несколько адресов, если вы хотите использовать несколько серверов DNS). Вы можете ввести в этом окне до трех адресов серверов DNS и, используя кнопки с изображениями стрелок, изменить порядок, в котором эти серверы будут опрашиваться при определении адреса, соответствующего имени узла.

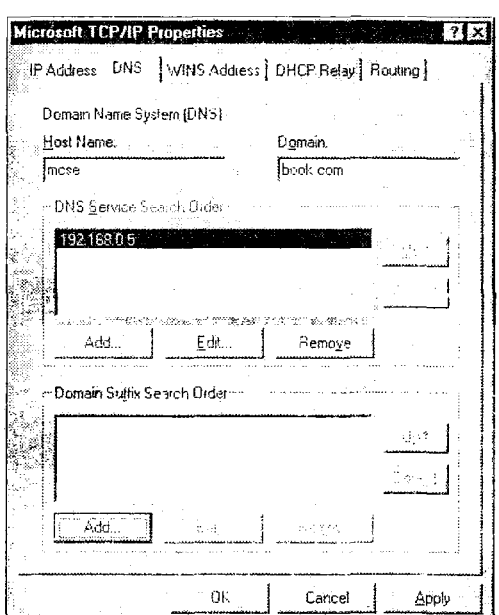


Рис. 3.5. Вкладка DNS окна настройки свойств TCP/IP

- **Domain Suffix Search Order.** Вы можете ввести в этом окошке дополнительные суффиксы доменов для использования при определении адреса. Эти суффиксы будут использоваться для образования полных доменных имен при попытке определить адрес машины, заданной только именем узла. Сначала в качестве суффикса будет использоваться имя локального домена, а затем подряд суффиксы из списка.

Вкладка настроек WINS

WINS позволяет компьютерам, работающим под управлением Windows, динамически регистрировать свои имена NetBIOS, а также производить поиск IP-адреса, соответствующего данному имени NetBIOS. На клиентах WINS должен быть задан IP-адрес сервера WINS. После этого клиент сможет для определения адресов обращаться непосредственно к серверу WINS. Для того чтобы при помощи WINS определить адрес, соответствующий данному имени, нет необходимости производить широковещательный запрос. Это снижает объем сетевого трафика, связанного с разрешением имен. Эта технология полезна и при использовании компьютеров, которые либо не имеют временно своего IP-адреса, либо часто изменяют его (например, при использовании DHCP). Динамическая база данных на сервере WINS автоматически обновляется при смене IP-адресов клиентов. Вкладка настроек WINS показана на рис. 3.6.

Ниже приведен список, поясняющий функции элементов управления на этой вкладке.

- **Adapter.** WINS может настраиваться отдельно для каждого из установленных сетевых адаптеров. Используйте список Adapter для выбора того адаптера, для которого вы хотите произвести настройку WINS.
- **Primary WINS Server** и **Secondary WINS Server.** Введите в этих полях адреса основного и дополнительного серверов WINS. Если Windows NT не получает ответа от основного сервера WINS, она производит обращение к дополнительному.
- **Enable DNS for Windows Resolution.** Этот флажок позволяет вам использовать DNS-имена узлов и полные доменные имена при работе с приложениями Windows. Эти приложения обычно ожидают, что будет указано имя NetBIOS, но, если вы установите этот флажок, также можно будет использовать имена DNS.
- **Enable LMHOSTS Lookup.** Этот флажок позволяет использовать статический файл соответствий между именами NetBIOS и IP-адресами. Этот файл может использоваться для поддержки рабо-

ты сервера WINS. Однако этот файл статический и должен обновляться вручную при изменении имен или адресов. Пример файла LMHOSTS и файла HOSTS может быть найден в каталоге \winnt\system32\drivers\etc. Файл LMHOSTS будет подробно обсуждаться в главе 8, «Определение имен узлов», и в главе 10, «Определение имен NetBIOS».

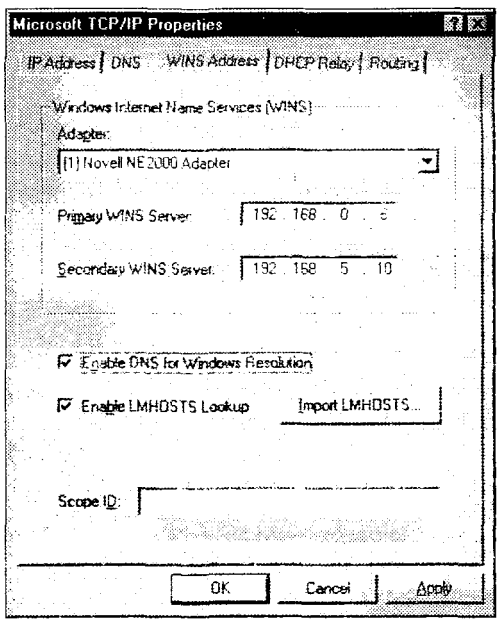


Рис. 3.6. Вкладка WINS окна настройки свойств TCP/IP

Совет

Пример такой возможности — использование команд NETUSE или NETVIEW. Команда NETUSE обычно имеет вид NETUSE T:*имя NetBIOS**имя разделяемого ресурса*. Однако, если вы установили флажок Enable DNS For Windows Resolution, команда может использоваться в следующей форме: NETUSE T:*FQDN или IP-адрес**имя разделяемого ресурса*.

- **Import LMHOSTS.** Эта кнопка позволяет автоматически импортировать файл LMHOSTS. Этот файл может располагаться как на локальной системе, так и на другом компьютере сети.
- **Scope ID.** Оставьте это поле пустым, если у вас нет необходимости изменить его (и, конечно, вы должны понимать, что делаете). Это поле позволяет отделить коммуникации NetBIOS от обычно широковещательного трафика NetBIOS. Однако только машины, име-

ющие одну и ту же запись в поле Scope ID, смогут взаимодействовать друг с другом. Это может помочь в установлении политики безопасности, если вы имеете компьютер (или несколько), к которым вам нужно ограничить доступ. Но помните: только машины, имеющие одну и ту же запись в поле Scope ID, смогут взаимодействовать друг с другом. Вы можете ввести в поле Scope ID любую строку, например «resource». Имейте в виду, что регистр букв имеет значение — строки «Resource» и «resource» различны.

Вкладка DHCP Relay

Протокол DHCP (упомянутый в начале этой главы) обеспечивает передачу TCP/IP-узлам локальной сети необходимых настроек. Однако в связи с тем, что машины, обращающиеся к серверу DHCP за необходимой информацией, еще не имеют собственного IP-адреса, они производят широковещательные запросы в локальной сети, которые обычно не проходят через маршрутизаторы в другие подсети.

Если в вашей сети имеется более одной подсети, но не в каждой из них имеется свой сервер DHCP, компьютер под управлением Windows NT или Windows 95 (с дополнительным программным обеспечением) может быть настроен как агент ретрансляции DHCP (DHCP Relay Agent). Агент ретрансляции DHCP может быть настроен на прием и переотправку DHCP-запросов непосредственно серверу DHCP в другой подсети. DHCP производит обработку таких запросов и возвращает требуемую информацию компьютеру, отправившему запрос.

Чтобы можно было настроить узел как агент ретрансляции DHCP, должно быть установлено соответствующее программное обеспечение. Если вы еще не установили необходимые компоненты, Windows NT предложит вам сделать это после изменения настроек на вкладке DHCP Relay окна диалога настройки свойств TCP/IP.

Чтобы произвести настройку агента ретрансляции DHCP, выполните следующие шаги:

1. Откройте вкладку DHCP Relay. Вы можете оставить значения по умолчанию в полях Seconds Threshold и Maximum Hops. Значение по умолчанию в 4 секунды в поле Seconds Threshold означает, что ретрансляция DHCP-запроса будет произведена только в том случае, если в течение четырех секунд на DHCP-запрос не ответит локальный сервер DHCP. Значение в поле Maximum Hops запрещает ретрансляцию пакетов, имеющих счетчик хопов более указанного числа. Эта возможность является функцией TTL (Time to Live, время жизни) полученного пакета.
2. Введите IP-адрес сервера DHCP, которому будут отправляться полученные DHCP-запросы (или несколько адресов, если вы хотите использовать несколько серверов).

3. После того как вы завершите настройку агента ретрансляции, подтвердите сделанные настройки и укажите Windows NT, нужно ли произвести установку дополнительных компонентов системы (или они уже были установлены).

Вкладка свойств маршрутизации

Эта вкладка содержит только один элемент управления. Это флажок, позволяющий включить или выключить IP-маршрутизацию для данного компьютера. Если компьютер настроен на использование нескольких сетевых адаптеров, установка этого флажка разрешает передачу пакетов с одного сетевого интерфейса на другой. Это превращает ваш Windows-компьютер в простейший маршрутизатор. Если вы разрешаете использование этой возможности, вы должны добавить описания маршрутов в таблицу маршрутизации или разрешить использование информационного протокола маршрутизации (RIP, Routing Information Protocol). Вы можете не изменять таблицу маршрутизации и не использовать RIP, если ваш компьютер под управлением Windows NT физически соединен со всеми сегментами и в сети не присутствует других маршрутизаторов. Однако, если в вашей сети существует несколько маршрутизаторов и сегментов, необходимо произвести настройку статической таблицы маршрутизации или установить RIP. Подробную информацию о маршрутизации и RIP вы найдете в главе 6, «Реализация IP-маршрутизации».

Перезагрузка компьютера

После того как вы закончите настройку TCP/IP, для того, чтобы новые настройки начали работать, вы должны перезагрузить Windows NT. Сделанные вами изменения будут сохранены, и будет произведен пересмотр привязок всех адаптеров и служб, которые теперь установлены. Если автоматической презагрузки Windows NT не произойдет, вы должны сделать это вручную.

Проверка и тестирование настройки

Теперь, после того как вы завершили установку и настройку TCP/IP, вы должны убедиться, что все работает правильно. Вам помогут две очень полезные утилиты — `IPCONFIG` и `PING`.

`IPCONFIG` является утилитой командной строки Windows NT, предоставляющей вам доступ к большей части информации о настройке TCP/IP без использования графического интерфейса (рис. 3.7). Используйте эту команду с ключом `/ALL` для вывода имени узла, адресов DNS, маршрутизации и IP-информации о каждом настроенном адаптере.

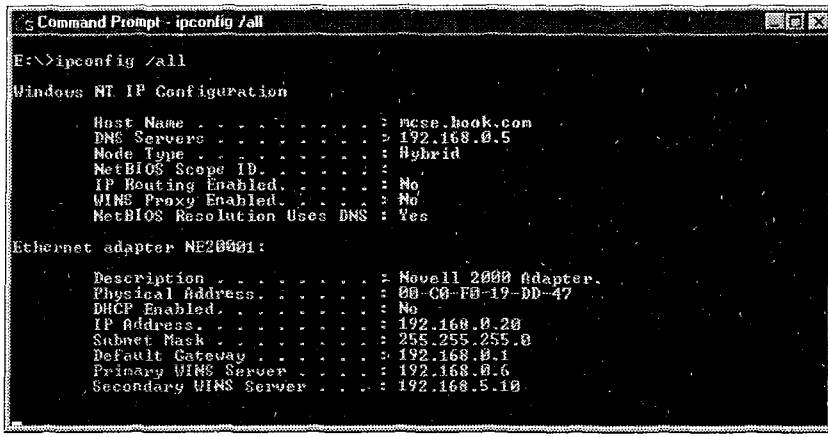


Рис. 3.7. Вывод команды IPCONFIG /ALL

Используйте эту команду для проверки правильности введенной вами при настройке информации. Если все выглядит правильно, вы должны использовать утилиту PING (Packet InterNet Groper, пакетный ощупыватель Интернета) для того, чтобы проверить, что ваши настройки действительно работают.

PING является утилитой, использующей протокол ICMP (обсуждавшийся в главе 2) для запроса ответа с TCP/IP-узла. Синтаксис команды PING таков:

PING <IP-адрес или имя узла>

Когда вы используете утилиту Microsoft PING, она обычно производит четыре эхо-запроса, выводя соответствующие ответы TCP/IP-узла на экран (рис. 3.8).

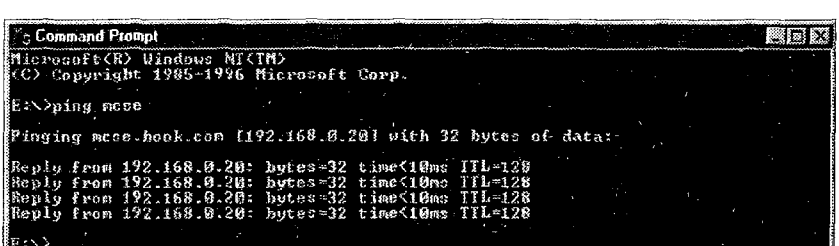


Рис. 3.8. Вывод команды PING

Хотя утилита PING может работать как с IP-адресами, так и с именами узлов или полными доменными именами, при определении про-

блемы в сети рекомендуется использовать IP-адрес. Это исключит из рассмотрения проблемы со службой определения имен.

Первый шаг в тестировании конфигурации — запуск PING для своего собственного локального адаптера, адрес которого 127.0.0.1. При этом соединения с какой-либо удаленной машиной не произойдет, но будет протестирована локальная IP-конфигурация от программного обеспечения сетевого адаптера до семейства протоколов. Если вы получите ответ с этого адреса, можете быть уверены как минимум в том, что TCP/IP правильно настроен на локальном узле.

Затем запустите PING для IP-адреса, который вы присвоили данному компьютеру. Если вы получите ответ и с этого адреса, можете предположить, что ваш IP-адрес правильно настроен.

После этого попытайтесь запустить PING для какого-либо компьютера в вашем локальном сетевом сегменте. Если вы не знаете точного IP-адреса, можете попробовать PINGовать адреса, близкие к адресу, присвоенному вашему компьютеру. Например, если ваш адрес 192.168.0.66, попробуйте запустить PING для адреса 192.168.0.67 или 192.168.0.68.

После того как вы убедитесь, что ваша система может нормально работать внутри вашего сегмента или локальной подсети, вы должны проверить, может ли информация с вашего компьютера проходить через маршрутизаторы.

Запустите PING для IP-адреса интерфейса маршрутизатора, соединенного с вашим сегментом. Если вы получите ответ, проверьте IP-адреса других интерфейсов маршрутизатора (не подключенных к вашей локальной сети). Наконец, если все работает, запустите PING для узла вне вашей подсети (по другую сторону от маршрутизатора).

Если у вас возникли проблемы с одним из перечисленных адресов, используйте полученную вами к этому моменту информацию для определения причины проблемы. Если вы не получаете ответа с вашего собственного адреса, — проблема в настройках вашего компьютера. Если вы получаете ответ от систем в вашем сегменте, но не можете вступить во взаимодействие с узлами за маршрутизатором, проблема может быть как в ваших собственных настройках, так и в настройках маршрутизатора или компьютера, от которого вы пытаетесь получить ответ. Как видите, чтобы установить имеющуюся проблему, вы должны быть методичны, спокойны и последовательны в поиске неисправности.

Вопросы для подготовки к экзамену

Question 1

You are getting ready to install and configure TCP/IP on your Windows NT Server. Which of the following items are not requirements to complete the installation? (Check all correct answers.)

- ❑ A. You must be a member of the local administrators group for the machine you're configuring.
- ❑ B. You must be a domain administrator for the domain in which the machine is installed.
- ❑ C. You must have some type of sccess to the original installation files.
- ❑ D. You must have a good understanding of the required settings and configurations.

Вопрос 1

Вы собираетесь установить и настроить поддержку TCP/IP на Windows NT Server. Что вам не потребуется для завершения установки? (Укажите все правильные ответы.)

- ❑ A. Вы должны быть членом локальной группы администраторов на компьютере, который вы настраиваете.
- ❑ B. Вы должны быть администратором домена, в котором установлен настраиваемый компьютер.
- ❑ C. Вы должны иметь доступ к дистрибутиву системы.
- ❑ D. Вы должны хорошо понимать, какие настройки следует произвести.

Правильный ответ — B. Вам не обязательно быть администратором домена для того, чтобы установить поддержку TCP/IP на обычной NT Workstation или NT Server. Однако все перечисленное в пунктах A, C и D необходимо. Следует внимательно читать вопросы. На первый взгляд кажется, что следует отметить ответы A, C и D, поскольку они перечисляют необходимые требования. Но вы должны отметить то, что не требуется, поэтому, конечно, правильный ответ — B.

Question 2

Which of the following statements about DHCP are correct? (Choose two.)

- ❑ A. DHCP is a service that provides TCP/IP configuration information to machines that request it.
- ❑ B. DHCP is a service that provides for the resolution of friendly names to IP addresses.
- ❑ c. Each TCP/IP client must be configured to access a DHCP server if you want it to use this service.
- ❑ D. When configuring a client to use DHCP, you must supply the client with the IP address of the DHCP server.

Вопрос 2

Какие из следующих утверждений о DHCP верны? (Выберите два.)

- ❑ A. DHCP — это служба, предоставляющая информацию о настройках TCP/IP запрашивающей их системе.
- ❑ B. DHCP — это служба, обеспечивающая преобразование понятных пользователю имен в IP-адреса.
- ❑ C. Каждый TCP/IP-клиент, на котором вы хотите использовать DHCP, должен быть настроен на это.
- ❑ D. Когда вы настраиваете клиента на использование DHCP, вы должны указать IP-адрес сервера DHCP.

Ответ на этот вопрос — A и C. DHCP является службой, предоставляющей клиентам информацию о настройках TCP/IP, и каждый ее клиент должен быть настроен на использование этой службы. DHCP не предоставляет механизма для определения адресов, соответствующих именам. Следовательно, ответ B неверен. Кроме того, нет необходимости указывать IP-адрес сервера DHCP; поскольку обращающаяся к серверу DHCP система еще не имеет собственного IP-адреса, она может отправить только широковещательный запрос. Следовательно, ответ D неверен.

Question 3

On the Advanced IP Addressing Properties sheet, what is the total number of IP addresses that can be added through this interface?

- ○ A. 4
- ○ B. 5
- ○ C. 10
- ○ D. Unlimited

Вопрос 3

Какое количество IP-адресов может быть добавлено в окне диалога Advanced IP Addressing?

- ○ A. 4
- ○ B. 5
- ○ C. 10
- ○ D. Неограниченное число

Правильный ответ — B. В Windows NT вы можете установить до пяти IP-адресов в окне диалога Advanced IP Addressing. Вы можете установить и большее количество адресов, но для этого вам придется

вносить изменения в реестр. Следовательно, ответы A, C и D неверны.

Question 4

Which of the following statements about PPTP are correct? (Check all correct answers.)

- ❑ A. It has both a server and a client component.
- ❑ B. It uses a form of encryption.
- ❑ C. It can be used to send data securely over TCP/IP networks.
- ❑ D. It supports IP and IPX, but not NetBEUI.

Вопрос 4

Какие из следующих утверждений о PPTP верны? (Выберите все правильные ответы.)

- ❑ A. Это компонент как клиента, так и сервера.
- ❑ B. Он использует некоторый вид шифрования.
- ❑ C. Он может быть использован для безопасной передачи данных по TCP/IP-сетям.
- ❑ D. Он поддерживает IP и IPX, но не NetBEUI.

Правильные ответы на этот вопрос — A, B и C. PPTP (Point-To-Point Tunneling Protocol) используется для отправки шифрованных данных по TCP/IP-сетям — как по сетям открытого доступа, так и по закрытым. Для того чтобы использовать PPTP, как на клиенте, так и на сервере должно быть установлено соответствующее программное обеспечение. PPTP поддерживает IP, IPX и NetBEUI. Следовательно, ответ D неверен.

Question 5

You are attempting to resolve a communication problem with a computer named bob15 on a remote subnet. You can successfully PING other computers on the same subnet as bob15; however, when you try to PING bob15, you get no response. Which of the following could be the problem? (Check all correct answers.)

- ❑ A. Your default gateway is configured incorrectly.
- ❑ B. Bob15 has an incorrect default gateway.
- ❑ C. Bob15 has a NetBIOS Scope ID that is different than the other computers, including yours.
- ❑ D. Bob15 is offline.

Вопрос 5

Вы пытаетесь определить источник проблем с компьютером bob15 в удаленной подсети. При использовании утилиты PING другие компьютеры, находящиеся в той же подсети, что и bob15, отвечают, однако сам bob15 не отвечает. В чем может заключаться проблема? (Выберите все возможные ответы.)

- ❑ A. Ваш шлюз по умолчанию настроен неверно.
- ❑ B. На компьютере bob15 неверно указан шлюз по умолчанию.
- ❑ C. На компьютере bob15 установлен Scope ID, отличный от установленного на других компьютерах, в том числе вашем.
- ❑ D. Компьютер bob15 отключен от сети.

Правильные ответы — B и D. Если компьютеры той же подсети, в которой расположен bob15, отвечают вам, это означает, что ваш шлюз по умолчанию настроен правильно. Однако, если на компьютере bob15 неверно указан адрес шлюза по умолчанию, то ответ на команду PING может не дойти до вас. Установки NETBIOS не влияют на работу команды PING. Ответ C неверен. И, конечно, если компьютер выключен или отключен от сети, он также не будет отвечать вам.

Question 6

You want to install a Windows NT computer to route IP traffic between two segments. These will be the only two segments on your small network. Which of the following must be done in order to make this possible? (Check all correct answers.)

- ❑ A. The Windows NT computer must be configured with two network cards.
- ❑ B. Each network card must be attached to the same subnet.
- ❑ C. IP forwarding must be enabled on the multihomed computer.
- ❑ D. RIP routing must be configured on the Windows NT router.

Вопрос 6

Вы хотите использовать компьютер под управлением Windows NT для маршрутизации IP-трафика между двумя сегментами сети. Это единственные два сегмента вашей небольшой сети. Что вы должны сделать? (Укажите все правильные ответы.)

- ❑ A. В компьютер должны быть установлены две сетевые карты.
- ❑ B. Все сетевые карты компьютера должны быть подключены к одной подсети.
- ❑ C. На компьютере должна быть разрешена ретрансляция IP-пакетов.
- ❑ D. На маршрутизаторе на основе Windows NT должен быть настроен RIP.

Правильные ответы на этот вопрос — A и C. Вы должны поместить в ваш компьютер с Windows NT две сетевые карты и разрешить ретрансляцию IP-пакетов (IP forwarding), чтобы компьютер мог работать в качестве маршрутизатора. Вы не должны подключать обе сетевые карты к одному сегменту сети; наоборот, вы должны подключить их к разным сегментам, чтобы иметь возможность маршрутизировать трафик между сегментами. Вам не понадобится RIP или статическая таблица маршрутизации, поскольку ваш компьютер будет подключен к обоим сегментам. Также среди предложенных ответов не упомянуто, что вы должны настроить каждый из сетевых адаптеров для работы в своем сегменте. Это важно, поскольку это позволяет маршрутизатору на основе Windows NT знать, куда следует отправлять получаемые пакеты.

Question 7

You have been asked to configure several Windows NT Workstations for your company's network that uses DNS and WINS for name resolution.

Required Result:

- The computers must be able to communicate with each other via a computer name, Internet-style name and IP address.

Optional Desired Results:

- Keep the broadcast traffic to a minimum.
- Give the clients a level of fault tolerance for name resolution if the primary WINS server is unavailable.

Proposed Solution:

- Place an LMHOSTS file on each computer that has mappings for the computer names and IP addresses.

Which results the proposed solution produce?

- A. The proposed solution produces the required result and produces both of the optional desired results.
- B. The proposed solution produces the required result and produces only one of the optional desired results.
- C. The proposed solution produces the required result but does not produce any of the optional desired results.
- D. The proposed solution does not produce the required result.

Вопрос 7

Вам требуется настроить несколько Windows NT Workstation для работы в сети вашей компании, которая использует DNS и WINS для определения имен.

Требуемый результат:

- Компьютеры должны иметь возможность связываться друг с другом, используя имя компьютера, Интернет-имя компьютера и IP-адрес.

Желательные результаты:

- Объем широковещательного трафика должен быть минимален.

- Обеспечить для клиентов отказоустойчивость определения имен по отношению к отказу основного сервера WINS.

Предлагаемое решение:

- Поместить на каждый компьютер файл LMHOSTS, содержащий соответствия имен компьютеров и их адресов.

К каким результатам приведет предлагаемое решение?

- A. Будет достигнут как требуемый результат, так и оба желательных результата.
- B. Будет достигнут требуемый результат и один из желательных результатов.
- C. Будет достигнут только требуемый результат.
- D. Требуемый результат не будет достигнут.

Правильный ответ на этот вопрос — D. Требуемый результат не будет достигнут. Файл LMHOSTS не позволяет определить адрес узла по его Интернет-имени, такому как www.microsoft.com. Вы должны использовать сервер DNS или файл HOSTS для определения адреса узла по его Интернет-имени. Запомните, если в таком вопросе, как этот, не достигается требуемый результат, вы можете не обращать внимания на желательные результаты.

Question 8

You have been asked to configure several Windows NT Workstations for your company's network that uses DNS and WINS for name resolution.

Required Result:

- The computers must be able to communicate with each other via a computer name, Internet-style name, or IP address.

Optional Desired Results:

- Keep the broadcast traffic to a minimum.
- Give the clients a level of fault tolerance for name resolution if the primary WINS server is unavailable.

Proposed Solution:

- Configure the TCP/IP protocol for each NT Workstation and configure each Workstation with the IP address of the WINS server and the DNS server.

Which results does the proposed solution produce?

- A. The proposed solution produces the required result and produces both of the optional desired results.
- B. The proposed solution produces the required result and produces only one of the optional results.
- C. The proposed solution produces the required result but does not produce any of the optional desired results.
- D. The proposed solution does not produce the required result.

Вопрос 8

Вам требуется настроить несколько Windows NT Workstation для работы в сети вашей компании, которая использует DNS и WINS для определения имен.

Требуемый результат:

- Компьютеры должны иметь возможность связываться друг с другом, используя имя компьютера, Интернет-имя компьютера или IP-адрес.

Желательные результаты:

- Объем широковещательного трафика должен быть минимален.
- Обеспечить для клиентов отказоустойчивость определения имен по отношению к отказу основного сервера WINS.

Предлагаемое решение:

- Настроить поддержку протокола TCP/IP на каждой Windows NT Workstation и указать на каждой рабочей станции IP-адреса серверов DNS и WINS.

К каким результатам приведет предлагаемое решение?

- A. Будет достигнут как требуемый результат, так и оба желательных результата.
- B. Будет достигнут требуемый результат и один из желательных результатов.
- C. Будет достигнут только требуемый результат.
- D. Требуемый результат не будет достигнут.

Правильный ответ — B. После того как вы установите на клиентах адреса серверов WINS и DNS, все компьютеры будут в состоянии определить IP-адрес узла как по его имени NetBIOS, так и по его Интернет-имени. Использовать IP-адреса вы можете всегда. Одним из основных преимуществ использования WINS является снижение объема широковещательного трафика. Установленный сервер WINS позволяет вам сказать, что объем широковещательного трафика сведен к минимуму. Единственное, чего не хватает в приведенном решении — резервного сервера WINS на случай отказа основного. Для того чтобы ответ A был правильным, требовалось бы установить на каждой рабочей станции адреса как основного, так и резервного серверов WINS. Естественно, в вашей сети должно быть два сервера WINS.

Дополнительная информация

Произведите поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевые слова «IP addressing» и родственные.

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы можете произвести поиск на компакт-диске, используя ключевые слова «TCP/IP» и «IP Addressing». Полезные материалы о TCP/IP могут быть найдены в томе «Networking Guide» *Resource Kit*.

IP адресация

Термины, необходимые для понимания материала:

- IP-адрес
- Точечно-десятичная запись
- Октет
- Двоичный вид адреса
- Идентификатор сети
- Идентификатор узла
- InterNIC
- Классы
- Подсети
- Маски подсетей

Приемы и знания, которыми вы должны овладеть:

- Понимание компонентов IP-адреса
- Преобразование адресов из двоичного вида в десятичный и обратно
- Определение количества узлов в сети по ее классу
- Использование маски подсети для определения пункта назначения IP-пакета

В этой главе мы обсудим основные компоненты IP-адреса, а также то, как IP-адрес используется для отправки информации из одной сети в другую. Мы обсудим входящие в состав IP-адреса идентификатор сети и идентификатор узла, а также классы, подсети и маскирование подсетей. Кроме того, мы опишем преобразование между двоичной и десятичной системами счисления, поскольку оно необходимо для понимания формата IP-адресов.

IP-адресация: исследованная и объясненная

IP-адрес — это просто число, однозначно определяющее TCP/IP-узел в Интернете или интрасети. В TCP/IP-терминологии «узлом» называется любая машина, имеющая сетевой интерфейс, настроенный на использование TCP/IP. Узлом, например, может являться Windows NT Server, рабочая станция Unix или один из множества маршрутизаторов, используемых для передачи информации из одной сети в другую.

Совет

Хотя термин «узел» используется для обозначения любого устройства, подключенного к TCP/IP-сети, он также используется при сравнении имен DNS с именами NetBIOS. Например, www.microsoft.com является именем узла, в то время как SERVER2 является именем NetBIOS, однако обе эти машины считаются узлами TCP/IP-сети. Это может вызвать путаницу, но обычно смысл слова «узел» хорошо понятен из контекста.

Схема адресации Интернета (или IP-адресации) похожа на схему адресации, используемую обычной почтой при доставке писем. IP-адрес состоит из двух компонентов: идентификатора сети и идентификатора узла. Можно считать, что Интернет соответствует вашему городу, идентификатор сети — названию улицы, а идентификатор узла — номеру дома.

Термин «Интернет» на самом деле обозначает набор взаимосвязанных сетей, а не одну сеть. Границы каждой из этих взаимосвязанных сетей созданы маршрутизаторами, которые используются для сегментации и разделения сетевого трафика. Каждый интерфейс на маршрутизаторе обозначает отдельную сеть (или подсеть) и, следовательно, имеет отдельный идентификатор сети. Когда интерфейсы двух различных маршрутизаторов взаимодействуют друг с другом в одном физическом сегменте, они разделяют один идентификатор сети и определяются при помощи уникальных идентификаторов узла.

Идентификатор сети обозначает конкретную сеть (или сегмент), в которой узел физически находится. Можно провести аналогию с

названием улицы, на которой расположен конкретный дом. Этот адрес должен быть уникален во всей TCP/IP-сети, вне зависимости от того, является сеть глобальной TCP/IP-сетью или это просто небольшая локальная сеть компании, в которой реализован TCP/IP. Идентификатор сети используется для передачи информации на нужный сетевой интерфейс маршрутизатора (на нужную улицу — с точки зрения нашей аналогии). После того как информация попадает в нужную подсеть (в нужный сегмент сети), данные передаются нужному узлу — в соответствии с идентификатором узла. Все узлы, использующие один и тот же идентификатор сети, должны быть физически расположены в одном сегменте сети, чтобы информация могла достичь их. Если узел переносится из одного сетевого сегмента в другой, его сетевой адрес должен быть изменен.

Внимание

Уникальный идентификатор сети должен быть присвоен каждому физическому сегменту сети. Сети и подсети связываются при помощи маршрутизаторов. Следовательно, каждый интерфейс маршрутизатора должен использовать свой собственный идентификатор сети. Два маршрутизатора, имеющие интерфейсы, подключенные к одному физическому сегменту сети, разделяют для этих интерфейсов общий идентификатор сети, но имеют различные идентификаторы узла.

Идентификатор узла определяет конкретный узел в данной сети. Это очень похоже на номер дома в почтовом адресе, позволяющий найти дом среди таких же на улице. Эта часть адреса не должна повторяться для узлов одной подсети — каждый дом на улице должен иметь свой собственный номер. Узлы обычно имеют один сетевой интерфейс или сетевую карту, но некоторые узлы, такие как маршрутизаторы, могут быть настроены на использование нескольких сетевых интерфейсов. Каждый сетевой интерфейс узла должен иметь свой собственный уникальный IP-адрес, подобный показанному на рис. 4.1.

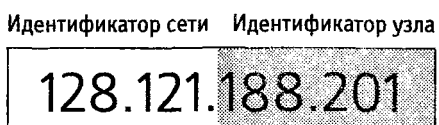


Рис. 4.1. Идентификатор сети и идентификатор узла в IP-адресе класса B

Форматы IP-адресов

IP-адреса могут представляться как в двоичном, так и в десятичном формате. Поскольку нам, людям, сложнее манипулировать числами,

чем нашим кремниевым компаньонам, мы обычно предпочитаем десятичный формат для записи IP-адресов.

Когда IP-адрес записан в десятичном формате, он состоит из четырех групп цифр, называемых октетами, каждая из которых отделана от соседней точкой. Такой способ записи IP-адресов называется точечно-десятичной записью.

Когда мы записываем адреса в десятичном формате, с первого взгляда не понятно, почему группа из трех цифр называется октетом (восемь знаков), но если мы рассмотрим двоичную запись адресов, все станет на свои места.

Компьютеры в отличие от людей «видят» мир двоичным. Для компьютера все состоит из «включено-выключено» («истина-ложь», «ноль-единица»). Такой незамысловатый взгляд на мир является следствием архитектуры вычислительной техники, хорошо подходящей для двоичных вычислений.

Для компьютера IP-адрес является 32-битовым числом (или 4-байтовым, поскольку каждый байт состоит из восьми бит). Каждый октет в десятичной записи может принимать значения от 0 до 255 и представляется восемью битами в двоичном формате, что и объясняет название «октет».

Например, в следующем примере число слева представляет собой двоичную версию адреса, записанного справа.

Двоичный IP-адрес	**IP-адрес в точечно-десятичной записи**
11000000 10101000 00000000 00000001	192.168.0.1

Вы легко можете убедиться, что двоичные числа слева соответствуют десятичным справа.

Преобразование между двоичным и десятичным форматами

Прежде чем вы начнете хорошо понимать IP-адресацию, вы должны хорошо понять, что такое двоичные числа и как они соответствуют десятичным. Этот обзор преобразования между двоичным и десятичным форматами предполагает, что вы уже понимаете это.

Как мы упоминали выше, каждый IP-адрес делится на четыре октета. Октет состоит из восьми бит. В двоичном формате каждый бит имеет значение 0 или 1. Эти нули и единицы соответствуют десятичным числам, равным 2^{n-1}, где n обозначает положение единицы в числе, считая справа налево. Единица указывает, что десятичное значение бита должно быть использовано, а ноль — что нет.

Внимание

Вы сможете использовать Microsoft Scientific Calculator в течение экзамена. Этот калькулятор позволяет вам производить преобразование чисел из десятичного формата в двоичный и обратно, переключая режим калькулятора. Это может сильно помочь вам, когда голова занята другими задачами. Однако вы не должны полагаться исключительно на калькулятор, поскольку время экзамена ограничено. Вместо этого вы должны убедиться, что легко можете произвести преобразование в уме и использовать калькулятор только в случае крайней необходимости.

Знание значений, перечисленных в табл. 4.1, поможет вам на экзамене. Это наиболее часто используемые значения, и знание их сэкономит время, которое вам потребуется для ответа на вопрос. Итак, знание стандартных двоично-десятичных пар значений и понимание того, как происходит преобразование нестандартных чисел (которые редко встречаются в экзамене), существенно помогут вам на экзамене.

Запомните, десятичным значением октета может быть число от 0 до 255, то есть сумма десятичных значений всех битов октета не может превышать 255 (табл. 4.1).

Таблица 4.1. Двоичные и десятичные значения некоторых октетов

Двоичное значение октета	Значения битов октета	Десятичное значение октета
00000000	0	0
10000000	128	128
11000000	128+64	192
11100000	128+64+32	224
11110000	128+64+32+16	240
11111000	128+64+32+16+8	248
11111100	128+64+32+16+8+4	252
11111110	128+64+32+16+8+4+2	254
11111111	128+64+32+16+8+4+2+1	255

В последней строке вы можете видеть, что если даже все биты октета равны 1, его десятичное значение не превышает 255. Вы можете заметить, что последовательность десятичных значений, приведенных в таблице, содержит большие пропуски. Эти пропуски могут быть заполнены при помощи отличных от приведенных девяти комбинаций «0» и «1» в октете. Например, чтобы получить значение 197, вам потребуется двоичное значение 11000101. В табл. 4.2 содержатся дополнительные примеры соответствия двоичных и десятичных значений.

Таблица 4.2. Дополнительные примеры соответствия двоичного и десятичного значений октета

Двоичное значение октета	Значения битов октета	Десятичное значение октета
11000101	128+64+0+0+0+4+0+1	197
11000110	128+64+0+0+0+4+2+0	198
11000111	128+64+0+0+0+4+2+1	199
11001000	128+64+0+0+8+0+0+0	200

Откуда берутся IP-адреса?

Каждый IP-адрес в Интернете или интрасети должен быть уникальным, вне зависимости от того, содержит сеть 1000 или 1000 000 узлов. Если сеть вашей компании настроена на использование TCP/IP и не соединена с Интернетом, то назначение и использование неповторяющихся адресов из пространства IP-адресов не является большой проблемой. Вы можете выбрать из всего пространства адресов те адреса, которые удовлетворяют вашим нуждам. В зависимости от размера компании один или несколько человек могут отвечать за назначение узлам каждой подсети сети компании уникальных IP-адресов. Однако, если сеть вашей организации должна быть соединена с Интернетом, становится значительно труднее убедиться, что данный IP-адрес уже не используется кем-либо еще.

За распределение и присвоение адресов в Интернете отвечает InterNIC (Сетевой информационный центр Интернета). Поскольку только одна группа отвечает за присвоение всех сетевых адресов в Интернете, достаточно просто следить за тем, чтобы адреса не повторялись. Однако InterNIC не следит за каждым адресом в Интернете. Вместо этого он выделяет организации сетевой идентификатор, позволяющий создать в данной подсети необходимое количество узлов (см. следующий раздел). Организация может устанавливать идентификаторы узлов в своей подсети так, как ей это удобно.

Классы адресов

Итак, вы уже знаете, что IP-адреса — это числа, однозначно определяющие все без исключения узлы или сетевые интерфейсы в IP-сети. Эти адреса состоят из двух компонентов: идентификатора сети и идентификатора узла, которые определяют, для какой подсети и для какого конкретно узла в ней предназначен пакет данных. Вы также уже знаете, что IP-адреса могут представляться как в точечно-десятичном, так и в двоичном формате. Люди предпочитают использовать десятичную запись, в то время как компьютеры работают с адресами в двоичном формате.

Теперь, после того как мы обсудили преобразование двоичных адресов в десятичные, вы можете заметить взаимосвязь между количеством бит в адресе и общим количеством адресов, которые могут быть образованы при помощи данного количества бит.

Когда Интернет только зарождался, было решено, что адресное пространство, состоящее из 32-х бит, будет достаточным для всех сетей и узлов, которые будут когда-либо подключены к Интернету. 32-разрядное адресное пространство позволяет использовать примерно 4,3 миллиарда (2^{32}) различных адресов. Основатели Интернета не могли представить то невероятное разрастание Сети, которое произошло в последующие годы. Если бы они могли это предвидеть, они добавили бы пару лишних разрядов в адресное пространство, экспоненциально увеличив количество узлов, которые могут поддерживаться данным стандартом[1].

Разделив доступное адресное пространство на классы, можно выделять организациям блоки адресов в соответствии с общим количеством узлов, которые должны поддерживаться в организации.

В табл. 4.3 показаны (слева направо) классы адресов, значение старших битов адреса (старших битов первого октета), диапазон десятичных значений первого октета в данном классе и доступное количество сетей и узлов, поддерживаемых в данном классе.

Внимание

Таблица 4.3 содержит информацию, которую вы должны выучить к экзамену. Умение на экзамене с первого взгляда определить класс IP-адреса, количество сетей и количество узлов в данном классе — бесценно.

Таблица 4.3. Классы адресов и соответствующие им идентификаторы сетей и узлов

Класс адреса	Старшие биты	Диапазон десятичных значений первого октета	Доступное количество сетей	Доступное количество узлов
Класс A	0	1–126	126	16 777 214
Класс B	10	128–191	16 384	65 534
Класс C	110	192–223	2 097 152	254

[1] Один из разработчиков TCP/IP, Винтон Серф (Vinton Cerf), в 1994 году отметил, что если бы он знал, что TCP/IP станет международным стандартом, он бы выбрал адресное пространство большее, чем 32 разряда (Vinton G. Cerf, «The Internet Phenomenon»). — *Примеч. перев.*

В адресах класса A первый октет представляет идентификатор сети. В адресах класса B первые два октета используются для идентификатора сети, и, наконец, в адресах класса C первые три октета используются для идентификатора сети. Таким образом, каждый адрес можно разделить на два компонента, как показано в табл. 4.4.

Таблица 4.4. Разделение IP-адреса на компоненты в соответствии с его классом

Класс адреса	IP-адрес	Идентификатор сети	Идентификатор узла
Класс A	w.x.y.z	w	x.y.z
Класс B	w.x.y.z	w.x	y.z
Класс C	w.x.y.z	w.x.y	z

Адреса класса A

Класс A использует для идентификатора сети только первый октет и три оставшихся октета — для идентификатора узла. Старший бит первого октета адреса этого класса всегда равен нулю, позволяя определить, что это адрес класса A (табл. 4.5). Поскольку старший бит всегда равен 0, для идентификатора сети остается только семь бит. Эти семь бит позволяют создать максимум 127 различных сетевых адресов, но сетевой идентификатор 127 зарезервирован для локального сетевого адаптера (loopback adapter), обсуждаемого далее. Таким образом, в классе A доступны только 126 различных сетевых адресов.

Оставшиеся 24 бита доступны для использования в идентификаторе узла. Это позволяет использовать 16 777 214 ($2^{24}-2$) адресов узлов. Поскольку этот класс адресов позволяет использовать столь большое количество узлов в сети, эти адреса выдаются только организациям, которым требуется обеспечить доступ к чрезвычайно большому количеству узлов. На самом деле большая часть, если не все, из этих адресов уже выделены каким-либо организациям, как правило, военным или университетам, многие годы назад.

Таблица 4.5. Адрес класса A — идентификаторы сети и узла

Класс адреса	IP-адрес	Идентификатор сети	Идентификатор узла
Класс A	124.29.88.7	124	29.88.7

Адреса класса B

Класс B использует для идентификатора сети первый и второй октеты и два оставшихся октета для идентификатора узла. Два старших бита первого октета адреса этого класса всегда равны 10 (единица-ноль),

позволяя определить, что это адрес класса B (табл. 4.6). Поскольку старшие биты всегда равны 10, для идентификатора сети остается только четырнадцать бит. Эти четырнадцать бит позволяют создать максимум 16 384 различных сетевых адреса.

Оставшиеся 16 бит доступны для использования в идентификаторе узла. Что позволяет использовать 65 534 (2^{16}–2) адреса узла. Этот класс адресов предназначен для средних или больших сетей, и, хотя их непросто получить, некоторые из этих адресов еще доступны.

Таблица 4.6. Адрес класса B — идентификаторы сети и узла

Класс адреса	IP-адрес	Идентификатор сети	Идентификатор узла
Класс B	130.29.88.7	130.29	88.7

Адреса класса C

Класс C использует для идентификатора сети первые три октета и оставшийся октет — для идентификатора узла. Три старших бита первого октета адреса этого класса всегда равны 110 (единица-единица-ноль), позволяя определить, что это адрес класса C (табл. 4.7). Поскольку старшие биты всегда равны 110, для идентификатора сети остается только двадцать один бит. Это позволяет создать максимум 2 097 152 различных сетевых адреса.

Оставшиеся 8 бит доступны для использования в идентификаторе узла. Это позволяет использовать 254 (2^8–2) адреса узла. Этот класс адресов предназначен для небольших сетей, которым нужно поддерживать ограниченное количество узлов. Поскольку доступно очень много сетевых адресов класса C, их проще всего получить. Однако в связи с быстрым ростом Интернета, организация, желающая получить адрес класса C, должна продемонстрировать, что она нуждается в целом блоке из 254 адресов узлов.

Таблица 4.7. Адрес класса C — идентификаторы сети и узла

Класс адреса	IP-адрес	Идентификатор сети	Идентификатор узла
Класс C	192.29.88.7	192.29.88	7

Совет

Если вашей компании нужно несколько IP-адресов для подключения к Интернету, вы обычно можете получить небольшой блок адресов через посредника, например, от провайдера Интернета. Провайдеры обычно получают большой блок адресов с целью раздачи их тем клиентам, которым нужно только несколько адресов.

Если организации необходимо больше адресов, чем может предоставить подсеть класса C, но меньше, чем содержится в подсети класса B, она может получить несколько блоков адресов класса C. Однако это неоправданно усложняет таблицы маршрутизации Интернета. Обычно одной организации соответствует одна запись в таблице маршрутизации. Эта запись идентифицирует всю сеть организации при помощи указания ее сетевого идентификатора. После того как пакеты на адреса с данным сетевым идентификатором переправляются в сеть организации, ее дальнейшее распределение между узлами сети — работа локальных маршрутизаторов.

Необходимость эффективного использования доступного адресного пространства (а также необходимость уменьшения размеров таблиц маршрутизации на основных маршрутизаторах Интернета) стимулировала создание новой схемы IP-адресации, называемой CIDR (Classless Inter-Domain Routing, бесклассовая междудоменная маршрутизация). CIDR позволяет объединять несколько маршрутов для одной организации, использующей несколько сетевых адресов класса C. CIDR также позволяет выделить только часть большого блока адресов (например, класса A). CIDR не распознает классы IP-адресов, определяемые старшими битами адреса; вместо этого используются сетевые идентификаторы переменной длины наподобие масок подсетей. Дополнительную информацию о масках подсетей вы найдете в разделе «Разделение сети: подсети и маски подсетей» ниже в этой главе.

Адреса класса D

Класс D используется для широковещательных сообщений. Как говорилось в главе 2, широковещательные сообщения используются для отправки информации определенной группе узлов. Эти узлы включаются в группы после того, как они зарегистрируют себя на локальном маршрутизаторе, используя широковещательный адрес — один из адресов класса D. Старшие биты адреса класса D всегда установлены в 1110 (единица-единица-единица-ноль); оставшиеся биты используются для обозначения логической группы узлов.

Адреса класса E

Класс E — экспериментальный класс адресов, зарезервированный для будущего использования. Адреса в этом классе определяются четырьмя старшими битами, установленными в 1111 (единица-единица-единица-единица).

Советы по IP-адресации

Чтобы соединить вашу сеть с Интернетом, вы должны получить сетевой идентификатор и соответствующий блок IP-адресов от InterNIC. Вы не можете выбрать произвольный идентификатор сети. Ваш сете-

вой идентификатор будет основан на классе адресов, необходимом для поддержки того количества узлов, которое есть в вашей сети. Однако, если вы настраиваете закрытую TCP/IP-сеть или интрасеть, вы должны при определении того, какой класс адресов использовать, следовать приведенным ниже советам. Мы предполагаем, что вы не разделяете сеть на подсети. В противном случае вы найдете необходимую информацию в разделе «Разделение сети: подсети и маски подсетей».

Правильная адресация сетей

Прислушайтесь к следующим советам, когда выбираете и назначаете IP-адреса.

- **Планируйте на будущее.** Первое и важнейшее: выбирайте класс, который допускает дальнейший рост вашей сети.
- **Убедитесь в уникальности.** При присвоении сетевого идентификатора интрасети важно помнить о том, что каждая сеть должна иметь свой собственный идентификатор. Другими словами, каждый сегмент вашей сети, подключенный к маршрутизатору, должен иметь отдельный идентификатор сети.
- **Избегайте использования зарезервированных адресов.** Некоторые адреса не могут нормально использоваться в Интернете в качестве IP-адреса. Сетевой адрес класса A 127 зарезервирован для диагностических целей. Он называется локальным адресом (loopback address) и используется для тестирования семейства протоколов TCP/IP на компьютере без отправки информации в сеть. Список зарезервированных адресов может быть найден на Web-узле Internic по адресу http://ds.internic.net.

Кроме того, в сетевых идентификаторах не могут использоваться числа 0 (октет из всех нулей) и 255 (октет из всех единиц). Сетевой идентификатор не может состоять из всех единиц или всех нулей. Все нули в сетевом идентификаторе означают, что узел находится в локальной сети и пакеты для него не будут маршрутизироваться, в то время как использование всех единиц означает, что пакет представляет собой широковещательное сообщение.

Правильная адресация узлов

Когда вы выбираете идентификаторы узлов внутри данной сети, вы просто должны следить за выполнением нескольких правил:

- **Убедитесь в уникальности.** Все идентификаторы узлов в сети или подсети должны быть различны.
- **Избегайте использования зарезервированных адресов.** Числа 0 (все нули в октете) и 255 (все единицы в октете) не могут исполь-

зоваться в идентификаторах узлов. Иначе говоря, идентификатор узла не может состоять из всех нулей или всех единиц. Все нули в идентификаторе узла означают, что пакет предназначен для определенной сети, без указания конкретного узла, в то время как использование всех единиц означает, что пакет представляет собой широковещательное сообщение для всех узлов определенной сети.

- **Будьте методичны.** Идентификаторы узлов могут присваиваться последовательно, вне зависимости от типа компьютера, которому вы присваиваете адрес. Однако вы сэкономите себе массу времени при поиске неисправностей, назначая идентификаторы узлов в соответствии с каким-либо правилом. Например, многие администраторы сетей используют небольшие числа для идентификаторов маршрутизаторов и большие числа для серверов. Остальные числа выделяются рабочим станциям сети (табл. 4.8).

Таблица 4.8. Пример метода назначения идентификаторов узлов в сети

Сетевое устройство	Диапазон адресов
Маршрутизатор	192.168.0.1–192.168.0.5
Рабочая станция	192.168.0.6–192.168.0.245
Сервер	192.168.0.246–192.168.0.254

Разделение сети: подсети и маски подсетей

После того как мы рассмотрели различные классы доступных IP-адресов, вы можете видеть, что все адресное пространство может быть разделено на три большие группы: класс A, класс B и класс C. Однако иногда необходимо дополнительное подразделение блоков адресов на подсети, поскольку блоки адресов, выделенные InterNIC организации, могут не соответствовать топологии существующей сети. Как вы помните, каждый сетевой идентификатор соответствует одному физическому сегменту сети. Если вы получаете адрес класса C, но в вашей сети два различных физических сегмента, вам желательно далее разделить ваш блок адресов класса C.

Прежде чем мы продолжим, остановимся на минуту. Вспомните, что пространство IP-адресов делится на три класса адресов и каждый из этих трех классов поддерживает определенное количество узлов. Количество доступных идентификаторов сети и идентификаторов узла в каждом классе является функцией количества бит, выделенных на образование соответствующего компонента адреса. Например, в адресах класса B два старших бита установлены в 10 (единица-ноль),

что позволяет использовать только 14 бит для идентификатора сети и 16 бит для идентификатора узла. Проверив старшие биты адреса, вы легко можете определить, какая часть адреса составляет идентификатор сети и какая — идентификатор узла.

Однако, если необходимо провести дальнейшее разделение части адресного пространства, выделенной вам InterNIC, понадобится передать часть бит, выделенных исходно для идентификатора узла, идентификатору сети. Но если вы сделаете это, не сможете легко определить длину идентификатора сети по адресу. Для того чтобы облегчить этот процесс, предназначены маски подсетей.

Маски подсетей

Маска подсети — это 32-битный адрес, позволяющий определить, сколько бит в адресах используется для идентификатора сети. Маска сети показывает длину идентификатора сети, используя все единицы в позициях, соответствующих идентификатору сети (табл. 4.9).

Таблица 4.9. Маски подсетей по умолчанию для адресов классов A, B и C

Класс адресов	Десятичное значение маски	Двоичное значение маски
Класс A	255.0.0.0	11111111.00000000.00000000.00000000
Класс B	255.255.0.0	11111111.11111111.00000000.00000000
Класс C	255.255.255.0	11111111.11111111.11111111.00000000

Для адресов класса A маской подсети по умолчанию является 255.0.0.0, поскольку только первый октет таких адресов используется для идентификатора подсети. Аналогично, маска подсети для адресов класса C — 255.255.255.0, поскольку такие адреса используют три первых октета для идентификатора сети.

При инициализации каждый TCP/IP-узел сравнивает свой собственный IP-адрес с заданной маской подсети при помощи процесса, называемого «логическое И» (табл. 4.10), и сохраняет результат. Когда узлу будет нужно определить, предназначен пакет для локальной сети или для удаленной, он сравнит IP-адрес узла-адресата со своей маской подсети, а затем сравнит результат с тем, что было получено при инициализации. Если результаты совпадают, пакет предназначен для локального узла и не маршрутизируется. Если результаты различны, пакет предназначен для узла в другой подсети и передается маршрутизатору. Этот процесс описан более подробно в главе 5, «Адресация подсетей».

Таблица 4.10. Логическое «И»

Двоичная запись	Десятичная запись
IP-адрес	192.168.2.66
11000000.10101000.00000010.01000010	
Маска подсети	255.255.255.0
11111111.11111111.11111111.00000000	
Результат логического «И»	
11000000.10101000.00000010.00000000	

Операция логического «И» выполняется поразрядно. Результат операции над двумя единицами равен единице; результат операции над нулем и любым числом равен нулю.

Если вы решили разделить вашу сеть класса С на две различных подсети, вы должны расширить маску подсети, чтобы она показывала, какие биты были добавлены к идентификатору сети. Для того, чтобы создать две дополнительные подсети в рамках сети класса С, большинство людей используют маску 255.255.255.192. Число 192 в последнем октете означает, что два старших бита этого октета используются для идентификатора сети. В принципе, два добавочных бита позволяют создать четыре различных комбинации, но, поскольку идентификатор сети не может состоять из всех нулей или всех единиц, остаются только две возможности (подсети 64 и 128). Пример для полученной маски подсети приведен в табл. 4.11.

Таблица 4.11. Логическое «И» — еще раз

Двоичная запись	Десятичная запись
IP-адрес	192.168.2.66
11000000.10101000.00000010.01000010	
Маска подсети	255.255.255.192
11111111.11111111.11111111.11000000	
Результат логического «И»	
11000000.10101000.00000010.01000000	

Устранение проблем с IP-адресацией

Две основные проблемы с IP-адресацией — это неверные сетевые идентификаторы для узлов в одной сети и повторяющиеся идентификаторы узлов в сети.

Если узел использует неверный идентификатор сети, информация, которая должна дойти до него, будет отправлена в другую сеть. Эта

проблема может возникнуть при переносе компьютера из одной сети в другую.

Если два узла в одной сети пытаются использовать один и тот же идентификатор узла, могут возникнуть ошибки приема и передачи. Каждый из двух компьютеров может «повиснуть» или начать работать нестабильно. В принципе, такой проблемы не должно быть с компьютерами, использующими Windows NT, поскольку при инициализации отправляют широковещательное сообщение с адресом, который они собираются использовать, и не станут производить инициализацию, если какой-либо из узлов сети сообщит о том, что этот адрес уже используется. Однако не все узлы используют такой метод инициализации.

Вопросы к экзамену

Question 1

By default, the first ___ octet(s) of a Class B address are used to identify the network ID.

- A. 1
- B. 2
- C. 3
- D. 4

Вопрос 1

Количество октетов, используемых по умолчанию в адресах класса B.

- A. 1
- B. 2
- C. 3
- D. 4

Правильный ответ на этот вопрос — B. По умолчанию в адресах класса B используются два первых октета для указания идентификатора сети. В адресах класса A по умолчанию используется первый октет, в адресах класса C по умолчанию используются первые три октета. Хотя вы можете изменять количество битов при помощи изменения масок подсетей, используемых для идентификатора сети, в данном вопросе вас спрашивали про значения по умолчанию. Таким образом, ответы A, C и D неверны.

Question 2

What class would the address 13.245.88.23 fall under?

- ○ A. Class A
- ○ B. Class B
- ○ C. Class C
- ○ D. Class D

Вопрос 2

К какому классу принадлежит адрес 13.245.88.23?

- ○ A. A
- ○ B. B
- ○ C. C
- ○ D. D

Правильный ответ на этот вопрос — A. Как вы помните, класс IP-адреса можно определить по значению первого октета. Адреса класса A имеют значения первого октета от 1 до 126. Адреса класса B соответствуют значениям первого октета от 128 до 191, а класс C расположен в диапазоне 192–223. Класс D зарезервирован для широковещательных сообщений; он использует значения первого октета от 224 до 239. Итак, ответы B, C и D неверны.

Question 3

Which of the following addresses are used for special purposes? (Check all correct answers.)

- ☐ A. 127, when used in the first octet of a Class B address.
- ☐ B. 255, when used in the last octet of a Class C address.
- ☐ C. 0, when used in the first octet of a Class A address.
- ☐ D. 192, when used in the last octet of a Class C address.

Вопрос 3

Какие из следующих адресов являются зарезервированными? (Выберите все правильные ответы.)

- ☐ A. Адреса класса A, со значением первого октета 127.
- ☐ B. Адреса класса C, со значением последнего октета 255.
- ☐ C. Адреса класса A, со значением первого октета 0.
- ☐ D. Адреса класса C, со значением последнего октета 192.

Правильные ответы — A, B и C. Использование значения 127 в первом октете адреса класса A ограничено. Следовательно, ответ «a» верен. Такие адреса зарезервированы для тестирования сетевого адаптера. Аналогично, адрес класса C со значением последнего октета 255 имеет специальное назначение. Такой адрес означает, что пакет является широковещательным сообщением для всех узлов данной сети. Использование 0 в качестве первого октета адреса класса A означает, что это пакет для локального узла и не должен быть отправлен в сеть. Адреса класса C со значением последнего октета 192 не несут никакого специального смысла. Однако, если «192» является последним октетом маски подсети, это означает, что два бита были перенесены из идентификатора узла в идентификатор сети для разделения сети на подсети.

Question 4

What is the decimal value of the octet 11111001?

- A. 224
- B. 225
- C. 248
- D. 249

Вопрос 4

Каково десятичное значение октета 11111001?

- A. 224
- B. 225
- C. 248
- D. 249

Правильный ответ — D. Сложив суммы значений битов в октет, мы получаем десятичное значение октета. Итак, из 11111001 мы получаем 128+64+32+16+8+0+0+1=249. Для того чтобы правильно ответить на этот вопрос, вы должны уметь преобразовывать двоичные числа в десятичный вид. Для этого достаточно запомнить последовательность 128+64+32+16+8+4+2+1 и выбирать из нее слагаемые, соответствующие единицам в октете. Если вы забыли десятичное значение бита в октете, оно может быть определено по формуле 2^{n-1}, где n — номер бита в октете, считая справа налево.

Question 5

What is the binary value of the decimal number 225?

- A. 11100000
- B. 11100001
- C. 11111000
- D. 11111001

Вопрос 5

Каково двоичное значение числа 225?

- A. 11100000
- B. 11100001
- C. 11111000
- D. 11111001

Правильный ответ на этот вопрос — B. Для того чтобы правильно ответить на этот вопрос, вы должны уметь преобразовывать десятичные числа в двоичный вид. Для этого достаточно запомнить последовательность 128+64+32+16+8+4+2+1 и выбирать из нее по очереди *наибольшие слагаемые* так, чтобы сумма не превышала исходного десятичного числа. Для числа в этом вопросе первое слагаемое, которое вы должны выбрать, — 128. Затем выберем следующее слагаемое так, чтобы сумма не превосходила 225. Продолжайте эту операцию слева направо (от больших слагаемых к меньшим), пока не получите исходное число. В данном вопросе вы представите 225 в качестве суммы 128+64+32+0+0+0+0+1. Теперь замените каждое ненулевое слагаемое на 1. У вас получится искомое двоичное число, в данном вопросе 11100001.

Question 6

You have just been promoted to network administrator, and your company is ready to implement TCP/IP on its network. Your company network is composed of two separate networks, containing three Windows NT servers and approximately 35 workstations each. Which of the following address classes would be most appropriate for this size network?

- A. Class A
- B. Class B
- C. Class C
- D. Cannot be determined from the information given.

Вопрос 6

Вы получили должность администратора сети, и ваша компания готова к реализации TCP/IP в сети. Сеть вашей компании состоит из двух отдельных подсетей, каждая из которых содержит три NT-сервера и примерно 35 рабочих станций. Какой из классов адресов лучшим образом подходит для такой сети?

- ○ A. Класс A
- ○ B. Класс B
- ○ C. Класс C
- ○ D. Невозможно определить на основе имеющихся данных.

Правильный ответ на этот вопрос — C. Хотя сеть класса A или класса B, конечно, подойдет вам, но сеть класса C также обеспечит необходимое вам адресное пространство[1]. В то же время компании не понадобится поддерживать несообразно большое адресное пространство.

Question 7

Which of the following are commonly existing addressing problems? (Check all correct answers.)

- ☐ A. The host is configured with an incorrect network ID.
- ☐ B. The host has not been configured to use DNS.
- ☐ C. The host has the same host ID as another host on the same network.
- ☐ D. The host has the same network ID as other hosts on the same network.

Вопрос 7

Какие из следующих предложений описывают часто встречающиеся типичные проблемы с адресацией? (Выберите все правильные ответы.)

- ☐ A. На узле установлен неверный идентификатор сети.
- ☐ B. Узел не настроен на использование DNS.
- ☐ C. Узел использует тот же идентификатор узла, что и другой узел в той же сети.
- ☐ D. Узел использует тот же идентификатор сети, что и другие узлы в той же сети.

[1] Действительно, поскольку у вас имеются две подсети, вы должны выделить как минимум два бита дополнительно на идентификатор сети. Таким образом, на идентификатор узла остается 6 бит, которые позволяют образовать 64 различные комбинации, из которых две зарезервированы (все нули и все единицы). Итак, вы сможете поддерживать в каждой подсети 64-2=62 узла, что вполне достаточно согласно условию вопроса. — *Примеч. перев.*

Правильные ответы на этот вопрос — A и C. Узлы, на которых установлен неверный идентификатор сети, — камень преткновения в мире TCP/IP. Когда компьютер переносится из одной физической сети в другую, важно помнить, что установленный на нем идентификатор сети должен быть изменен. Ответ B неверен, потому что DNS используется не для адресации, а для определения адресов, соответствующих именам узлов. Ответ C верен, поскольку в одной сети не могут существовать два разных узла с одним идентификатором узла. Ответ D неверен, поскольку все узлы в одной сети должны использовать один и тот же идентификатор сети.

Дополнительная информация

Произведите поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевые слова «subnet mask», «address classes», «ANDing» и родственные.

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы можете произвести поиск на компакт-диске, используя ключевые слова «TCP/IP» и «IP Addressing». Полезные материалы о TCP/IP могут быть найдены в томе «Networking Guide» *Resource Kit*.

Адресация подсетей

Термины, необходимые для понимания материала:

- Подсеть
- Маска подсети
- Маска подсети по умолчанию
- Специальная маска подсети
- Операция логического «И»
- Идентификатор сети
- Идентификатор узла
- CIDR

Приемы и знания, которыми вы должны овладеть:

- Определение необходимого для организации количества идентификаторов сети
- Определение необходимого для сети или подсети количества идентификаторов узлов
- Определение подходящей для конкретной ситуации маски подсети
- Определение правильных идентификаторов сетей для данной маски подсети
- Определение соответствующих идентификаторов узлов для каждой сети или подсети

Значительная доля вопросов экзамена Microsoft по TCP/IP посвящена проверке вашего знания подсетей и работы с ними. Вам будет предложено определить подходящую маску подсети для конкретной организации, определить, в какой подсети находится данный узел, а также определить проблемы, связанные с использованием неверных масок подсетей.

Многие считают, что подсети — самая сложная тема экзамена по TCP/IP, и фактически это наименее понятная часть администрирования TCP/IP-сети. Скорее всего, это происходит из-за плохого понимания двоичных чисел и того, как они соответствуют десятичным. Работа с подсетями была бы намного нагляднее, если бы люди могли легко оперировать с большими двоичными числами, не испытывая необходимости в преобразовании их в десятичные. В этой главе мы постарались объяснить связь между IP-адресами в двоичном формате и их эквивалентами в десятичной записи, поскольку это имеет непосредственное отношение к работе с подсетями. Если вы постоянно думаете об IP-адресах как о двоичных числах, даже когда вы смотрите на их десятичную запись, вы на верном пути к тому, чтобы стать профессиональным TCP/IP-администратором.

Адресация подсетей: исследованная и объясненная

Из предыдущих глав вы узнали, что IP-адрес является 32-разрядным двоичным числом, состоящим из четырех октетов (групп по восемь бит). IP-адрес также может быть записан в точечно-десятичном формате (например, 128.13.134.45). IP-адрес делится на два компонента: идентификатор сети и идентификатор узла. Такое разделение IP-адресов помогает маршрутизаторам в передаче пакетов через TCP/IP-сеть, уменьшая сложность таблиц маршрутизации, необходимых для определения пути к конкретному узлу.

Маршрутизаторам между любыми двумя узлами не требуется знать точное расположение узлов в сети. Вместо этого они используют идентификатор сети, входящий в состав IP-адреса, для того, чтобы отправить пакет маршрутизатору, соединенному с соответствующей сетью. Затем этот маршрутизатор самостоятельно определит, какому из узлов локальной сети нужно передать пакет.

По умолчанию граница между идентификатором сети и идентификатором узла располагается между двумя октетами. В табл. 5.1 приведен пример идентификаторов сети и узла по умолчанию для адреса класса B.

Таблица 5.1. Адрес класса B — идентификаторы сети и узла

Класс адреса	IP-адрес	Идентификатор сети	Идентификатор узла
Класс B	130.29.88.7	130.29	88.7

Положение границы по умолчанию между идентификаторами сети и узла соответствует одному из трех классов адресов. Классы используются для разделения всего 32-битового адресного пространства на группы адресов, которые могут поддерживать различное число узлов. В табл. 5.2 приведены классы адресов и количество узлов, которые может поддерживать каждый из классов. InterNIC (Internet Network Information Center, информационный центр Интернета) использует классы для выделения организациям сетевых адресов, соответствующих необходимому количеству идентификаторов узлов. Идентификаторами узлов в выделенном блоке организация может распоряжаться по своему усмотрению.

Таблица 5.2. Классы адресов и соответствующие им идентификаторы сетей и узлов

Класс адреса	Старшие биты	Диапазон десятичных значений первого октета	Доступное количество сетей	Доступное количество узлов
Класс A	0	1–126	126	16 777 214
Класс B	10	128–191	16 384	65 534
Класс C	110	192–223	2 097 152	254

Однако InterNIC выделяет только один идентификатор сети на организацию. Это вполне подходит для небольшой организации, получающей сетевой адрес класса C (что позволяет поддерживать до 254 узлов), если ее сеть состоит из одного сегмента и не планируется в дальнейшем создавать новые сегменты. Однако большинство организаций имеют несколько сетей и собираются создавать дополнительные сети в будущем, следовательно, одного сетевого идентификатора для них недостаточно. Дополнительные сетевые идентификаторы могут быть получены при помощи разделения выделенного адресного пространства.

Что такое подсеть?

Прежде чем пытаться воспринять понятие подсети, важно понять, что каждая организация, подключенная к Интернету, обычно определяется одним идентификатором сети, выделенным ей InterNIC. Этот

идентификатор сети не может быть изменен никаким образом. Однако вы можете использовать идентификаторы узлов в выделенном блоке так, как хотите. В частности, вы можете использовать некоторые из идентификаторов узлов для разделения вашей сети на подсети.

Подсеть — это сеть или идентификатор сети, созданный при помощи переноса нескольких бит из части IP-адреса, содержащей идентификатор узла, в часть, содержащую идентификатор сети. Если ваша сеть состоит из четырех физических сегментов, соединенных маршрутизаторами, вам потребуются дополнительные сетевые идентификаторы для правильной маршрутизации информации между этими сегментами. Вы можете получить их, изменив маску подсети по умолчанию (подробно описанную в следующем разделе) так, чтобы идентификатор сети содержал дополнительные биты за счет идентификатора узла.

Если ваша организация не подключена к Интернету, вам не потребуется разбивать данный класс адресов на подсети, поскольку вы можете использовать все адресное пространство TCP/IP. Это означает, что вы можете использовать так много идентификаторов сетей по умолчанию, как захотите. Точно так же вы можете поступать, если ваша сеть соединена с Интернетом через прокси-сервер или брандмауэр. Эти устройства скрывают внутреннюю структуру сети, обслуживая все запросы информации через один IP-адрес. Другими словами, каждый пакет, покидающий сеть, воспринимается как пришедший непосредственно с прокси-сервера, а не с узла, который его отправил. Прокси-сервер сам заботится о распределении полученной информации нужным узлам.

Маски подсетей по умолчанию

В главе 4, «IP-адресация», мы ввели понятия маски подсети. Маска подсети — это 32-разрядное двоичное число, которое позволяет определить, какая часть TCP/IP-адреса обозначает идентификатор сети, а какая — идентификатор узла. Каждый бит, установленный в маске в 0, соответствует биту в IP-адресе, относящемуся к идентификатору узла.

По умолчанию каждый адрес имеет предопределенное количество бит, выделенных на идентификатор сети и идентификатор узла. Адрес класса B использует первые 16 бит для идентификатора сети и имеет маску по умолчанию 255.255.0.0, в то время как адрес класса C использует первые 24 бита для идентификатора сети, и его маска по умолчанию — 255.255.255.0. В табл. 5.3 показаны маски сетей по умолчанию для классов адресов от A до C.

Таблица 5.3. Маски подсетей по умолчанию для адресов классов A, B и C

Класс адресов	Десятичное значение маски	Двоичное значение маски
Класс A	255.0.0.0	11111111.00000000.00000000.00000000
Класс B	255.255.0.0	11111111.11111111.00000000.00000000
Класс C	255.255.255.0	11111111.11111111.11111111.00000000

Как упоминалось выше, InterNIC выделяет один идентификатор сети на всю сеть вашей организации. Если сеть требует более одного идентификатора, вы можете расширить маску сети по умолчанию, включив в идентификатор сети дополнительные биты из идентификатора узла. Это позволяет создать дополнительные идентификаторы сетей.

Например, предположим, что вы работаете в компании, которая имеет три физические сети. Вы получили идентификатор сети класса C — 192.168.24.0. Вы должны создать как минимум три идентификатора сети в выделенном вам адресном пространстве для поддержки существующей топологии сети. Вы можете сделать это, расширив маску по умолчанию (255.255.255.0) и включив три бита из идентификатора узла в идентификатор сети, получив в результате маску 255.255.255.224. Эти три бита позволят вам создать шесть идентификаторов сетей, поскольку из трех битов могут быть получены шесть (2^3–2) допустимых комбинаций: 001, 010, 011, 100, 101, 110. Как вы помните, идентификатор сети не может состоять из всех нулей или всех единиц, следовательно, вы не можете использовать комбинации 000 и 111. На рис. 5.1 и 5.2 показаны результаты расширения маски сети. Не беспокойтесь, если вы не поняли этот пример до конца — оставшаяся часть главы прояснит то, что непонятно.

		Идентификатор			
		сети			узла
IP-адрес	192.168.24.65	11000000	10101000	00011000	01000001
Маска подсети по умолчанию	255.255.255.0	11111111	11111111	11111111	00000000

Рис. 5.1. До расширения маски сети по умолчанию

После того как вы расширили маску сети и включили в идентификатор сети три дополнительных бита, вы можете создать дополнительные идентификаторы подсетей. В нашем случае узел 192.168.24.65 из шестьдесят пятого узла сети 192.168.24.0 превращается в первый узел подсети 192.168.24.64, поскольку три бита, перенесенные в иден-

		Идентификатор		
		сети	подсети	узла
IP-адрес	192.168.24.65	11000000 10101000 00011000	010	00001
Маска подсети по умолчанию	255.255.255.224	11111111 11111111 11111111	111	00000

Рис. 5.2. *После расширения маски сети по умолчанию*

тификатор сети, приводят к появлению подсетей 192.168.24(.32), (.64), (.96), (.128), (.160) и (.192). В табл. 5.4 перечислены первые IP-адреса каждой из созданных сетей.

Таблица 5.4. *Адрес первого узла каждой новой подсети*

IP-адрес	Идентификатор сети	Идентификатор узла
192.168.24.33	11000000.1010000.00011000.0010 (32)	0001
192.168.24.65	11000000.1010000.00011000.0100 (64)	0001
192.168.24.97	11000000.1010000.00011000.0110 (96)	0001
192.168.24.129	11000000.1010000.00011000.1000 (128)	0001
192.168.24.161	11000000.1010000.00011000.1010 (160)	0001
192.168.24.193	11000000.1010000.00011000.1100 (192)	0001

Конечно, появление дополнительных идентификаторов сетей приводит к потере доступных идентификаторов узлов. Используя применяемую в нашем примере маску подсети 255.255.255.224, вы имеете 30 узлов в каждой подсети (или 180 узлов во всей сети) вместо 254 узлов, использование которых позволяет маска подсети по умолчанию. Чтобы найти количество корректных идентификаторов узлов после создания подсетей, используйте формулу 2^n-2, где n обозначает номер самой левой цифры октета, не вошедшей в маску подсети. В нашем примере это $2^5-2=30$.

После того как правильная маска сети была определена и установлена, TCP/IP-узел использует ее значение для того, чтобы определить, предназначен пакет для локальной сети или для удаленной, применяя операцию, называемую логическим «И».

Как работает логическое «И»

При инициализации TCP/IP-узла он использует логическое «И» для сравнения своего IP-адреса с маской подсети и сохраняет результат в памяти. Логическое «И» — это математическая операция, вы-

полняемая над двоичными числами. Каждый из 32 битов IP-адреса сравнивается с соответствующим битом маски подсети. Результат сравнения двух битов равен 1, если оба бита равны 1, и 0 в противном случае. Эта операция позволяет TCP/IP-узлу определить свой собственный идентификатор сети. Пример этой операции приведен в табл. 5.5 (используется маска подсети из разобранного выше примера).

Таблица 5.5. Логическое «И»

	IP — десятичное значение	**Идентификатор сети — двоичное значение**	**Идентификатор узла — двоичное значение**
IP-адрес исходного узла	192.168.2.65	11000000.10101000. 00000010.010	00001
Маска подсети	255.255.255.224	11111111.11111111. 11111111.111	00000
Результат исходной операции логического «И»	192.168.2.64	11000000.10101000. 00000010.010	00000
IP-адрес локального узла	192.168.2.91	11000000.10101000. 00000010.010	11011
Маска подсети	255.255.255.224	11111111.11111111. 11111111.111	00000
Результат второй операции логического «И»	192.168.2.64	11000000.10101000. 00000010.010	00000
IP-адрес удаленного узла	192.168.2.97	11000000.10101000. 00000010.011	00001
Маска подсети	255.255.255.224	11111111.11111111. 11111111.111	00000
Результат третей операции логического «И»	192.168.2.96	11000000.10101000. 00000010.011	00000

В табл 5.5 используется маска подсети из 27 бит, и при помощи исходной операции логического «И» узел определяет, что его сетевой идентификатор — 192.168.24.64. Это число сохраняется в памяти для того, чтобы определять, следует отправлять пакет на маршрутизатор или он предназначен для локальной сети.

Как только данный узел должен отправить информацию другому узлу, он производит операцию логического «И» над маской подсети

и IP-адресом узла-адресата, сравнивая полученный результат со своим собственным идентификатором сети, полученным при инициализации. Если эти два числа совпадают, то узел-адресат находится в той же подсети, что и данный узел, и информация может быть отправлена ему непосредственно (см. результат второго «И» в табл. 5.5). Если эти два числа различны, то узел-адресат находится в другой подсети и информация пересылается локальному маршрутизатору для отправки в нужную подсеть (см. результат третьего «И» в табл. 5.5).

Реализация архитектуры подсетей

Теперь, когда компоненты и процессы, связанные с разбиением сети на подсети, вам ясны, пришло время применить знания на практике. Оставшаяся часть этой главы посвящена обсуждению преимуществ создания подсетей на базе данного идентификатора сети, описанию шагов по правильной оценке необходимого количества и размера подсетей и описанию процесса правильной реализации подсетей после того, как они были спланированы.

Преимущества подсетей

Разбиение на подсети имеет множество преимуществ. Разделение позволяет использовать различные методы для связи узлов. Например, маршрутизатор может соединять сеть на основе Ethernet и сеть на основе Token Ring. Разбиение на подсети также позволяет преодолеть физические ограничения на мощность сети. Одна сеть на основе Ethernet может поддерживать ограниченное количество узлов. Применяя подсети, вы сможете включить в сеть в целом большее количество узлов. Такая архитектура также увеличивает эффективность каждого отдельного сегмента, снижая в нем широковещательный трафик. И наконец, концепция подсетей позволяет взаимодействовать физически различным сетям, например глобальным сетям.

Ниже приведены пять основных шагов, которые вы должны выполнить при правильном разделении сети на подсети.

1. Определите общее требуемое количество идентификаторов сетей. Не забудьте подумать о дальнейшем развитии сети.
2. Определите общее количество идентификаторов узлов, которое должна поддерживать каждая подсеть. Опять же, не забудьте, что в дальнейшем к сети могут оказаться подключены новые узлы.
3. Определите маску подсети, которая позволит поддерживать необходимые количества идентификаторов сетей и узлов в подсети.
4. Определите, какие идентификаторы сетей будут использоваться.
5. Назначьте идентификаторы узлам в подсетях.

Необходимое количество идентификаторов сетей

Первым шагом в разделении сети на подсети является определение необходимого количества идентификаторов сетей. Как вы помните, вы должны назначить свой идентификатор сети каждому сегменту, подключенному к маршрутизатору. На рис. 5.3 изображен пример конфигурации сети и показаны сегменты, требующие отдельных идентификаторов сетей.

Вы можете видеть, что на рис. 5.3 имеются четыре различные сети, входящие в состав организации, и одна внешняя сеть, обеспечивающая доступ в Интернет. Каждый локальный сетевой сегмент требует уникального идентификатора сети, так же как и сегмент, соединяющий сеть организации с Интернетом. Однако вы не должны самостоятельно создавать идентификатор сети для сегмента снаружи вашего шлюза по умолчанию (подключенного к Интернету). Этот идентификатор сети назначается InterNIC и не должен повторяться нигде во всей Сети. Кроме того, этот сегмент обычно управляется вашим провайдером Интернета, который и отвечает за организацию в нем правильной адресации. Как вы помните, нужно создать логическое разбиение выделенного вам адресного пространства, соответствующее физическим сегментам сети. Предположим, что вы хотите использовать одну маску подсети для всей организации и не хотите изменять ее в дальнейшем. При этом очень важно произвести планирование с расчетом на расширение сети в дальнейшем. На рис. 5.3 показаны четыре подсети в составе сети организации. В такой ситуации вы должны производить планирование исходя из того, что в дальнейшем будет добавлено от четырех до восьми подсетей в зависимости от ожидаемого роста организации.

Необходимое количество идентификаторов узлов

После того как вы определили необходимое количество отдельных идентификаторов подсетей, вы должны определить, какое количество идентификаторов узлов потребуется в каждой подсети. Идентификатор узла требуется для каждой сетевой карты внутри данного сегмента — для рабочих станций или серверов, настроенных на использование TCP/IP-сети, для принтеров, непосредственно подключенных к сети, и для каждого подключенного к данному сегменту интерфейса маршрутизатора. Некоторые маршрутизаторы, например основанные на Windows NT Server или Workstation, требуют только двух идентификаторов узла; однако большинство промышленных маршрутизаторов требуют от 8 до 24 идентификаторов узла. Запомните, что каждый интерфейс маршрутизатора требует отдельного идентификатора узла. На рис. 5.4 показан пример конфигурации сети и различные устройства, требующие отдельных идентификаторов узла.

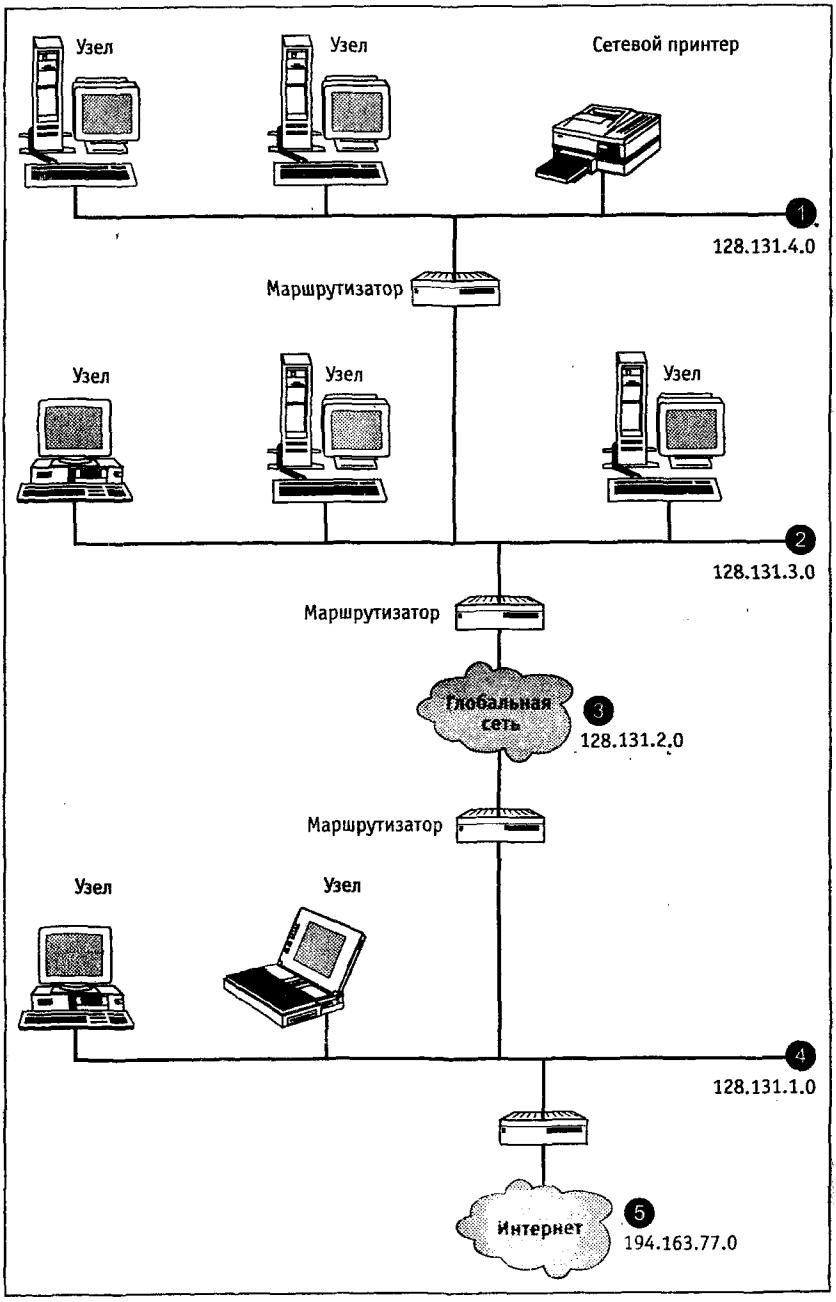


Рис. 5.3. Пример сети, требующей пять идентификаторов сети

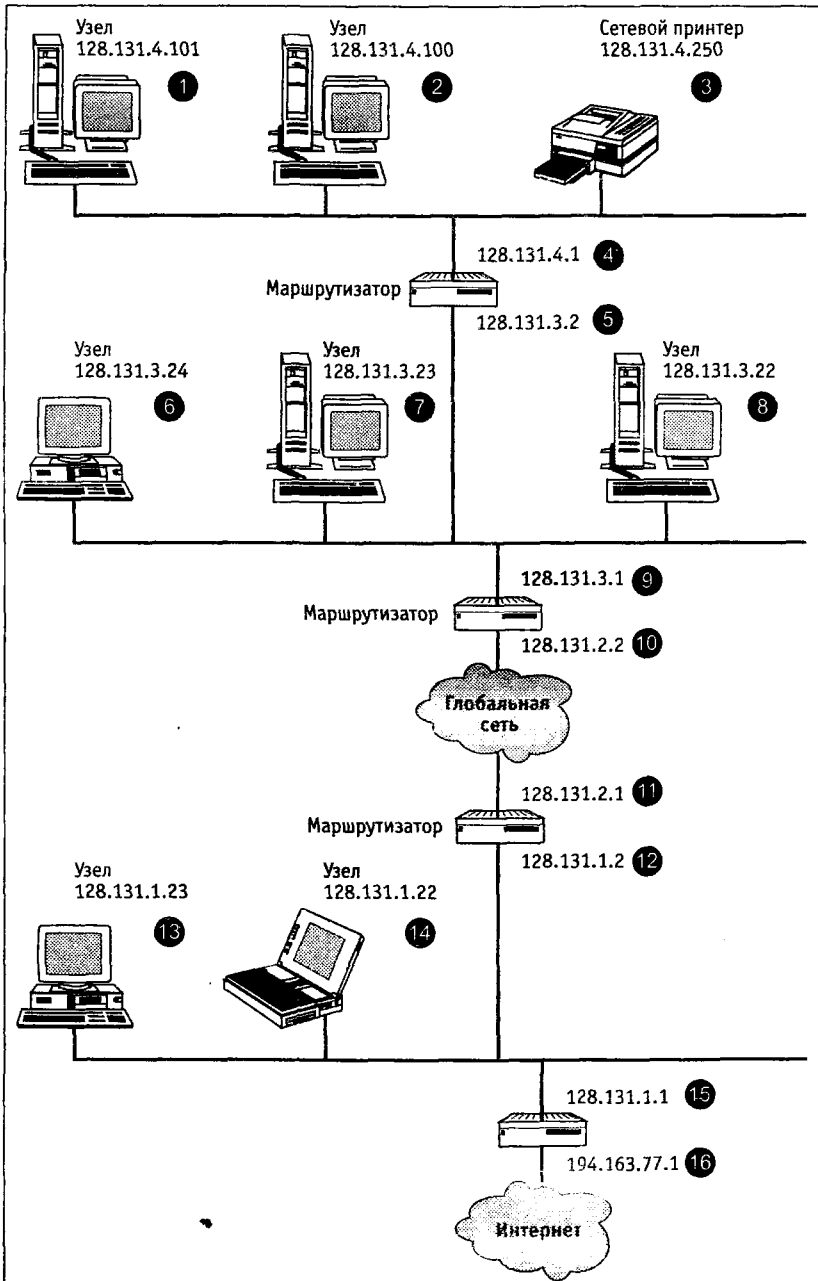


Рис. 5.4 Пример сети, требующей 16 идентификаторов узлов

При определении правильного числа идентификаторов узла, требующегося для подсети, вы должны рассчитывать на дальнейшее развитие сети. Если ваша самая большая подсеть требует 35 идентификаторов узлов, вы должны рассчитывать на величину порядка 60 узлов в будущем. Выбирайте маску подсети так, чтобы она поддерживала такую конфигурацию и не понадобилось бы ее изменять в будущем. Только представьте себе трудности, которые возникнут при перенастройке каждой рабочей станции и каждого маршрутизатора при изменении маски подсети.

Определение маски подсети

После того как вы определили требуемые количества идентификаторов сетей и узлов, вы должны определить маску подсети, которая позволит вам выполнить эти требования. Определение маски подсети иногда похоже на балансирование на канате. Вы должны перенести достаточное количество бит из идентификатора узла в идентификатор сети, чтобы иметь возможность создать необходимое количество идентификаторов сети, но при этом вы не можете перенести слишком много бит, иначе не сможете поддерживать нужное количество узлов.

Давайте предположим, что ваша компания получила идентификатор сети класса С 192.169.220.0. Этот идентификатор сети позволяет поддерживать до 254 узлов в одной сети. Однако ваша компания уже имеет шесть сетей, в самой большой из которых девять узлов. Ваша цель — определить маску подсети, которая поддерживала бы существующую конфигурацию вашей сети и допускала бы ее дальнейшее развитие.

Поскольку для сети класса С может быть использовано только ограниченное количество масок подсетей, может оказаться полезным просмотреть их все. В табл. 5.6 приведены количества идентификаторов сетей, обеспечиваемых различными масками подсетей, и количества поддерживаемых этими подсетями узлов.

Таблица 5.6. Возможные маски подсетей для адреса класса С

Маска подсети	Количество подсетей	Количество узлов в подсети	Общее количество узлов
255.255.255.192	2	62	124
255.255.255.224	6	30	180
255.255.255.240	14	14	196
255.255.255.248	30	6	180
255.255.255.252	62	2	124
255.255.255.254	126	—	—
255.255.255.255	254	—	—

В табл. 5.6 не включена маска подсети по умолчанию для сети класса C (255.255.255.0), поскольку она предоставляет только один идентификатор сети. В таблице также отсутствует маска .128, поскольку она обеспечивает только один дополнительный бит для идентификатора сети, а идентификатор сети не может состоять ни из всех нулей, ни из всех единиц. Кроме того, маски .254 и .255 позволяют создать множество идентификаторов сетей но в получающихся подсетях не может быть ни одного узла. Следовательно, у вас есть только пять масок, из которых вы можете выбирать.

Ваша компания уже имеет шесть сетей, которые вы должны поддерживать, поэтому вы не можете выбрать маску 255.255.255.192. Ближайшая маска 255.255.255.224 позволяет создать шесть подсетей по 30 узлов в каждой. Однако при выборе маски вы должны позаботиться о возможности дальнейшего расширения, а маска 225.225.255.224 не позволит вам в дальнейшем добавить еще одну сеть. Следовательно, будет лучше выбрать маску 255.255.255.240. Эта маска передает четыре бита из идентификатора узла в идентификатор сети и позволяет создать в сети 14 подсетей. Оставшиеся четыре бита позволяют поддерживать до 14 узлов в каждой подсети.

Маска подсети 255.255.255.240 будет лучшим выбором в рассматриваемом случае. Она позволит в будущем довести число подсетей до 14 и добавить даже в самую большую из существующих подсетей пять узлов. Теперь, после того как вы увидели связь между максимальным количеством подсетей и максимальным количеством узлов в подсети, давайте перейдем к обсуждению того, как маска подсети может быть определена без использования соответствующей таблицы.

Вычисление подходящей маски подсети вручную

Первый шаг в вычислении маски подсети — определение необходимого на текущий момент количества подсетей. После того как это число определено, вам следует понять, сколько бит должно быть передано идентификатору сети для того, чтобы вы могли создать нужное число подсетей. Например, если ваша сеть состоит из шести сегментов, наименьшее необходимое число подсетей равняется шести. Двоичная запись числа 6 — 110 (единица-единица-ноль), следовательно, вам потребуются минимум три дополнительных бита в идентификаторе сети, чтобы создать шесть подсетей[1].

---

[1] Это правило не всегда работает. Например, двоичная запись числа 7 — 111 (единица-единица-единица), но для создания семи подсетей вам потребуются четыре дополнительных бита. Правильно будет рассматривать двоичную запись числа **подсетей**, увеличенного на единицу. — *Примеч. перев.*

Такая маска подсети позволит вам выполнить текущие требования, но не позволит в дальнейшем добавить новые подсети. Если вы используете не три, а четыре дополнительных бита для идентификаторов сетей, вы сможете создать до $2^4-2=14$ подсетей. Запомните, вы должны вычесть две из шестнадцати возможных комбинаций, поскольку идентификатор сети не может состоять из всех единиц или всех нулей.

Последний шаг в ручном вычислении маски сети — определить, достаточно ли оставшихся бит адреса для поддержки того числа узлов, которое содержится в ваших подсетях. В нашем примере осталось четыре бита, что позволяет поддерживать до 14 узлов в каждой подсети. Поскольку в самой большой из ваших подсетей только девять узлов, эта маска вам вполне подходит и допускает дальнейший рост сети.

Выбор используемых идентификаторов сетей

После того как вы определили маску подсети, которая удовлетворяет вашим требованиям, вы должны решить, какие именно идентификаторы сетей вы будете использовать. Важно понимать, что после разделения на подсети многие корректные ранее IP-адреса становятся недопустимыми. Если вы используете эти адреса в вашей сети, появятся коммуникационные ошибки.

Первый шаг в определении идентификаторов сетей, которые вы будете использовать, состоит в том, чтобы выписать все возможные комбинации дополнительных битов. Маска подсети 255.255.255.240 означает, что в идентификатор сети добавлено четыре дополнительных бита. Их возможные комбинации перечислены в табл. 5.7.

Таблица 5.7. Все возможные комбинации, образуемые четырьмя битами

0–1	2–3	4–5	6–7	8–9	10–11	12–13	14–15
0000	0010	0100	0110	1000	1010	1100	1110
0001	0011	0101	0111	1001	1011	1101	1111

Второй шаг состоит в том, что вы должны отбросить комбинации, состоящие из всех нулей и всех единиц. Возможно, вам будет легче запомнить, что первый и последний идентификаторы сети нельзя использовать. После того как вы удалите неразрешенные комбинации, у вас останутся двоичные числа, соответствующие значениям от 1 до 14.

На третьем шаге вы должны добавить к полученным идентификатором сетей четыре бита для идентификаторов узлов и преобразовать полученные числа в десятичный вид (табл. 5.8).

Четвертый шаг самый простой — просто припишите полученные десятичные значения к маске подсети по умолчанию для используемо-

го класса адресов, и — ура! вы получили значение масок для созданных вами подсетей.

Таблица 5.8. Приписывание четырех бит для идентификатора узла

Двоичный номер подсети	Десятичный номер подсети	Маска подсети (десятичное значение)
0001 0000	.16	255.255.255.240
0010 0000	.32	255.255.255.240
0011 0000	.48	255.255.255.240
0100 0000	.64	255.255.255.240
0101 0000	.80	255.255.255.240
0110 0000	.96	255.255.255.240
0111 0000	.112	255.255.255.240
1000 0000	.128	255.255.255.240
1001 0000	.144	255.255.255.240
1010 0000	.160	255.255.255.240
1011 0000	.176	255.255.255.240
1100 0000	.192	255.255.255.240
1101 0000	.208	255.255.255.240
1110 0000	.224	255.255.255.240

Поскольку вычисление всех масок подсетей достаточно утомительно, многие администраторы сетей упрощают этот процесс. Они вычисляют наименьшее значение, которое может быть составлено из бит, выделенных на идентификатор сети, и затем складывают это значение само с собой. Сделав это столько раз, сколько имеется разрешенных двоичных комбинаций, вы получите идентификаторы всех подсетей в сети со значительно меньшими усилиями.

Используя предыдущий пример, вычислим десятичное значение наименьшей комбинации. В нашем случае это будет 0001, с приписанными четырьмя нулями (соответствующими битам идентификатора узла) — 00010000, или 16. Используя это *приращение*, найдем все остальные значения. Первая подсеть имеет номер .16, далее, складывая 16 само с собой, найдем номер следующей подсети — .32, потом .48 и т. д. Этот метод может сберечь массу времени, когда вам нужно создать в сети много подсетей. Также существуют различные таблицы, которые помогут вам провести разделение сети на подсети; однако вы не можете использовать такие таблицы на экзамене Microsoft.

Определение используемых идентификаторов узлов

Последним шагом в разбиении сети на подсети является определение корректных идентификаторов узлов для каждой из созданных вами

подсетей. Начните с рассмотрения первого идентификатора узла в каждой подсети.

Первый идентификатор узла в подсети всегда равен 1. Для примера из предыдущего раздела первое значение, которое вы можете составить из оставшихся бит, — 0001. Добавьте это значение к идентификатору первой подсети (который равен 16), и вы получите 0001 0000 + 0000 0001 = 0001 0001, что в десятичной записи — 17. Поскольку при помощи четырех бит можно образовать только 14 корректных идентификаторов узлов, далее вы должны последовательно увеличивать полученное число на 1, пока значение идентификатора узла не дойдет до 14. Далее, поскольку идентификатор узла не может состоять из всех единиц, значение 1111 (в десятичной записи 15) недопустимо. В табл. 5.9 приведены все корректные идентификаторы для подсети .16 из предыдущего примера. Вы можете повторить показанный процесс для каждой подсети.

Таблица 5.9. Построение идентификаторов узлов в данной подсети

Идентификатор подсети	Идентификатор узла	Десятичный IP-адрес
0001 0000 (16)	0000 0001 (1)	w.x.y.17
0001 0000 (16)	0000 0010 (2)	w.x.y.18
0001 0000 (16)	0000 0011 (3)	w.x.y.19
0001 0000 (16)	0000 0100 (4)	w.x.y.20
0001 0000 (16)	0000 0101 (5)	w.x.y.21
0001 0000 (16)	0000 0110 (6)	w.x.y.22
0001 0000 (16)	0000 0111 (7)	w.x.y.23
0001 0000 (16)	0000 1000 (8)	w.x.y.24
0001 0000 (16)	0000 1001 (9)	w.x.y.25
0001 0000 (16)	0000 1010 (10)	w.x.y.26
0001 0000 (16)	0000 1011 (11)	w.x.y.27
0001 0000 (16)	0000 1100 (12)	w.x.y.28
0001 0000 (16)	0000 1101 (13)	w.x.y.29
0001 0000 (16)	0000 1110 (14)	w.x.y.30

CIDR: бесклассовая междоменная маршрутизация

Как было отмечено в главе 4, CIDR (Classless Inter-Domain Routing, бесклассовая междоменная маршрутизация) используется для снижения объема таблиц маршрутизации на основных маршрутизаторах Интернета. Эти маршрутизаторы поддерживают записи для каждого идентификатора сети, выделенного InterNIC. Вообще говоря, каждая такая запись соответствует отдельной организации. Однако, когда

InterNIC выделяет одной организации несколько идентификаторов сетей, это вносит ненужную сложность в таблицы маршрутизации и увеличивает их размер.

Если одна организация имеет три сетевых идентификатора класса C, потребуются три записи в таблицах маршрутизации, чтобы информация для этой организации правильно маршрутизировалась. CIDR позволяет объединить несколько маршрутов к организации; эти маршруты создаются при помощи объединения сетевых идентификаторов методом, противоположным разделению на подсети. CIDR поддерживает в некотором роде надсети. Вместо увеличения количества бит в маске оно уменьшается.

Ранее это было невозможно, поскольку каждый класс адресов имел фиксированную маску по умолчанию. Если количество бит в маске будет меньше, чем в маске по умолчанию, это приведет к тому, что границы класса адресов перестанут существовать, следовательно, нужно использовать «бесклассовую» маршрутизацию. CIDR также позволяет выделить только часть адресов, соответствующих идентификатору сети, определенной организации. Например, только часть адресов сети класса B может быть присвоена организации, а оставшаяся часть может быть выдана кому-либо еще. CIDR работает только в непрерывном адресном пространстве.

Чтобы понять, как это действует, предположим, что вашей организации выделены сетевые идентификаторы 192.169.220.0, 192.169.221.0 и 192.169.222.0. Если вы рассмотрите эти адреса в двоичном виде, то увидите, что они отличаются только в двух последних битах третьего октета. Следовательно, уменьшив маску сети по умолчанию на два бита, вы сможете эффективно сгруппировать эти три идентификатора сетей (табл. 5.10).

Таблица 5.10. Использование CIDR для объединения в группы адресов класса C

	Десятичное значение	**Двоичное значение**
Идентификатор сети	192.169.220.0	11000000.10101001.110111–00.00000000
Идентификатор сети	192.169.221.0	11000000.10101001.110111–01.00000000
Идентификатор сети	192.169.222.0	11000000.10101001.110111–10.00000000
Новая маска подсети	255.255.252.0	11000000.10101001.110111–00.00000000
Результат логического «И»	192.169.220.0	11000000.10101001.110111–00.00000000

Как вы понимаете, результат логического «И» полученной маски с любым IP-адресом, который попадает в одну из этих трех сетей, образует идентификатор сети 192.169.220.0. Следовательно, вы можете уменьшить количество записей в таблице маршрутизации с трех до одной. Однако CIDR работает не со всеми маршрутизаторами, поэтому, прежде чем вы начнете реализацию CIDR в вашей сети, проверьте, что ваши маршрутизаторы поддерживают ее.

Вопросы для подготовки к экзамену

Question 1

Choose from the following options the answer that best describes the purpose of a subnet mask.

- A. The subnet mask is used to mask a portion of an IP address for TCP/IP.
- B. The subnet mask aids in determining the location of other TCP/IP hosts.
- C. The subnet mask is used to help TCP/IP distinguish the network ID from the host ID. This aids in determining the location of other TCP/IP hosts.
- D. The subnet mask is used to help TCP/IP distinguish the network ID from the host ID. This aids in determining the IP address of other hosts.

Вопрос 1

Выберите ответ, который наилучшим образом описывает функции маски подсети.

- A. Маска сети используется для маскирования части IP-адреса в TCP/IP-сети.
- B. Маска подсети позволяет определить расположение других TCP/IP-узлов.
- C. Маска подсети используется для того, чтобы помочь TCP/IP отделить идентификатор сети от идентификатора узла. Это помогает в определении положения других TCP/IP-узлов.
- D. Маска подсети используется для того, чтобы помочь TCP/IP отделить идентификатор сети от идентификатора узла. Это помогает в определении IP-адресов других TCP/IP-узлов.

Наилучший ответ на этот вопрос — C. Маска подсети используется TCP/IP-узлом при инициализации для определения собственного идентификатора сети. Затем полученная информация используется для определения расположения узла-адресата — находится он в локальной сети или нет. Ответ A частично верен, но не является лучшим ответом, поскольку не содержит достаточно информации. Ответ B не подходит по той же причине. Ответ D неверен, поскольку

ку маска подсети не помогает определить IP-адрес другого узла. IP-адрес удаленного узла должен быть уже известен, чтобы можно было применить маску подсети.

Question 2

Which of the following options is the default subnet mask for a Class B network ID?

- ○ A. 255.0.0.0
- ○ B. 255.255.0.0
- ○ C. 255.255.255.0
- ○ D. 255.255.255.255

Вопрос 2

Какова маска подсети по умолчанию для идентификатора сети класса B?

- ○ A. 255.0.0.0
- ○ B. 255.255.0.0
- ○ C. 255.255.255.0
- ○ D. 255.255.255.255

Правильный ответ на этот вопрос — B. Запомните, что маска подсети по умолчанию для какого-либо класса адресов соответствует количеству октетов, используемому адресами этого класса для идентификаторов сети. Адреса класса B используют первые два октета IP-адреса для идентификатора сети. Следовательно, в маске по умолчанию первые два октета должны быть заполнены единицами (что означает 255 в десятичной записи), чтобы показать, что идентификатор сети занимает два первых октета. В ответе A приведена маска по умолчанию для адреса класса A. Ответ C содержит маску подсети для адреса класса C, а ответ D — широковещательный адрес.

Question 3

Which of the following are benefits of subnetting a given network ID? (Check all correct answers.)

- ☐ A. Subnetting allows for the interconnection of networks that use different network technologies.
- ☐ B. Subnetting allows you to overcome the physical limitations of a network's capacity.
- ☐ C. Subnetting allows for the arbitrary allocation of IP addresses, regardless of host location.
- ☐ D. Subnetting allows you for an effective increase in network bandwidth, by cutting down on the amount of broadcasts a network must process.

Вопрос 3

Каковы преимущества разделения идентификатора сети на подсети? (Выберите все правильные ответы.)

- ❑ A. Разделение на подсети позволяет взаимодействовать сетям, использующим разные сетевые технологии.
- ❑ B. Разделение на подсети позволяет преодолеть физические ограничения на размер сети.
- ❑ C. Разделение на подсети позволяет произвольно назначать IP-адреса, вне зависимости от расположения узла.
- ❑ D. Разделение на подсети позволяет эффективно увеличить пропускную способность сети, снижая объем широковещательного трафика.

Правильные ответы на этот вопрос — A, B и D. Поскольку маршрутизаторы обычно могут передавать информацию между сетями на основе Ethernet и сетями на основе Token Ring, разделение на подсети позволяет узлам, использующим разные сетевые технологии, взаимодействовать друг с другом. Разделение на подсети также позволяет вам преодолеть присущие некоторым сетевым технологиям, таким как Ethernet, физические ограничения на число поддерживаемых узлов в одном сегменте. Если у вас в сети должно быть больше узлов, чем может содержать один сегмент Ethernet, разделение на подсети поможет вам распределить эти узлы по нескольким сегментам. Наконец, поскольку разделение на подсети физически изолирует каждый сегмент сети от других сегментов, объем широковещательного трафика значительно снижается. Это эффективно увеличивает пропускную способность каждой подсети. Ответ C неверен, поскольку при разделении сети на подсети требуется, чтобы IP-адреса присваивались адресам вполне определенным образом, в соответствии с тем, в какой подсети находится узел.

Question 4

Which of the following does not require a unique host ID?

- ○ A. A Windows NT Workstation enabled to use TCP/IP and IPX/SPX.
- ○ B. A Windows NT Server configured to use NetBEUI only.
- ○ C. A network printer configured to use TCP/IP.
- ○ D. Every interface on a TCP/IP router.

Вопрос 4

В каком случае узлу не нужен уникальный TCP/IP-адрес?

- A. Windows NT Workstation, настроенная на использование TCP/IP и IPX/SPX.
- B. Windows NT Server, настроенный на использование только NetBEUI.
- C. Сетевой принтер, настроенный на использование TCP/IP.
- D. Произвольный интерфейс TCP/IP-маршрутизатора.

Правильный ответ на этот вопрос — B. Каждый узел, настроенный на использование TCP/IP в IP-сети нуждается в уникальном TCP/IP-адресе. Это относится к рабочим станциям, серверам, сетевым принтерам и IP-маршрутизаторам. Вариант из ответа B не требует, чтобы узлу был выделен TCP/IP-адрес, поскольку описываемая машина не настроена на использование TCP/IP.

Question 5

By default, how many hosts will a Class B address support?

- A. 254
- B. 16 384
- C. 65 534
- D. 2 097 152

Вопрос 5

Сколько узлов может по умолчанию поддерживать сеть класса B?

- A. 254
- B. 16 384
- C. 65 534
- D. 2 097 152

Правильный ответ на этот вопрос — C. Формула для вычисления количества допустимых идентификаторов узлов, образованных n битами, имеет вид $2^n - 2$. По умолчанию в сети класса B используется 16 бит для идентификаторов узлов. Следовательно, количество узлов равно $2^{16} - 2 = 65\,534$. Ответ A неверен, поскольку 254 узла поддерживает по умолчанию сеть класса C. Ответ «b» неверен, поскольку 16 384 — это количество идентификаторов сетей, доступное по умолчанию в пространстве адресов класса B. Ответ D неверен, поскольку 2 097 152 является количеством идентификаторов сетей, доступных по умолчанию в пространстве адресов класса C.

Question 6

The host David is configured with the IP address 202.121.74.37 and the subnet mask 255.255.255.224. David needs to send information to the host Goliath, which is configured with the IP address 202.121.74.66 and the subnet mask 255.255. 255.224. Use the ANDing process to determine which of the following options is correct.

- A. Goliath is on the 202.121.74.64 subnet; therefore, David and Goliath are on separate subnets. David will need to forward the information to its default gateway.
- B. Goliath is on the 202.121.74.224 subnet; therefore, David and Goliath are on the same subnets. David will not need to forward the information to its default gateway.
- C. David and Goliath are both using the same subnet mask and are therefore on the same subnets. These two hosts can communicate directly with one another without using the default gateway.
- D. David and Goliath are both using the same subnet mask and are therefore on different subnets. These two hosts must communicate with one another through at least one router.

Вопрос 6

Узел David имеет IP-адрес 202.121.74.37 и маску подсети 255.255.255.224. David должен передать информацию узлу Goliath, который имеет IP-адрес 202.121.74.66 и маску подсети 255.255.255.224. Используйте операцию логического «И», чтобы определить, какой из следующих ответов верен.

- A. Goliath находится в подсети 202.121.74.64; следовательно, David и Goliath находятся в различных подсетях. David должен передать информацию на шлюз по умолчанию.
- B. Goliath находится в подсети 202.121.74.224; следовательно, David и Goliath находятся в одной подсети. David не должен передать информацию на шлюз по умолчанию.
- C. David и Goliath используют одну маску подсети; следовательно, они находятся в одной подсети. Эти два узла могут взаимодействовать непосредственно, не используя шлюз по умолчанию.
- D. David и Goliath используют одну маску подсети; следовательно, они находятся в разных подсетях. Эти два узла при взаимодействии должны использовать как минимум один маршрутизатор.

Правильный ответ на этот вопрос — A. Goliath имеет IP-адрес 202. 121.74.66 и маску подсети 255.255.255.224. Применив операцию логического «И», мы увидим, что Goliath находится в подсети .64. Аналогично убедимся, что David находится в сети .32. Оба узла используют одну маску подсети, но имеют различные идентификаторы сетей. Следовательно, чтобы узлу David отправить информацию на узел Goliath, ему нужно передать ее на шлюз по умолчанию. Ответ B неверен, поскольку 255.255.255.224 не является допустимым номером

подсети. Значение .224 на самом деле является частью маски подсети. Ответ C неверен, поскольку тот факт, что два узла имеют одну маску подсети, не означает, что они оба находятся в одной подсети. Ответ D неверен по той же причине.

Question 7

Shannon is getting ready to subnet his IP network and must determine the number of network IDs required before he can calculate an appropriate subnet mask for his network. Which of the following options would help him properly calculate the number of necessary network IDs? (Check all correct answers.)

- ❑ A. Calculate a unique network ID for each segment of the network bordered by a router.
- ❑ B. Calculate a unique network ID for each interface of a router.
- ❑ C. Calculate a unique network ID for each network printer on a segment.
- ❑ D. Calculate only one unique network ID for network segments bordered by two or more routers.

Вопрос 7

Иван собирается разделить свою IP-сеть на подсети и должен определить требуемое количество подсетей, чтобы правильно рассчитать маску подсети. Что поможет ему определить необходимое количество подсетей? (Укажите все правильные ответы.)

- ❑ A. Подсчет количества сегментов сети, ограниченных одним маршрутизатором.
- ❑ B. Подсчет количества интерфейсов маршрутизаторов.
- ❑ C. Подсчет количества сетевых принтеров в сегменте.
- ❑ D. Подсчет количества сегментов сети, ограниченных двумя или более маршрутизаторами.

Правильный ответ на этот вопрос — A и D. При определении общего количества различных идентификаторов сети вы должны подсчитать все сегменты сети, каждый из которых ограничен как минимум одним маршрутизатором. Замкнутая сеть (без доступа в нее извне) с двумя маршрутизаторами, каждый из которых имеет два интерфейса, нуждается в трех идентификаторах сети. Ответ B неверен, поскольку в приведенном примере с маршрутизаторами нужно только три идентификатора сети, а не четыре. Ответ C неверен потому, что каждый сетевой принтер или узел в сегменте требует свой собственный идентификатор узла, но все они в пределах сегмента имеют один идентификатор сети.

Question 8

You work for the Signature Wiget C company, which has recently been assigned the Class B network ID 128.131.0.0. Your company currently has 45 individual network segments or subnets. You have been told that new offices will be added in Rome, Paris, and Chicago over the next 12 months, and your network will need to support at least 50 new subnets. What subnet mask should you use for you network to support the largest number of hosts per subnet?

- A. 255.255.0.0
- B. 255.255.240.0
- C. 255.255.252.0
- D. 255.255.254.0

Вопрос 8

Вы работаете в компании, которая недавно получила сеть класса B 128.131.0.0. Ваша компания на текущий момент имеет 45 отдельных сегментов. Вы знаете, что в ближайшие 12 месяцев будут созданы новые офисы в Риме, Париже и Чикаго, после чего вам потребуется поддержка как минимум 50 дополнительных подсетей. Какую маску подсети вы должны использовать, чтобы поддерживать максимально возможное количество узлов в одной подсети?

- A. 255.255.0.0
- B. 255.255.240.0
- C. 255.255.252.0
- D. 255.255.254.0

Правильный ответ на этот вопрос — D. Значение .254 в третьем октете маски позволяет поддерживать до 126 подсетей. Это минимальная маска подсети, удовлетворяющая требованиям на количество подсетей, и, следовательно, она обеспечивает поддержку максимально возможного количества узлов в подсети. Маска подсети, указанная в ответе A, является маской по умолчанию для адресов класса B и обеспечивает поддержку только одного идентификатора сети. Маска из ответа D позволяет использовать только 14 отдельных подсетей и не подходит в нашем случае. Маска в ответе C поддерживает 62 подсети. Применение этой маски не позволит провести планируемое расширение компании до 95 подсетей.

Question 9

The Billington Steambath Company currently has nine divisions, and each one requires its own subnet. It has been assigned the network ID 130.121.0.0. Billington anticipates the need to support up to 3,000 hosts in each division. Which subnet would you recommend it use?

- A. 255.255.224.0
- B. 255.255.240.0
- C. 255.255.248.0
- D. 255.255.252.0

Вопрос 9

Великорусская банная компания состоит из девяти подразделений, каждому из которых требуется своя собственная подсеть. Компания получила идентификатор сети 130.121.0.0. Требуется поддержка до 3000 узлов в подразделении. Какую маску подсети вы бы посоветовали использовать?

- A. 255.255.224.0
- B. 255.255.240.0
- C. 255.255.248.0
- D. 255.255.252.0

Правильный ответ на этот вопрос — B. Значение .240 в третьем октете маски позволяет поддерживать до 14 подсетей в сети. Эта маска подсети удовлетворяет требованиям вопроса и допускает дальнейшее развитие сети. Кроме того, при использовании такой маски каждая подсеть может содержать 4094 узла. Такие подсети удовлетворяют требованиям Великорусской банной компании. Ответ A неверен, поскольку такая маска подсети не позволит поддерживать достаточное количество подсетей. Ответы C и D неверны, поскольку приведенные в них маски не позволят поддерживать требуемое количество узлов в подсети.

Question 10

Mary works for a new Internet Service Provider (ISP) that has a customer who has been assigned seven Class C addresses ranging from 223.68.168.0 to 223.68.174.0. Her employer would like for her to limit the number of routing table entries for this customer to one. If the routers at the ISP support CIDR, which of the following subnet masks should Mary use to achieve her objective?

- A. 255.255.224.0
- B. 255.255.240.0
- C. 255.255.248.0
- D. 255.255.254.0

Вопрос 10

Мария работает у нового провайдера Интернета. У этого провайдера есть клиент, который получил семь идентификаторов сетей класса C — от 223.68.168.0 до 223.68.174.0. Наниматель дал Марии задание свести количество записей в таблице маршрутизации для этого клиента до одной. Если маршрутизаторы провайдера поддерживают CIDR, какую из следующих масок подсетей должна использовать Мария?

- A. 255.255.224.0
- B. 255.255.240.0
- C. 255.255.248.0
- D. 255.255.254.0

Правильный ответ на этот вопрос — C. Маска подсети 255.255.248.0 уменьшает маску подсети по умолчанию на наименьшее количество бит, достаточное для того, чтобы свести все выделенные клиенту сети к одному идентификатору сети — 223.68.168.0 (табл. 5.11).

Таблица 5.11. Результаты логического «И», к вопросу 10

	Десятичные значения	Двоичные значения
Идентификатор сети	223.68.168.0	11011111.01000100.10101-000.00000000
Идентификатор сети	223.68.169.0	11011111.01000100.10101-001.00000000
Идентификатор сети	223.68.170.0	11011111.01000100.10101-010.00000000
Идентификатор сети	223.68.171.0	11011111.01000100.10101-011.00000000
Идентификатор сети	223.68.172.0	11011111.01000100.10101-100.00000000
Идентификатор сети	223.68.173.0	11011111.01000100.10101-101.00000000
Идентификатор сети	223.68.174.0	11011111.01000100.10101-110.00000000
Новая маска подсети	255.255.248.0	11111111.11111111.11111-000.00000000
Результат логического «И»	223.68.168.0	11011111.01000100.10101-000.00000000

Результат операции логического «И» любого из этих идентификаторов сети с маской — идентификатор сети 223.68.168.0. Следовательно, Мария может уменьшить количество записей в таблице маршру-

тизации с семи до одной. Ответы «a» и «b» неверны, поскольку они не маскируют достаточное количество битов идентификатора сети. Ответ «d» неверен, поскольку он маскирует слишком много битов в идентификаторе сети.

Дополнительная информация

Произведите поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевые слова «subnet mask», «address classes», «ANDing» и родственные.

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы можете произвести поиск на компакт-диске, используя ключевые слова «TCP/IP» и «IP Addressing». Полезные материалы о TCP/IP могут быть найдены в томе «Networking Guide» *Resource Kit*.

Реализация IP-маршрутизации

Термины, необходимые для понимания материала:

- Маршрутизатор
- Узел
- Удаленный узел
- Система с несколькими сетевыми интерфейсами
- Таблица маршрутизации
- Шлюз
- Аппаратный адрес (HWA)
- Статическая маршрутизация
- Динамическая маршрутизация
- Протокол управления маршрутизацией (RIP)
- Открой кратчайший путь первым (OSPF)
- Многопротокольный маршрутизатор (MPR)

Приемы и знания, которыми вы должны овладеть:

- Понимание маршрутизации Microsoft TCP/IP
- Объяснение разницы между статической и динамической маршрутизацией
- Использование функций и параметров команд ROUTE и TRACERT
- Реализация и настройка систем с несколькими сетевыми интерфейсами

Как вы уже знаете из предыдущих глав, Microsoft не всегда придерживалась при реализации возможностей и функций TCP/IP стандартов Интернета, определенных в RFC. Одни конструкции Microsoft значительно проще, другие — сложнее. IP-маршрутизация не исключение. Наиболее трудная часть в изучении маршрутизации для Microsoft TCP/IP — терминология и методы. Эта глава далека от исчерпывающего описания реализации маршрутизации и недостаточно полна, чтобы вы смогли, руководствуясь приведенной здесь информацией, настроить IP-маршрутизацию в реальной жизни, но она содержит более чем достаточно информации для того, чтобы вы смогли сдать сертификационный экзамен.

IP-маршрутизация — исследованная и объясненная

Маршрутизация — это процесс, при помощи которого данные, передаваемые с компьютера в сети, направляются узлу-адресату, в случае когда последний находится в разных с исходным компьютером сетях. Единственная роль маршрутизатора в сети — просматривать поступающие пакеты и переправлять их в соответствующий пункт назначения (или же информировать отправителя, что пункт назначения неизвестен или недостижим). Маршрутизатор — это устройство, единственной целью которого является распределение сетевого трафика. Маршрутизатор может быть как отдельным устройством, так и службой на компьютере (например, на Windows NT Server). Поскольку маршрутизаторы позволяют сети взаимодействовать с другими сетями, они часто называются шлюзами. Шлюз — это TCP/IP-узел, одновременно подключенный к двум или большему количеству сетей. Такие устройства называются системами с несколькими сетевыми интерфейсами (см. ниже раздел «Системы с несколькими сетевыми интерфейсами и IP-маршрутизация»).

Маршрутизатор переправляет или ретранслирует пакеты, основываясь на коммуникационных путях, описанных в его таблице маршрутизации. Таблица маршрутизации — это просто база данных, в которой хранятся соответствия между IP-адресами сегментов и IP-адресами интерфейсов маршрутизатора. Когда с какого-либо узла приходят данные, маршрутизатор проверяет таблицу маршрутизации. Если удаленный узел-адресат (или его сетевой сегмент) не указан в таблице маршрутизации, то данные отправляются на шлюз по умолчанию. Шлюз по умолчанию, если он задан, — это узел, на который отсылаются все пакеты, отправленные на неизвестные адреса. Если узел-адресат найден, данные отправляются адресату. Если узел-адресат не найден, на узел-отправитель посылается сообщение об ошибке.

Процесс маршрутизации

Процесс маршрутизации пакетов данных из сети в соседнюю сеть не слишком трудно описать или понять. Следующий пример использует обозначения рис. 6.1.

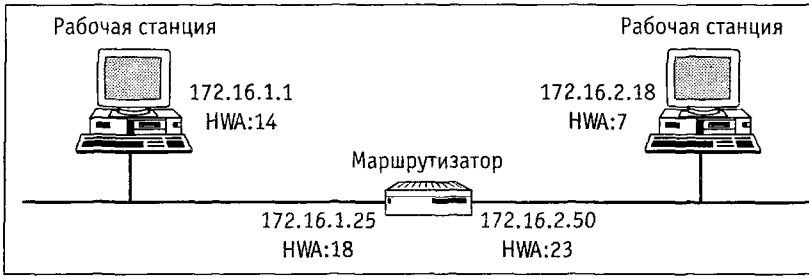


Рис. 6.1. Простейшая маршрутизация

1. Рабочая станция 172.16.1.1 проверяет, находится ли узел 172.16.2.18 в локальной сети.
2. Поскольку 172.16.2.18 не лежит в локальной сети, данные должны маршрутизироваться.
3. При помощи ARP определяется аппаратный адрес (Hardware Address, HWA) шлюза по умолчанию. IP-адрес шлюза по умолчанию задан при настройке рабочей станции 172.16.1.1, но аппаратный адрес шлюза должен быть найден при помощи ARP.
4. 172.16.1.1 отправляет пакет данных на шлюз по умолчанию 172.16.1.25, причем заголовок каждого пакета содержит:
   - Аппаратный адрес отправителя: 14.
   - IP-адрес отправителя: 172.16.1.1.
   - Аппаратный адрес получателя[1]: 18.
   - IP-адрес узла-адресата: 172.16.2.18.
5. Маршрутизатор, расположенный по адресу шлюза 172.16.1.25 и аппаратному адресу 18, определяет по заголовкам пришедших пакетов, что пакеты предназначены для дальнейшей передачи.
6. Маршрутизатор определяет, что пакеты предназначены для сети 172.16.2.
7. Маршрутизатор производит ARP-запрос для определения аппаратного адреса узла-адресата 172.16.2.18. Полученный аппаратный адрес сохраняется в кэше для последующего использования.

[1] Имеется в виду не узел-адресат, а шлюз. — *Примеч. перев.*

8. Маршрутизатор отправляет пакеты в сеть 172.16.2, поместив следующую информацию в заголовок:
   - Аппаратный адрес отправителя: 23.
   - IP-адрес отправителя: 172.16.1.1.
   - Аппаратный адрес получателя: 7.
   - IP-адрес узла-адресата: 172.16.2.18.
9. Данные передаются по сети 172.16.2; сетевая карта узла-адресата распознает свои аппаратный и IP адреса и получает пакет.

Вы должны заметить, что IP-адрес исходного узла сохраняется в заголовке пакета, когда пакет доходит до узла-адресата. Однако в качестве HWA указан аппаратный адрес последнего шлюза, через который прошел пакет (в данном случае это аппаратный адрес интерфейса маршрутизатора). Когда пакет «перепрыгивает» из одной сети в другую, IP-адреса узла-отправителя и узла-адресата не изменяются, но HWA изменяется в соответствии с устройствами, посредством которых передавался пакет.

Процесс маршрутизации становится более сложным и трудно воспринимаемым, если в него вовлекается несколько сетей или если узел-адресат не подключен непосредственно к маршрутизатору. Таблицы маршрутизации позволяют решить эти проблемы, а также аналогичные проблемы, которые возникают при маршрутизации. Таблицы маршрутизации позволяют маршрутизаторам определить, куда необходимо переслать пакет, когда его конечный пункт не указан в таблице. Запомните также, что таблицы маршрутизации содержат только список путей к сетям, но не к отдельным узлам.

Статическая и динамическая маршрутизация

Существуют два типа таблиц маршрутизации: статические и динамические. Системные администраторы должны создавать и обновлять статические таблицы маршрутизации вручную, поскольку таблицы не могут измениться без определенного вмешательства. Динамические таблицы маршрутизации создаются и поддерживаются автоматически при помощи протокола маршрутизации. До появления Windows NT 4 динамическая маршрутизация была доступна только при помощи применения дорогих дополнительных компонентов сторонних производителей. Теперь при помощи MPR и RIP динамическая маршрутизация поддерживается NT Server 4.

Таблица 6.1. Сравнение динамической и статической маршрутизации

Динамическая маршрутизация	Статическая маршрутизация
Функция протокола маршрутизации	Функция IP
Маршрутизаторы разделяют данные	Маршрутизаторы не разделяют данные
Таблицы поддерживаются автоматически	Таблицы создаются вручную
Требует RIP или OSPF	Поддерживается системами с несколькими сетевыми интерфейсами
Используется в больших и сложных сетях	Используется в небольших сетях с простой архитектурой

Статическая IP-маршрутизация

Статическая маршрутизация — встроенная функция IP и не требует каких-либо дополнительных служб для работы. Статическая таблица маршрутизации должна создаваться и поддерживаться на каждом маршрутизаторе вручную. Статический маршрутизатор может быть отдельным маршрутизирующим устройством, или NT сервером с несколькими сетевыми интерфейсами (этот вариант обсуждается ниже в разделе «Системы с несколькими сетевыми интерфейсами и IP-маршрутизация»).

Статическая таблица маршрутизации определяет связи между сетями и интерфейсами шлюза или маршрутизатора для доступа к ним. Статическая таблица маршрутизации состоит из следующих пяти столбцов:

- **Адрес сети.** Адрес каждой известной сети, включая локальный адрес (0.0.0.0) и широковещательный адрес (255.255.255.255).
- **Маска сети.** Маска подсети, используемая для каждой из сетей.
- **Адрес шлюза.** IP-адрес входной точки (интерфейса маршрутизатора) для каждой сети.
- **Интерфейс.** IP, назначенный сетевому интерфейсу.
- **Метрика.** Число ретрансляций («хопов») для достижения сети.

В табл. 6.2 приведен пример таблицы маршрутизации.

Внимание

При работе со статическими таблицами маршрутизации запомните:

- Статический маршрутизатор может взаимодействовать только с теми сетями, которые были внесены в таблицу маршрутизации.
- Статический маршрут может быть определен как адрес шлюза (точка входа) в таблице маршрутизации.

Таблица 6.2. Простейшая статическая таблица маршрутизации

Сеть	Маска	Метрика	Интерфейс	Шлюз
0.0.0.0 (путь по умолчанию)	0.0.0.0	1	10.57.11.169	10.57.8.1
127.0.0.0 (локальный адрес)	255.0.0.0	1	127.0.0.1	127.0.0.1
10.57.8.0 (адрес локальной подсети)	255.255.248.0	1	10.57.11.169	10.57.11.169
10.57.11.169 (интерфейс сетевой карты)	255.255.255.255	1	127.0.0.1	127.0.0.1
10.57.255.255 (широковещательный адрес подсети)	255.255.255.255	1	10.57.11.169	10.57.11.169
224.0.0.0 (групповой адрес)	224.0.0.0	1	10.57.11.169	10.57.11.169
255.255.255.255 (ограниченный широковещательный адрес)	255.255.255.255	1	157.57.11.169	10.57.11.169

Шлюзы

Шлюз — это специальный компьютер или маршрутизатор, который имеет более полный список окружающих сетей, чем обычный компьютер одной из сетей. Когда данные направляются на один из компьютеров вне текущей сети, они передаются на шлюз. Шлюз (маршрутизатор) читает заголовок пакетов и определяет, является узел-адресат локальным (то есть находится ли он в одной из сетей, к которым подключен маршрутизатор) или же пакет должен быть ретранслирован на шлюз по умолчанию. В конечном счете пакет достигает пункта назначения или же отправитель получает сообщение об ошибке, в котором указано, почему распределение пакета не удалось.

Может быть определено более одного шлюза по умолчанию, но для маршрутизации будет использоваться только первый. Другие шлюзы будут использоваться только в том случае, если основной шлюз отключен от сети или недостижим. Это может улучшить производительность сети, особенно при ошибках передачи или сильной загруженности сети.

Команда ROUTE

Команда ROUTE является утилитой TCP/IP, которая используется для создания или модификации статических таблиц маршрутизации на компьютере, работающем под управлением Windows NT Server. Эта команда имеет следующий синтаксис:

```
route [-f] [-p] [команда [адресат] [маска] [шлюз]
[метрика]]
```

Параметры имеют следующий смысл:

- **-f** — Удаление всех записей для шлюзов. Если этот параметр используется в сочетании с другими, то сначала производится удаление записей для шлюзов.
- **-p** — Добавить (при помощи команды **add**) постоянные записи. По умолчанию добавляемые записи не сохраняются при перезапуске системы. Все постоянные пути могут быть выведены на экран при помощи команды **print** (рис. 6.2).

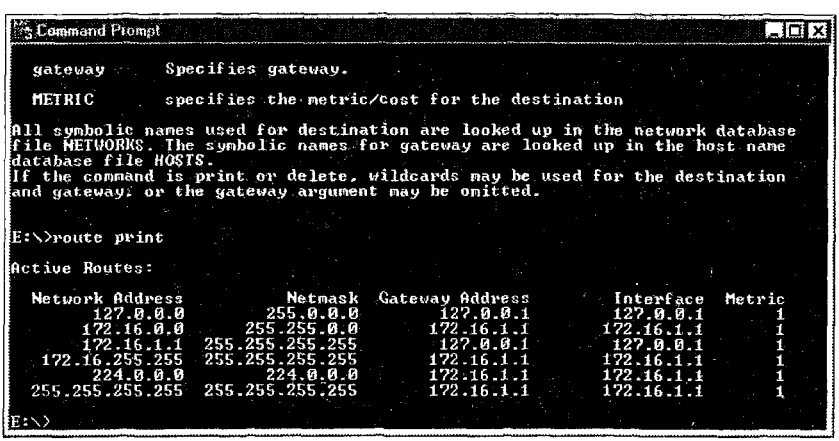


Рис. 6.2. Пример использования команды ROUTE

- *команда* — может быть указана одна из четырех команд: **print** (вывести список путей), **add** (добавить путь), **delete** (удалить путь), **change** (изменить существующий путь).
- *адресат* — определяет компьютер, которому нужно послать указанную *команду*.
- *маска* — Определяет маску подсети для указанного пути. По умолчанию используется 255.255.255.255.
- *шлюз* — шлюз для указанного пути.

- *метрика* — Установка поля **метрика** в таблице маршрутизации в указанное значение. Может быть задано любое значение от 1 до 9999.

Внимание

Запомните, что все произведенные изменения в статической таблице маршрутизации будут потеряны после перезапуска системы. Чтобы произвести постоянные изменения, используйте команду ROUTE с параметром -p.

Команда TRACERT

TRACERT — это еще одна полезная TCP/IP-утилита, используемая из командной строки (рис. 6.3). Эта утилита предназначена для проверки маршрутизации и измерения времени прохождения пакетов. Эта команда имеет следующий синтаксис:

```
tracert [-d] [-h количество_ретрансляций]
[-j список_систем] [-w тайм-аут] имя_системы
```

Параметры имеют следующий смысл:

- **-d** — не переводить IP-адреса в имена систем.
- **-h** *количество_ретрансляций* — максимально допустимое количество ретрансляций («хопов») при поиске системы.
- **-j** *список_систем* — свободный выбор пути среди систем в указанном списке.
- **-w** *тайм-аут* — ожидать каждый ответ указанное число миллисекунд.
- *имя_системы* — Имя системы, поиск пути к которой производится.

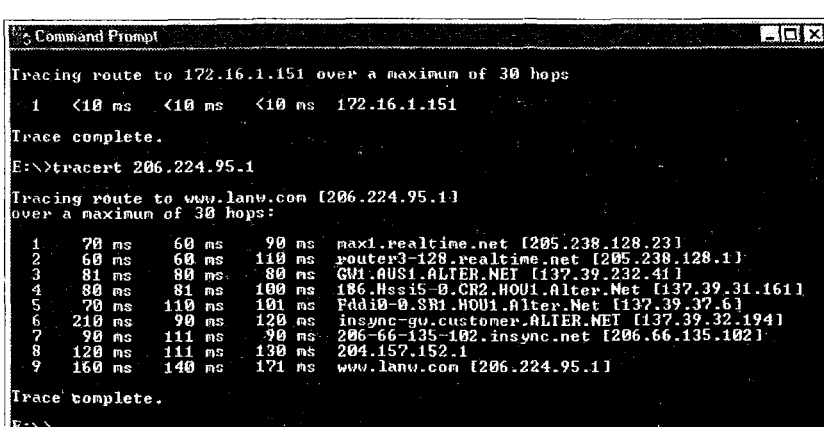


Рис. 6.3. Пример использования команды TRACERT

Внимание

TRACERT — отличная утилита для проверки пути. Вы также можете использовать ее для определения скорости действия путей.

Динамическая IP-маршрутизация

Динамическая маршрутизация обычно предпочтительнее статической в больших сетях со сложной архитектурой, поскольку она позволяет избежать утомительной ручной поддержки огромного количества таблиц маршрутизации. При динамической маршрутизации нагрузка на администратора сети минимальна и часто ограничивается просто указанием шлюза по умолчанию для каждого маршрутизатора. Все остальная настройка и создание таблиц маршрутизации происходит автоматически при помощи протокола маршрутизации.

Два наиболее часто используемых протокола для TCP/IP-маршрутизации — это RIP (Routing Information Protocol, протокол управления маршрутизацией) и OSPF (Open Shortest Path First, открой кратчайший путь первым). Оба эти протокола создают сетевой трафик при обновлении таблиц маршрутизации, но RIP является более «болтливым» протоколом по сравнению с OSPF (он передает по сети через регулярные промежутки времени все таблицы маршрутизации, в то время как OSPF передает по сети только изменения в таблицах). Поэтому OSPF чаще используется в больших сетях, а RIP обычно используется для «локальной маршрутизации» на одном узле. OSPF может связывать между собой несколько RIP-доменов. Это приводит к образованию «иерархии протоколов», которая появляется во многих сетях, в которых OSPF реализован не полностью.

Протокол управления маршрутизацией (RIP)

RIP определяет количество ретрансляций для каждого из определенных путей и использует эту информацию для выбора наиболее эффективного пути.

Внимание

Таблица маршрутизации, поддерживаемая RIP, содержит следующую информацию:

- IP-адрес узла назначения.
- Количество ретрансляций («хопов») — от 0 до 15.
- IP-адрес следующего маршрутизатора в пути.
- Время доставки для каждого пути.
- Время изменения информации о маршрутизации.

Если бы RIP не следил за количеством ретрансляций, могла бы возникнуть проблема подсчета бесконечности. В некоторых сетях, когда канал оказывается недоступным, RIP начинает последовательный поиск лучшего альтернативного пути, что может привести к возникновению логического цикла. Такой цикл может повторяться неограниченно. Чтобы избежать подобных ситуаций, RIP поддерживает счетчик ретрансляций, который может иметь значение от 1 до 15. Когда этот предел оказывается превышенным для проверяемого пути, путь считается бесконечным и удаляется из таблицы маршрутизации. В больших сетях могут возникнуть проблемы с распределением пакетов, если это значение будет слишком мало. Аналогично, путь, проходящий через 16 или более промежуточных пунктов, не будет работать с RIP (16 и бесконечность — синонимы для RIP). RIP позволяет использовать только один путь в один момент времени между двумя узлами, поэтому он не может распределять пакеты по путям в зависимости от нагрузки или распределять нагрузку по нескольким каналам.

Другой недостаток RIP — постоянная широковещательная рассылка таблиц маршрутизации (которая и позволяет называть этот протокол «болтливым»). Это дает возможность каждому маршрутизатору составлять свою таблицу маршрутизации, основываясь как на своих собственных данных, так и на данных других компьютеров сети. Если в сети присутствует несколько маршрутизаторов, то такая рассылка может заметно снизить производительность сети. Обычно широковещательная рассылка производится каждые 30 секунд (для Windows NT, для других систем по умолчанию каждые 60 секунд).

Открой кратчайший путь первым (OSPF)

По сравнению с RIP OSPF является «протоколом второго поколения» и имеет множество преимуществ (подробно они описаны ниже): OSPF создает меньшую нагрузку на сеть, поддерживает сети значительно большего размера, существенно менее «болтлив» и поддерживает множественные пути между узлом-отправителем и узлом-адресатом.

- Каждому каналу может быть присвоен свой вес (количество ретрансляций).
- Ограничение на количество ретрансляций («хопов») — 65 535.
- Каждый узел содержит базу сетевых путей в виде дерева, в вершине которого находится данный узел.
- Если существуют пути с одинаковым весом, нагрузка распределяется между ними.
- Широковещательная рассылка таблиц маршрутизации производится только при появлении изменений.

- Сообщения об изменениях в таблице маршрутизации отправляются только маршрутизаторам, непосредственно связанным с данным; метод «прочти сам и передай дальше» уменьшает нагрузку на сеть.

Когда OSPF реализован в качестве единственного протокола маршрутизации в сети (на компьютерном языке это называется «однородное маршрутизирующее окружение» или «однородная маршрутизирующая система»), каждый маршрутизатор поддерживает свою собственную таблицу маршрутизации, но должен хранить информацию только о непосредственно подключенных к нему подсетях и лишь о тех маршрутизаторах, которые ему непосредственно доступны (так называемых смежных маршрутизаторах).

Windows NT Server 4 не поддерживает OSPF, что, в частности, объясняет, почему вопросы по этому протоколу не появляются в экзамене по TCP/IP. Основная информация, приведенная здесь, достаточна для того, чтобы вы понимали, о чем речь.

Интеграция статической и динамической маршрутизации

Статические и динамические таблицы маршрутизации могут быть интегрированы просто путем определения в каждой статической таблице путей к динамическим маршрутизаторам и определения путей к устройствам, использующим статические таблицы маршрутизации, на динамических маршрутизаторах. Такие двусторонние ссылки позволяют динамическому маршрутизатору работать в качестве шлюза между сетями со статической маршрутизацией. Фактически, это общий подход, позволяющий небольшим несложным сетям взаимодействовать друг с другом.

Внимание

Хотя технология ссылок, которую мы только что описали, позволяет динамическому маршрутизатору работать в качестве шлюза между сетями, использующими статическую маршрутизацию, статические и динамические таблицы маршрутизации не могут взаимодействовать друг с другом и обмениваться информацией о маршрутизации. Поскольку статические таблицы маршрутизации могут изменяться только вручную, это невозможно.

Системы с несколькими сетевыми интерфейсами и IP-маршрутизация

Система с несколькими сетевыми интерфейсами имеет два или более установленных сетевых интерфейса. Каждая сетевая карта имеет свой собственный IP-адрес и маску подсети. Такая система может

маршрутизировать данные между сетями. Чтобы разрешить IP-маршрутизацию на системе с несколькими сетевыми интерфейсами, просто установите флажок Enable IP Forwarding на вкладке Routing окна настройки свойств TCP/IP (показанной на рис. 6.4), которое можно открыть, дважды щелкнув значок Network в окне панели управления.

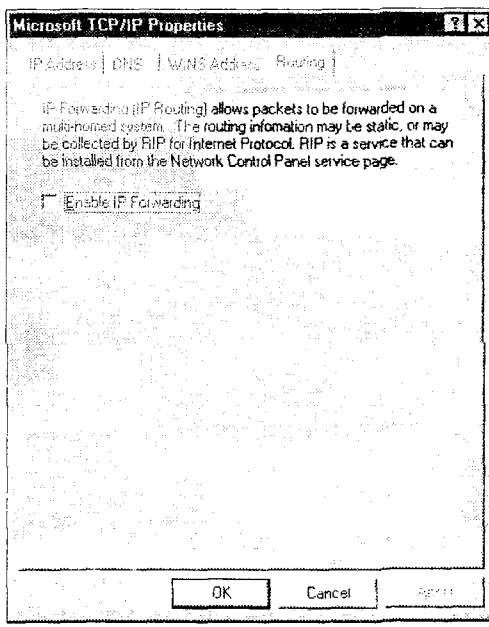


Рис. 6.4. Вкладка Routing окна настройки свойств TCP/IP

Маршрутизация при помощи Windows NT

Microsoft Windows NT Server 4 может работать в качестве простейшего маршрутизатора. Многопротокольный маршрутизатор Microsoft (Microsoft's MultiProtocol Router, MPR) — служба, обеспечивающая динамическую маршрутизацию IP-трафика между различными подсетями, а также поддерживающая IPX-маршрутизацию и агентов ретрансляции DHCP. Однако для использования MPR в сервер следует установить не менее двух сетевых карт, которые должны быть настроены так, чтобы каждая сетевая карта лежала в своей подсети. Другими словами, для работы MPR сервер должен иметь несколько сетевых интерфейсов.

RIP — протокол, используемый для динамического обмена информацией о маршрутизации между маршрутизаторами. После того как RIP установлен, NT будет маршрутизировать соответствующие про-

токолы и динамически обмениваться информацией с другими маршрутизаторами, на которых работает протокол RIP. Кроме того, агент ретрансляции BOOTP для DHCP будет ретранслировать DHCP-запросы серверам DHCP, расположенным в других подсетях, к которым подключен NT-маршрутизатор. Таким образом, один сервер DHCP может обслуживать несколько подсетей.

Внимание

MPR состоит из:

- RIP для TCP/IP.
- Агента ретрансляции BOOTP для DHCP (также известного как агент ретрансляции DHCP).
- RIP для IPX (не обсуждаемого в этой книге).

Маршрутизатор может обмениваться информацией о маршрутизации с ближайшими маршрутизаторами, если использование RIP разрешено. Информация об изменениях в архитектуре сети (например, об отказавшем маршрутизаторе) рассылается ближайшим маршрутизаторам. Маршрутизаторы также производят широковещательную рассылку всей известной информации о маршрутизации через определенные промежутки времени. RIP-маршрутизаторы динамически разделяют информацию.

Внимание

Windows NT может быть как динамическим, так и статическим маршрутизатором. Динамические маршрутизаторы разделяют информацию о маршрутизации с другими маршрутизаторами и автоматически создают таблицы маршрутизации. Статические маршрутизаторы используют созданные вручную таблицы маршрутизации.

Динамическая маршрутизация разрешена, если вы установили RIP для IP. Это можно сделать при помощи вкладки Services окна Network, открываемого из панели управления. После того как RIP установлен, дальнейшая настройка не требуется. Служба будет запущена, и флажок Enable IP Routing в окне диалога Advanced TCP/IP Configuration будет установлен автоматически. RIP для IP работает как служба. Она может быть запущена и остановлена при помощи приложения Services панели управления.

Статическая маршрутизация не создает сетевого трафика, вызываемого динамическим обновлением таблиц маршрутизации, что позволяет снизить нагрузку на сеть. Однако статические маршрутизаторы требуют, чтобы таблицы маршрутизации создавались и изменялись вручную, что может наложить на администратора сети нежелательную нагрузку.

Для того чтобы разрешить статическую маршрутизацию, выполните следующие шаги:

1. Откройте панель управления и, дважды щелкнув на значке Network, соответствующее окно.
2. Откройте вкладку Services. Если RIP для IP установлен на вашем компьютере, то вы должны удалить его, прежде чем разрешить статическую маршрутизацию. Чтобы удалить RIP для IP, выберите его в списке сетевых служб на вкладке Services и нажмите кнопку Remove. (Если RIP для IP останется установленным, будет работать динамическая маршрутизация.)
3. Откройте вкладку Protocols, выберите протокол TCP/IP и нажмите кнопку Properties.
4. Откройте вкладку Routing, установите флажок IP Forwarding и нажмите кнопку OK.

После того как компьютер будет перезагружен, динамическая маршрутизация IP будет полностью запрещена. По умолчанию RIP отправляет широковещательные сообщения об обновлениях таблицы маршрутизации каждые 30 секунд. Вы можете изменить этот интервал при помощи значения реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\IpRip\Parameters\UpdateFrequency.

Интервал может быть установлен от 15 для 88 440 секунд.

Вопросы для подготовки к экзамену

Question 1

A router is or can be which of the following? (Check all correct answers.)

- ❑ A. A multihomed computer.
- ❑ B. An information service.
- ❑ C. A gateway.
- ❑ D. A standalone device.

Вопрос 1

Чем из перечисленного ниже является или может являться маршрутизатор? (Выберите все правильные ответы.)

- ❑ A. Система с несколькими сетевыми интерфейсами.
- ❑ B. Информационная служба.
- ❑ C. Шлюз.
- ❑ D. Отдельное устройство.

Маршрутизатор является или может являться системой с несколькими сетевыми интерфейсами, шлюзом и отдельным устройством. **Следовательно, ответы A, C и D правильны.** Маршрутизатор не является информационной службой. Следовательно, ответ «b» неверен.

Question 2

If the address of the destination host is unknown, where is the data sent?

- ○ A. To the first network address in the routing table.
- ○ B. To the router's cache.
- ○ C. To the default gateway.
- ○ D. To the RIP host.

Вопрос 2

Куда отправляются данные, если адрес назначения неизвестен?

- ○ A. На первый сетевой адрес в таблице маршрутизации.
- ○ B. В кэш маршрутизатора.
- ○ C. На шлюз по умолчанию.
- ○ D. На узел RIP.

Все пакеты данных, адрес назначения которых неизвестен, отправляются на шлюз по умолчанию. **Следовательно, ответ C правилен.** Другие ответы неверны (A и D) или не имеют смысла (B).

Question 3

Which items detailed in a routed packet are different after the packet reaches its destination than their original values at the source host? (Check all correct answers.)

- ☐ A. Source HWA
- ☐ B. Source IP address
- ☐ C. Destination HWA
- ☐ D. Destination IP address

Вопрос 3

Что изменяется в маршрутизируемом пакете по сравнению с исходными значениями после того, как пакет дойдет до узла-адресата? (Выберите все правильные ответы.)

- ☐ A. HWA исходного узла.
- ☐ B. IP-адрес исходного узла.
- ☐ C. HWA конечного узла.
- ☐ D. IP-адрес конечного узла.

Аппаратный адрес (HWA) исходного и конечного узлов изменяется каждый раз, когда пакет проходит через маршрутизатор. **Следовательно, ответы A и C верны.** IP-адреса исходного и конечного узла не изменяются при прохождении маршрутизируемого пакета по сети. Следовательно, ответы B и D неверны.

Question 4

Which of the following are characteristics of dynamic routing? (Check all correct answers.)

- ❑ A. Route tables manually maintained.
- ❑ B. Routers share data.
- ❑ C. Useful for small networks.
- ❑ D. Requires RIP or OSPF.

Вопрос 4

Какие из приведенных ниже предложений относятся к динамической маршрутизации? (Выберите все правильные ответы.)

- ❑ A. Таблицы маршрутизации поддерживаются вручную.
- ❑ B. Маршрутизаторы разделяют между собой данные.
- ❑ C. Разумно использовать в небольших сетях.
- ❑ D. Требует RIP или OSPF.

Динамическая маршрутизация позволяет маршрутизаторам разделять данные и требует RIP или OSPF. **Следовательно, ответы B и D верны.** Вручную поддерживаются статические таблицы маршрутизации, и именно они удобны в небольших сетях. Следовательно, ответы A и C неверны.

Question 5

Which of the following items are found in a static routing table? (Check all correct answers.)

- ❑ A. Interface HWA.
- ❑ B. Source host IP address.
- ❑ C. Hop metric.
- ❑ D. Network address.
- ❑ E. DHCP server IP address.
- ❑ F. Netmask.
- ❑ G. DNS server IP address.
- ❑ H. Gateway address.

Вопрос 5

Какие из следующих полей содержатся в статической таблице маршрутизации? (Выберите все правильные ответы.)

- ❑ A. HWA интерфейса.
- ❑ B. IP-адрес исходного узла.
- ❑ C. Метрика.
- ❑ D. Адрес сети.
- ❑ E. IP-адрес сервера DHCP.
- ❑ F. Маска подсети.
- ❑ G. IP-адрес сервера DNS.
- ❑ H. Адрес шлюза.

Статическая таблица маршрутизации содержит поля: метрику, сетевой адрес, маску подсети и адрес шлюза. **Следовательно, ответы C, D, F и H верны.** IP-адрес исходного узла и IP-адреса серверов DHCP и DNS не содержатся в таблице маршрутизации. Следовательно, ответы A, B, E и G неверны.

Question 6

More than one gateway can be defined. The primary or first default gateway is used unless it is offline or unreachable.

- ○ A. True
- ○ B. False

Вопрос 6

Может быть определено более одного шлюза. В качестве шлюза по умолчанию используется первый из них, за исключением случая, когда он отключен от сети или недоступен.

- ○ A. Да.
- ○ B. Нет.

Да, можно определить несколько шлюзов, но в качестве шлюза по умолчанию будет использоваться первый, за исключением случая, когда он отключен от сети или недоступен. **Следовательно, ответ A правилен.**

Question 7

The ROUTE utility can be used to perform which functions on a routing table? (Check all correct answers.)

- ❑ A. Add new routes.
- ❑ B. Test a route.
- ❑ C. Remove gateway entries.
- ❑ D. Display existing routes.

Вопрос 7

Какие операции позволяет выполнять утилита ROUTE над таблицей маршрутизации? (Выберите все правильные ответы.)

- ❑ A. Добавить новые пути.
- ❑ B. Протестировать путь.
- ❑ C. Удалить записи о шлюзе.
- ❑ D. Вывод списка существующих путей.

Утилита ROUTE позволяет добавлять новые пути (при помощи команды add), удалять записи о шлюзах (при помощи параметра -f), а также выводить существующие записи (при помощи команды print). **Следовательно, ответы A, C и D верны.** Утилита ROUTE не позволяет провести тестирование пути, для этого служит утилита TRACERT. Следовательно, ответ B неверен.

Question 8

By default, newly defined routes added to the static routing table are persistent across system reboots.

- ○ A. True
- ○ B. False

Вопрос 8

По умолчанию вновь определенные пути сохраняются в таблице маршрутизации после перезагрузки системы.

- ○ A. Да
- ○ B. Нет

Нет, по умолчанию пути не сохраняются после перезагрузки. Чтобы добавить постоянные пути, сохраняющиеся после перезагрузки, используйте параметр -p. **Поэтому ответ B верен.**

Question 9

Why is the dynamic routing protocol RIP limited to 15 hops?

- A. The routing table uses hex codes to store hop values.
- B. To prevent infinite counting of looped paths.
- C. To force large networks to be divided into smaller subnets.
- D. No network system ever needs more than 15 hops.

Вопрос 9

Почему протокол динамической маршрутизации RIP позволяет пути длиной не более 15 ретрансляций?

- A. Таблица маршрутизации использует шестнадцатеричный код для хранения количества ретрансляций.
- B. Для предотвращения появления бесконечных циклов.
- C. Для того, чтобы большие сети разбивались на подсети.
- D. Не бывает сетей, в которых используются маршруты большей длины.

RIP использует маршруты длиной не более 15 ретрансляций («хопов»), чтобы предотвратить образование бесконечных циклов. **Следовательно, ответ B верен.** Таблицы маршрутизации не используют шестнадцатеричных кодов для хранения количества ретрансляций; данное ограничение на длину пути позволяет RIP работать в относительно больших сетях; существует множество сетей, использующих пути большей длины (например, Интернет). Следовательно, ответы A, C и D неверны.

Question 10

A computer with more than one NIC that is configured so that it's active in more than one network is called what? (Choose the best answer.)

- A. Internetworked
- B. Multihomed
- C. An MPR host
- D. A RIP server

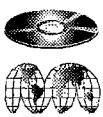
Вопрос 10

Компьютер, имеющий несколько сетевых карт, настроенных так, что они находятся в разных сетях, называется: (Выберите лучший ответ.)

- A. Межсетевым
- B. Системой с несколькими сетевыми интерфейсами
- C. Узлом MPR
- D. Сервером RIP

Компьютер с несколькими сетевыми картами называется системой с несколькими сетевыми интерфейсами. Следовательно, ответ B верен. Такой компьютер не обязан быть маршрутизатором, но, даже если он им является, термины «узел MPR» и «сервер RIP» неверны. Следовательно, ответы C и D неверны. Межсетевой компьютер — компьютер, включенный в несколько сетей. Технически ответ «a» верен, но он недостаточно точен.

Дополнительная информация



Произведите поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com) и на компакт-диске *Windows NT Server Resource Kit*, используя ключевые слова «routing», «RIP», «ROUTE», «TRACERT», «MPR» и «gateway».

Определение IP-адресов

Термины, необходимые для понимания материала:

- Протокол сопоставления адреса (ARP)
- Кэш ARP
- ARP-прокси
- RARP

Приемы и знания, которыми вы должны овладеть:

- Определение локальных и удаленных адресов

Один из тонких моментов при работе с TCP/IP — соответствие между аппаратными (MAC) и логическими (IP) адресами. В этой главе мы обсудим протокол определения адресов (Address Resolution Protocol, ARP) и то, как он работает в TCP/IP-сети. ARP очень редко встречается в вопросах экзамена, и если он все же появляется, то обычно в качестве способа запутать вас. Поэтому важно знать, что делает ARP, чтобы вы знали, когда он является неправильным ответом на поставленный вопрос.

ARP: исследованный и объясненный

Как обсуждалось в главе 2, «Концепции и планирование: TCP/IP и Windows NT», семейство протоколов TCP/IP не принимает во внимание канальный или физический уровни модели OSI. Если пакет передается по сети, он должен содержать аппаратный (MAC) адрес получателя. TCP/IP-протокол сопоставления адреса (ARP) используется для определения аппаратных адресов. ARP подробно описывается в RFC 826.

Этот процесс, по существу, очень прост. Когда компьютер должен отправить какие-либо данные, ARP отправляет в локальную сеть широковещательный запрос об аппаратном адресе узла с данным IP-адресом. Если узел с указанным IP-адресом находится в локальной сети, он отвечает на ARP-запрос. Если узел находится в удаленной сети, то шлюз по умолчанию возвращает в ответ на запрос свой аппаратный адрес, и пакет данных приходит на него.

После того как узел-отправитель выясняет аппаратный адрес, соответствующий данному IP-адресу, он записывает это соответствие в ARP-кэш, который обсуждается подробнее ниже в этой главе в разделе «ARP-кэш». Если через некоторое время происходит отправка данных той же системе, аппаратный адрес берется из кэша и широковещательный запрос не производится.

Определение локальных адресов

Процесс определения адресов в локальной сети состоит из четырех шагов. Для иллюстрации этого процесса рассмотрим следующий пример.

Вы сидите за своим столом и хотите подключиться при помощи Telnet к Unix-системе в Центре управления компьютерами. IP-адрес вашего компьютера — 187.34.234.200; используется маска подсети 255.255.255.0 (сеть класса C); адрес Unix-системы — 187.34.234.10, и на ней используется та же маска подсети. Используя полученные вами в предыдущих главах этой книги знания, вы можете определить, что эта Unix-

система находится в одной подсети с вашим компьютером, следовательно, в этой ситуации требуется определить локальный адрес.

Вы вводите с клавиатуры Telnet 187.34.234.10. После этого ваш компьютер производит поиск соответствующего аппаратного адреса в ARP-кэше. Мы предположим, что в кэше нет аппаратного адреса, соответствующего данному IP-адресу. Итак, работа ARP продолжается.

ARP отправляет широковещательный запрос в локальную сеть: «Не мог бы владелец IP-адреса 187.34.234.10 сообщить свой аппаратный адрес?» Этот широковещательный запрос содержит в себе достаточно информации об обратном адресе отправителя, для того чтобы владелец запрашиваемого адреса (Unix-система) мог отправить ответ непосредственно вашему компьютеру.

Итак, Unix-компьютер отправляет ответ, содержащий его аппаратный адрес. Когда ваш компьютер получает этот ответ, он добавляет информацию в кэш ARP, чтобы ему не пришлось — по крайней мере в ближайшем будущем — снова «заниматься болтовней». После завершения всего процесса компьютеры готовы к обмену данными.

Определение удаленных адресов

Теперь давайте рассмотрим тот же пример, но с участием маршрутизатора. Для этого предположим, что адрес Unix-системы 109.220.10.10, и снова используется маска по умолчанию сети класса C. В этот раз Unix-система окажется в другой подсети и данные для нее проходят через маршрутизатор с локальным адресом 187.34.234.1. Это слегка изменит процесс, но не настолько сильно, чтобы беспокоиться по этому поводу.

Итак, вы сидите за вашим столом и вводите Telnet 109.220.10.10. Ваш компьютер мгновенно определяет, что вы пытаетесь обратиться к компьютеру в удаленной подсети. Для большинства компьютеров это не вызывает никаких проблем, поскольку они имеют только один способ отсылки данных в удаленную подсеть — шлюз по умолчанию. Следовательно, ваш компьютер, определив, что данные должны отсылаться в удаленную сеть, производит в кэше ARP поиск аппаратного адреса шлюза по умолчанию, в нашем примере — маршрутизатора.

Если аппаратный адрес шлюза по умолчанию (187.34.234.1) не найден в ARP-кэше, отправляется широковещательный ARP-запрос аппаратного адреса маршрутизатора.

Маршрутизатор отвечает на ARP-запрос, отправленный вашим компьютером, и сообщает свой аппаратный адрес. Вот в этот момент процесс начинает идти иначе, чем в случае с локальной сетью. Ваш компьютер отправляет при помощи ICMP эхо-запрос Unix-системе через

маршрутизатор, который пытается достичь конечного узла. При этом маршрутизатор начинает свой собственный ARP-сеанс — и так происходит с каждым маршрутизатором по пути следования пакета, пока очередной маршрутизатор не обнаружит, что для него узел-адресат является локальным. Теперь давайте предположим, что в пути между вашим компьютером и Unix-системой находятся три маршрутизатора, каждый из которых должен определить аппаратный адрес компьютера-адресата (иначе говоря, адрес не находится в ARP-кэше каждого из маршрутизаторов). Ближайший к вам маршрутизатор отправляет ARP-запрос следующему маршрутизатору, тот отправляет запрос третьему, и третий маршрутизатор отправляет запрос уже непосредственно компьютеру-адресату.

Наконец, Unix-система сообщает своему локальному маршрутизатору свой аппаратный адрес, а также ответ на ICMP-запрос. Этот процесс определения удаленного адреса также называется «ARP-прокси», поскольку маршрутизатор выполняет для запросов роль прокси-сервера.

Внимание

Наиболее важное отличие, которое вы должны запомнить, между определением локальных и удаленных адресов заключается в следующем: при определении удаленного адреса ответ на запрос содержит аппаратный адрес шлюза по умолчанию; при определении локального адреса ответ на запрос содержит аппаратный адрес непосредственно узла-получателя.

ARP-кэш

Как вы убедились, ARP-кэш является важной частью процесса определения адресов. Он сохраняет информацию о соответствии аппаратных и IP-адресов компьютеров сети. Каждый раз, когда ваш компьютер пытается передать информацию на удаленный узел, он производит поиск аппаратного адреса этого узла в ARP-кэше. Если ARP-кэш не содержит нужного аппаратного адреса, то компьютер производит ARP-запрос — эта процедура была описана выше. После того как аппаратный адрес определен, происходит обновление ARP-кэша, в котором сохраняется полученная информация. ARP-кэш может выглядеть так, как показано на рис. 7.1.

Как вы понимаете, запись не остается в ARP-кэше навсегда. По умолчанию записи остаются там в течение 10 минут. По прошествии этого срока запись удаляется из кэша. В некоторых реализациях TCP/IP отсчет начинается заново, если компьютер взаимодействовал с узлом, которому соответствует запись.

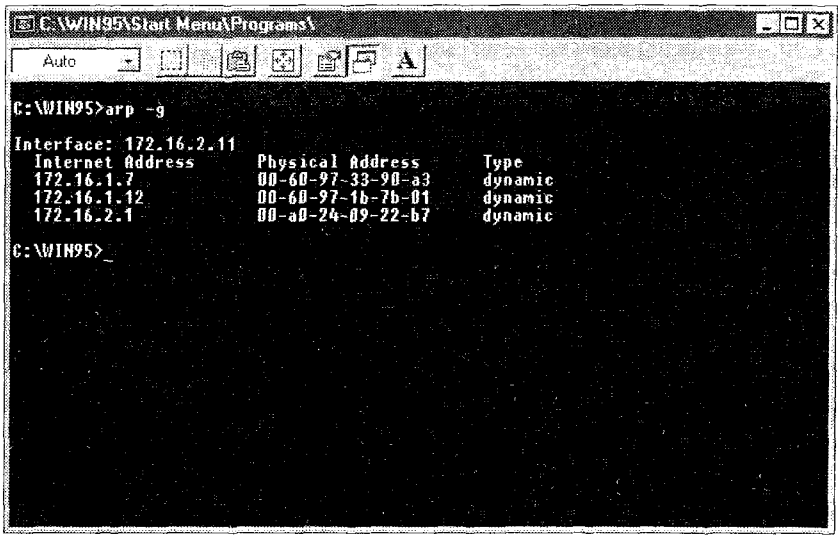


Рис. 7.1. ARP-кэш содержит аппаратные и IP-адреса компьютеров сети

Windows NT трактует ARP-кэш несколько по-иному. Удаление записей из кэша происходит при его переполнении, даже если срок годности записей не истек. NT удаляет первыми наиболее старые записи, невзирая на то, как часто они использовались.

ARP.EXE

Microsoft включила в состав операционных систем Windows утилиту ARP.EXE для просмотра и модификации ARP-кэша. На рис. 7.1 показано, как эта утилита может быть использована для просмотра ARP-кэша на компьютере, работающем под управлением Windows 95.

Адреса можно вводить в ARP-кэш вручную по помощи утилиты ARP.EXE, используя следующий синтаксис:

```
arp -s IP-адрес MAC-адрес
```

Создаваемые таким образом статические записи не удаляются автоматически из кэша, однако они удаляются при перезагрузке системы или при получении широковещательного сообщения, свидетельствующего о неверности записи. Например, если вы добавили в ARP-кэш соответствие между адресами 199.200.100.11 и 10-CE-08-6C-23-1A и ваш компьютер получил широковещательное сообщение о том, что у компьютера с аппаратным адресом 10-CE-08-6C-23-1A IP-адрес 199.200.100.100, то введенная вами запись будет изменена. Если запись обновляется в соответствии с широковещательным сообщением, ее тип изменяется

со статического на динамический и правило десяти минут вступает в силу. Чтобы удалить статическую запись, используйте следующую команду: arp -d IP-адрес MAC-адрес. Ключи -a и -g могут использоваться для вывода всей таблицы или определенных записей, отсортированной по аппаратным или IP-адресам. Имейте в виду, что ключ -g не работает в Windows for Workgroups. Список возможных ключей утилиты ARP.EXE приведен в табл. 7.1.

Внимание

При сдаче экзамена вы должны быть знакомы с утилитой ARP.EXE и ее ключами. Вы можете встретиться с вопросом, в котором дан результат выполнения команды ARP.EXE с определенным ключом, или с вопросом, для ответа на который вам нужно будет знать, как эта утилита может быть использована для поиска неисправности.

Таблица 7.1. *Ключи утилиты ARP и их описание*

Ключ	Описание
-a	Вывод записей, содержащихся в ARP-кэше
-g	Вывод записей, содержащихся в ARP-кэше (этот ключ недоступен в Windows for Workgroups)
-N	Вывод записей, содержащихся в ARP-кэше и относящихся к определенному сетевому интерфейсу
-s	Добавление статической записи в ARP-кэш. Синтаксис: ARP -s IP-адрес MAC-адрес
-d	Удаление статической записи из ARP-кэша

Протокол обратного определения адресов

Мы также считаем нужным упомянуть протокол обратного определения адресов (Reverse Address Resolution Protocol, RARP). Его функции обратны ARP. Он позволяет определить IP-адрес по данному аппаратному адресу и используется большей частью на бездисковых рабочих станциях, которые должны получить свой IP-адрес с сервера. Рабочая станция отправляет широковещательный RARP-запрос, который обрабатывается сервером RARP. Сервер RARP отправляет IP-адрес рабочей станции.

Важно отметить, что RARP в отличие от ARP требует сервера для назначения IP-адресов рабочим станциям. Поэтому RARP используется не так широко; после появления DHCP он является скорее любопытной диковинкой, но не функциональным протоколом.

Проблемы при определении адресов

Наиболее часто встречающаяся проблема при определении адресов связана с неверными масками подсетей. Проблема возникает потому, что при определении адреса узла используется маска подсети для определения расположения узла. Если из-за неверной маски подсети определено, что удаленный компьютер находится в локальной сети, будет производиться непрерывная отправка широковещательных запросов в попытках определить адрес. В худшем случае неверно заданные маски подсетей могут привести к *широковещательному шторму*. Широковещательный шторм — явление, возникающее при неверной работе сетевых устройств и выражающееся в переполнении сети широковещательными пакетами.

Вопросы для подготовки к экзамену

Question 1

For local address resolution, what step does the sending computer take if it does not find the information in its cache?

- A. Sends a request to the ARP server.
- B. Sends a broadcast packet.
- C. Sends a request to the router.
- D. Checks its HOSTS file for the information.

Вопрос 1

Что предпринимает компьютер, если при определении локального адреса он не найден в ARP-кэше?

- A. Отправляет запрос на ARP-сервер.
- B. Отправляет широковещательный запрос.
- C. Отправляет запрос маршрутизатору.
- D. Производит поиск в файле HOSTS.

Правильный ответ на этот вопрос — B. Если компьютер не может найти аппаратного адреса узла-адресата в кэше, он отправляет в сеть широковещательный запрос. Ответ A неверен, поскольку не существует такой вещи, как ARP-сервер. Ответ C неверен, поскольку вопрос относился к определению локального адреса, а маршрутизатор опрашивается только при определении удаленного адреса. Файл HOSTS не содержит информацию об аппаратных адресах. Следовательно, ответ D неверен.

Question 2

Which of the following commands will display the ARP cache for a Windows for Workgroups computer? (Check all correct answers.)

- ❑ A. arp -a
- ❑ B. arp -r
- ❑ C. arp -s
- ❑ D. arp -g

Вопрос 2

Какие из следующих команд позволят вывести содержимое ARP-кэша на экран компьютера, работающего под управлением Windows for Workgroups. (Укажите все правильные ответы.)

- ❑ A. arp -a
- ❑ B. arp -r
- ❑ C. arp -s
- ❑ D. arp -g

Правильный ответ на этот вопрос — A. В большинстве Windows-систем для вывода содержимого ARP-кэша на экран используются команды arp -a и arp -g. Запомните, однако, что в Windows for Workgroups работает только ключ -a. Таким образом, ответ D неверен. Команда arp не имеет ключа -r, а ключ -s предназначен для добавления статической записи в кэш. Следовательно, ответы B и C также неверны.

Question 3

What is the default time an entry will stay in the ARP cache?

- ○ A. 20 minutes
- ○ B. 5 minutes
- ○ C. 10 minutes
- ○ D. 15 minutes

Вопрос 3

Какое время по умолчанию сохраняется запись в ARP-кэше?

- ○ A. 20 минут
- ○ B. 5 минут
- ○ C. 10 минут
- ○ D. 15 минут

Правильный ответ на этот вопрос — C. По умолчанию запись сохраняется в ARP-кэше в течение 10 минут.

Question 4

Under what circumstances is a static ARP cache entry changed or deleted? (Check all correct answers.)

- ❑ A. When the computer is powered off.
- ❑ B. When the **arp -a** command is issued for that entry.
- ❑ C. When contradictory information is received via broadcast.
- ❑ D. When the **arp -d** command is issued for that entry.

Вопрос 4

При каких обстоятельствах статическая запись в ARP-кэше может быть удалена или изменена? (Укажите все правильные ответы.)

- ❑ A. При выключении компьютера.
- ❑ B. При выполнении команды **arp -a** для этой записи.
- ❑ C. При противоречии между этой записью и информацией, полученной из широковещательного сообщения.
- ❑ D. При выполнении команды **arp -d** для этой записи.

Правильные ответы на этот вопрос — A, C и D. Статическая запись в ARP-кэше может быть изменена или удалена при выключении компьютера, при противоречии ее широковещательному сообщению или при использовании ключа -d. Запомните: команда arp -a выводит на экран записи из кэша, но не изменяет их. Следовательно, ответ D неверен.

Question 5

What type of address resolution takes place with proxy ARP?

- ○ A. Local address resolution.
- ○ B. Kinetic address resolution.
- ○ C. Router address resolution.
- ○ D. Remote address resolution.

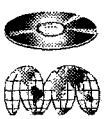
Вопрос 5

Какой тип определения адресов имеет место при использовании ARP-прокси?

- A. *Определение локальных адресов.*
- B. *Кинетическое определение адресов.*
- C. *Маршрутизируемое определение адресов.*
- D. *Определение удаленных адресов.*

Правильный ответ на этот вопрос — D. ARP-прокси — термин для обозначения определения удаленных адресов, поскольку шлюз по умолчанию или маршрутизатор играет роль прокси-сервера для локального компьютера. Определение локальных адресов не использует прокси. Следовательно, ответ A неверен. Словосочетание «кинетическое определение адресов» звучит красиво, но такого термина не существует. Маршрутизируемое определение адресов — также фикция. Следовательно, ответы B и C тоже неверны.

Дополнительная информация



Произведите поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевые слова «ARP», «IP address», «Address Resolution Protocol» и родственные.

Определение имен узлов

Термины, необходимые для понимания материала:

- Имя узла
- Файл HOSTS
- Имя NetBIOS
- Файл LMHOSTS
- Определение имен узлов
- DNS (Domain Name Service, служба формирования имен узлов)
- Кэш имен NetBIOS
- FQDN (fully qualified domain name, полное доменное имя)
- Домены DNS и домены NetBIOS (Windows NT)

Приемы и знания, которыми вы должны овладеть:

- Создание допустимого имени узла для рабочей станции или сервера на основе Windows NT
- Настройка имени узла и имени домена DNS в Windows NT
- Настройки и поиск ошибок в типичном файле HOSTS
- Настройка компьютера под управлением Windows NT для использования определения имен NetBIOS с именами узлов

IP-адресация может быть трудным процессом. В этой главе описываются различные методы, используемые для определения IP-имен. Вы найдете здесь обсуждение краткой истории именования узлов, настройки имени узла, а также FQDN (fully qualified domain name, полное доменное имя). Кроме того, мы исследуем службу формирования имен узлов (Domain Name Service, DNS), файлы HOSTS и LMHOSTS, а также именование NetBIOS.

Имена узлов: исследованные и объясненные

В главе 4, «IP-адресация», мы обсудили необходимость для каждого узла TCP/IP-сети иметь свой собственный уникальный IP-адрес. IP-адрес удаленной системы должен быть известен локальному компьютеру для того, чтобы установить с ней связь. Однако IP-адреса достаточно длинные, и большинству из нас трудно их запоминать. Поэтому для идентификации IP-узлов используются более естественные для пользователя имена, например «Dilbert» или «PrintServ1». Такие имена проще запомнить, и они более осмысленны, чем, скажем, 128.98.212.12.

Хотя имена проще запомнить и они нагляднее определяют TCP/IP-узел, должна существовать возможность определения IP-адреса, соответствующего имени, прежде чем два узла начнут взаимодействие. В этой главе объясняется, каковы могут быть допустимые имена узлов, что такое полные доменные имена (получаемые объединением имени узла и имени домена) и каков процесс, используемый для определения IP-адреса, соответствующего имени узла.

Задание имен узлов

IP-адрес может использоваться для указания TCP/IP-узлов в большинстве приложений Windows Sockets, таких как PING, FTP, Telnet и Web-броузеры. Однако запоминание IP-адресов ваших любимых Web-страниц или нескольких FTP-серверов может быть достаточно трудным, следовательно, эти TCP/IP-узлы имеют имена или псевдонимы, которые просто запомнить. Например, «Binkey», «Dopey», «Server1», «TLP133» и «DRT-398» являются допустимыми именами узлов.

Имена узлов удобны еще и потому, что они позволяют вам найти и идентифицировать машину невзирая на ее физическое расположение или IP-адрес. Напомним, что IP-адрес компьютера соответствует его физическому расположению в сети. Если компьютер переносится из одной сети или подсети в другую, его IP-адрес должен быть изменен,

чтобы этот компьютер мог нормально участвовать в TCP/IP-коммуникациях. Использование имени узла для идентификации системы делает смену IP-адреса прозрачной для конечного пользователя.

Существуют определенные ограничения на вид используемого имени узла. RFC 1123 утверждает, что имя узла может содержать до 255 буквенных символов, включая a–z, A–Z, 0–9 и знак дефиса (-) или точку (.). Специальные символы, такие как !, % и * (восклицательный знак, знак процента и «снежинка»), не допускаются стандартами RFC. Кроме того, имя узла не может состоять только из цифр и не должно содержать знаков подчеркивания.

Ранее имя узла не могло начинаться с цифры, но правила изменились, следовательно, имена, такие как 411info.com или 3com.com, допустимы. RFC 1033 позволяет использовать символ подчеркивания, но этот RFC имеет статус FYI (for your information, к вашему сведению) и не является стандартом. Вы должны избегать использования символа подчеркивания в именах узлов вашей сети, поскольку это может вызвать проблемы с определением имен в Интернете.

Совет

Дополнительная информация о допустимых именах узлов и настройке DNS может быть найдена в документах RFC 1912, RFC 1035, RFC 1033 (информационный, не является стандартом) и RFC 1123. Эти файлы могут быть найдены по адресу http://ds.InterNIC.net/rfc/rfc####.txt. Замените «####» на номер нужного вам RFC.

Настройка имени узла

В процессе установки TCP/IP на Windows NT Workstation или Server вы должны указать допустимое уникальное имя узла для идентификации вашего компьютера в TCP/IP-сети. По умолчанию Windows NT будет использовать в качестве имени узла имя NetBIOS данного компьютера, заменив все недопустимые символы в нем (например, символ подчеркивания) на знак дефиса (-). Вы можете изменить предлагаемое по умолчанию имя, если хотите. Однако, чтобы упростить поиск возникших при определении имен проблем, рекомендуется выбрать имя, которое допустимо одновременно и как имя узла, и как имя NetBIOS. (Понятие «имена NetBIOS» было введено в главе 3, «Установка и настройка». Эта тема и будет обсуждаться подробнее в главе 10, «Определение имен NetBIOS».)

Для настройки имени узла на компьютере, работающем под управлением Windows NT, откройте панель управления и дважды щелкните значок Net. Затем откройте вкладку Protocols. Дважды щелкните значок протокола TCP/IP, чтобы открыть лист свойств TCP/IP. От-

кройте вкладку DNS и введите имя узла и имя домена в соответствующие поля в верхней части листа свойств. Сочетание имени узла и имени домена образует полное доменное имя (FQDN).

Совет

Не путайте домены DNS и домены Windows NT; это два различных типа не связанных между собой доменов. Домен DNS — логическая группа TCP/IP-узлов в IP-сети, и его имя присоединяется к имени узла для получения FQDN. Домен Windows NT состоит из группы Windows-машин, использующих один и тот же PDC или BDC для поддержания политики безопасности группы.

Имена узлов и FQDN

FQDN должно однозначно определять узел среди других узлов Интернета. Оно также обеспечивает уникальность имени узла в больших сетях (таких, как Интернет), поскольку пространство имен доменов Интернета имеет иерархическую структуру. Это означает, что каждое имя может быть разделено на несколько различных частей, в отличие от монолитных имен NetBIOS (которые используют однородное пространство имен). Руководство в каждом разделе и подразделе пространства имен может быть передано локальной группе, которая имеет возможность убедиться, что каждая ветвь и каждый узел имеют уникальное внутри раздела имя. На рис. 8.1 показан пример двух возможных ветвей пространства имен доменов DNS, а также указано, кто отвечает за поддержание каждого уровня пространства имен.

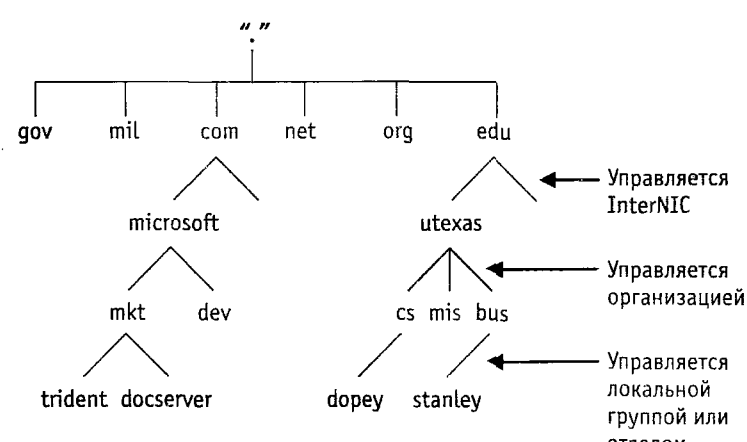


Рис. 8.1. Иерархическая структура пространства имен DNS и распределенные обязанности

InterNIC на настоящий момент поддерживает шесть широко используемых доменов верхнего уровня (отличных от сокращений названий стран): .gov, .mil, .net, .com, .edu и .org. В каждом из этих доменов имеются поддомены, каждый из которых обычно имеет имя, соответствующее названию компании или организации, которую он представляет.

В частности, имя «Microsoft», так же как и имена других компаний, может быть найдено в домене .com; например, microsoft.com или hp.com. Техасский университет и большинство других образовательных учреждений могут быть найдены по именам в домене .edu; например, utexas.edu или tamu.edu.

InterNIC контролирует имена во всех этих доменах верхнего уровня. Вы должны выбрать уникальное имя домена, которое еще не использовалось в том домене верхнего уровня, в котором вы хотите зарегистрировать вашу организацию. Вы также должны уплатить регистрационный взнос. Эта плата будет использована для поддержания серверов DNS в этих доменах верхнего уровня.

После того как ваш домен будет зарегистрирован, ваша организация получает контроль над пространством имен в этом домене. Microsoft может свободно создавать поддомены внутри домена microsfot.com и передавать контроль над этими поддоменами локальным группам. Она может, например, создать внутри основного домена поддомены вида marketing.microsoft.com или finance.microsoft.com. Финансовая группа и группа маркетинга имеют возможность присвоить файл-серверу в своих поддоменах одно и то же имя — «Fred» и быть уверены, что FQDN каждой из этих машин будет уникальным (в нашем примере — fred.marketing.microsoft.com и fred.finance.microsoft.com). Обратите внимание, что FQDN становится более конкретным справа налево.

В Windows NT существуют две утилиты командной строки, которые помогут вам быстро определить имя узла или FQDN конкретной системы. Первая, HOSTNAME, выводит имя узла, а вторая, IPCONFIG /ALL, FQDN для машины, на которой вы работаете. Первое имя в FQDN — первое слово слева до точки — имя локального узла.

Имена узлов, имена доменов и DNS

Прежде чем любые два IP-узла смогут связаться между собой, должен быть известен IP-адрес удаленного узла. Процесс преобразования дружественного пользователю имени узла или домена в IP-адрес называется определением имен. Файл HOSTS — один из способов искать IP-адреса, соответствующие именам узлов. Он представляет собой просто список имен узлов и соответствующих им IP-адресов. Файл HOSTS удобен, когда в сети содержится ограниченное количество IP-узлов. Однако для пользователей было бы достаточно трудно

поддерживать список имен всех TCP/IP-узлов Интернета, с которыми они соединяются.

DNS, распределенная база данных, содержащая соответствия имен узлов и доменов их IP-адресам, предназначена для предоставления службы определения имен TCP/IP-приложениям. DNS позволяет не поддерживать на одном компьютере полный список IP-узлов, распределяя его по многим машинам сети. Каждый сервер DNS отвечает за поддержание базы данных, содержащей соответствия между именами узлов и доменов и IP-адресами для своей локальной области сети. Сервер DNS может быть настроен так, что он будет обращаться к другим серверам DNS, когда не может найти IP-адрес для имени узла или домена в своей локальной базе данных.

Так же как имя узла логически идентифицирует TCP/IP-узел, имя домена логически идентифицирует группу TCP/IP-узлов. Имена доменов обычно соответствуют группам компьютеров или узлов внутри одной организации или компании.

Например, ваше локальное клиентское TCP/IP-приложение может обратиться к серверу DNS за определением IP-адреса, соответствующего имени www.widgets.com. Если ваш сервер DNS не имеет записи для искомого узла, то он обратится к серверу DNS, отвечающему за группу компьютеров в домене widgets.com. Этот второй сервер DNS, скорее всего, принадлежит компании widgets.com и поддерживает список всех узлов в данном домене.

Как работает определение имен узлов

Как было отмечено выше, хотя имена узлов удобно использовать и просто запоминать, TCP/IP требует преобразования этих имен в IP-адреса и, в конечном счете, в аппаратный адрес, до того, как будет установлено соединение с узлом. Определение имен обычно необходимо, когда клиентская утилита TCP/IP нуждается в соединении с TCP/IP-сервером. Определение имен нужно, например, клиентам Telnet и FTP, а также программе PING. На рис. 8.2 показан процесс определения имен в Microsoft Windows NT.

Внимание

Убедитесь, что вы поняли: WinSock-приложения, такие как PING, Telnet и FTP, могут использовать имена узлов и, следовательно, нуждаются в определении имен узлов при помощи файла HOSTS или сервера DNS. Не путайте эти приложения с Microsoft-приложениями, такими как NET: NET USE G:\\server1\share, — команда NetBIOS предназначена для соединения с ресурсом NetBIOS, и, следовательно, требует определения имен NetBIOS при помощи WINS или файла LMHOSTS. Дополнительную информацию об определении имен NetBIOS вы найдете в главе 10, «Определение имен NetBIOS».

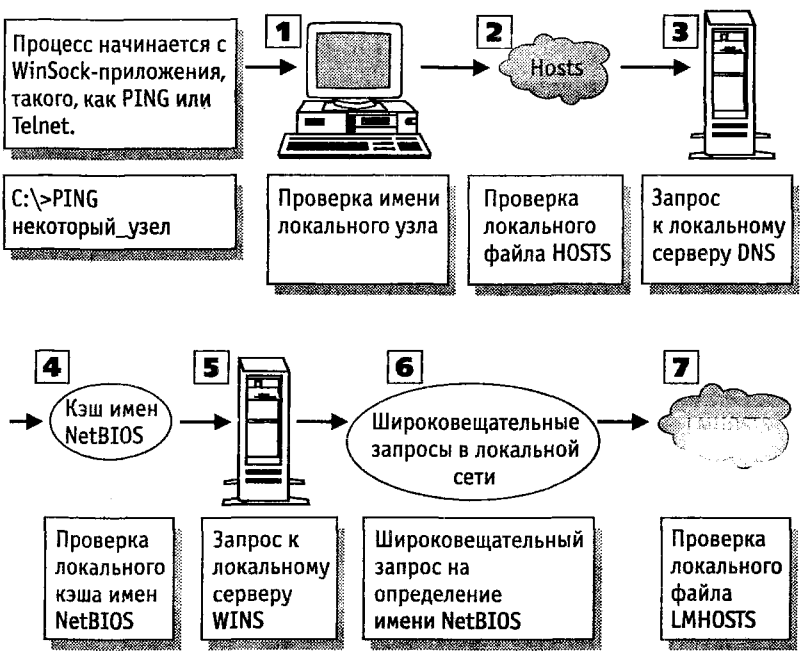


Рис. 8.2. Шаги, выполняемые при определении IP-адреса, соответствующего данному имени узла

В первую очередь TCP/IP проверяет, не содержится ли IP-адрес узла в его собственном кэше имен. Производится сравнение имени узла, с которым должно быть установлено соединение, с именем локального узла, заданным при настройке TCP/IP. Если имена совпадают, компьютер просто открывает TCP/IP-соединение сам с собой на нужном порту.

Если имена не совпадают, то производится поиск IP-адреса, соответствующего имени узла, в файле HOSTS. Этот файл представляет собой обычный текстовый файл, который считывается последовательно строка за строкой, от первой к последней. Если IP-адрес, соответствующий данному имени узла, не обнаружен в этом файле, то TCP/IP обращается к серверу DNS — если были произведены соответствующие настройки (DNS подробно обсуждается в разделе «DNS» ниже в этой главе). Если запрос сервера DNS не дал результатов, производится проверка локального кэша имен NetBIOS.

Все методы определения имен, упомянутые до этого момента, имели отношение только к определению имен узлов, поскольку определялись именно имена узлов, а не имена NetBIOS. Хотя вы можете ис-

пользовать для вашей Windows NT Workstation или Server одно и то же имя в качестве имени узла и имени NetBIOS, эти типы имен сильно отличаются друг от друга. Имя узла обозначает определенный IP-узел, в то время как имя NetBIOS обозначает компьютер под управлением Windows NT Workstation или Server, Windows NT домен, службу или разделяемый сетевой ресурс.

Если DNS не в состоянии определить IP-адрес по имени узла, Windows NT проверяет свой кэш имен NetBIOS в поиске IP-адреса, соответствующего данному имени. Смысл проверки кэша имен NetBIOS состоит только в предположении, что имя NetBIOS и имя узла совпадают.

Если нужное соответствие не найдено в кэше имен NetBIOS, Windows NT может отправить запрос серверу WINS, если были произведены соответствующие настройки. Сервер WINS работает подобно серверу DNS, обеспечивая определение IP-адресов, соответствующих дружественным пользователю именам. Однако сервер WINS содержит базу данных имен NetBIOS, а не имен узлов.

Если в базе данных WINS не было найдено нужного соответствия, Windows NT отправляет широковещательный запрос на определение имени NetBIOS в локальную сеть и ожидает ответа от одного из локальных компьютеров. Если ответ не поступает и запрашивавшая система настроена на использование файла LMHOSTS, то процесс определения имени продолжается.

Наконец, если все остальные методы определения имени не привели к успеху, Windows NT просматривает файл LMHOSTS в поиске подходящего к данному случаю соответствия имя-адрес. Файл LMHOSTS по своему назначению подобен файлу HOSTS, упомянутому выше. Файл LMHOSTS находится на локальной Windows NT-машине и используется для определения IP-адресов, соответствующих именам NetBIOS.

Если один из описанных методов определения имени возвращает IP-адрес, то процесс останавливается, даже если полученный IP-адрес недопустим. Если ни один из методов не позволит найти нужное соответствие имя-адрес, единственный способ установить соединение с удаленным узлом — использовать его IP-адрес вместо имени.

В оставшейся части этой главы мы более подробно рассмотрим перечисленные методы определения имен.

Файл HOSTS

Файл HOSTS представляет собой обычный текстовый файл — изначально, до появления DNS, он и использовался, — предназначенный

для определения имен. TCP/IP читает этот файл строка за строкой, пытаясь найти нужное соответствие имя-адрес. Этот файл может поддерживаться пользователем компьютера или же находиться на сервере и копироваться на каждую машину при ее загрузке. Однако этот файл должен обновляться каждый раз, как IP-адрес какого-либо указанного в нем узла изменяется.

Каждая строка файла HOSTS содержит в начале IP-адрес, за которым должен следовать по крайней мере один пробел и соответствующие этому IP-адресу имена узлов или FQDN. Ни в одной строке не может содержаться несколько IP-адресов, хотя несколько имен узлов или FQDN в одной строке допустимы. Если компьютер настроен на использование файла HOSTS, то этот файл читается строка за строкой каждый раз, когда требуется определить имя узла. Чтобы ускорить определение имен, поместите часто используемые записи в начало этого файла. На рис. 8.3 приведен пример файла HOSTS на компьютере, работающем под управлением Windows NT[1].

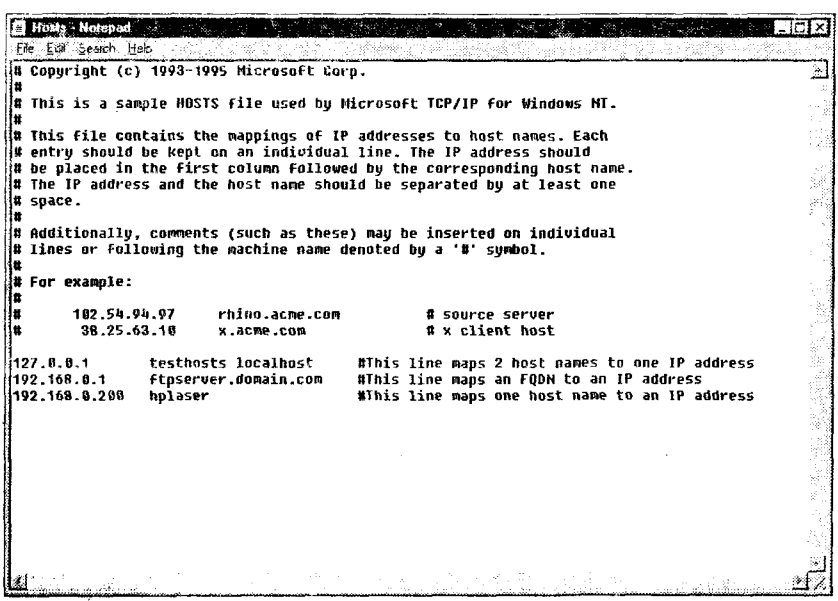


Рис. 8.3. Пример файла HOSTS для Windows NT

Файл HOSTS находится в каталоге *systemroot*\system32\drivers\etc и может редактироваться с использованием любого стандартного тек-

[1] Строки, начинающиеся с символа #, считаются комментариями и игнорируются. — *Примеч. перев.*

стового редактора, такого как Notepad. Убедись, что
те файл без расширения, поскольку многие програм
ют расширение по умолчанию. Для того чтобы сох
расширения при использовании Notepad, помести
вычки: "Hosts".

Внимание

Если вы часто устанавливаете соединение с узла
файле HOSTS, вы можете оптимизировать работу
часто используемые записи в начало файла. Эт
определения имен, поскольку файл считывается
от начала к концу.

Внимание

Для того чтобы Windows NT и TCP/IP могли
он должен находиться в правильном каталоге
Windows NT файл HOSTS находится в каталоге
drivers\etc.

Если файл HOSTS находится в неправильном катало
правильное имя, Windows NT не сможет найти ег
для определения имен. Чтобы убедиться, что ва
пользуется, вы можете изменить или добавить запи
затем использовать команду PING для провери дос
ного имени узла. Используйте такое имя, чтобы бы
оно отсутствует в вашей сети, например mymachin

Вы можете добавить в файл HOSTS следующую стр

```
192.168.0.1    mymachine123
```

Используйте IP-адрес вашего компьютера вместо

После этого, введя команду PING mymachine123, вы
эхо-ответ от указанного узла, если файл HOST испо
не получаете ответа после добавления приведенно
может быть вызвано одной из нескольких причин

- **Файл HOSTS находится в неверном каталоге и
имя.** Запомните, что файл HOSTS в Windows NT
ся в каталоге *sysstemroot*\system32\drivers\etc
имеется образец файла HOSTS. Если вы хотите
ственный файл, редактируя образец, не забуд
рение .SAM. Также убедитесь, что ваш редактор
либо другое расширение.

- **Файл HOSTS содержит одно имя дважды, и для первого появления имени указан неверный IP-адрес.** Если файл HOSTS часто используется и обновляется, то он может быстро вырасти в размере. Даже если узел, уже описанный в файле, будет добавлен в него повторно, то для определения IP-адреса будет использоваться первая запись. При редактировании больших файлов HOSTS используйте возможность поиска в текстовом редакторе, чтобы убедиться в отсутствии повторяющихся записей.
- **Запись в файле HOSTS содержит неверный IP-адрес или опечатку в имени узла.** Эту проблему порой очень тяжело обнаружить. Однако вы можете использовать поиск в текстовом редакторе для обнаружения нужной записи и ее последующего исправления.

Внимание

При решении сетевых проблем крайне важно установить, что является причиной проблемы: физический канал связи между узлами или система определения имен. Простейший способ выяснить это — использование команды PING для известного вам IP-адреса вместо имени узла или имени NetBIOS. Если вы получите ответ, это свидетельствует об исправности физического канала связи и о какой-либо проблеме в системе определения имен.

DNS

Если Windows NT не может найти нужного соответствия имя-адрес в файле HOSTS, она отправляет запрос серверу DNS (если система настроена соответствующим образом на вкладке свойств TCP/IP). Если система не настроена на использование DNS, то она переходит к следующему шагу — проверке кэша имен NetBIOS.

Предположим, что система настроена на использование как минимум одного сервера DNS. В таком случае TCP/IP отправляет запрос первому серверу DNS из списка, заданного при настройке на вкладке свойств DNS. Сервер DNS производит поиск указанного имени узла или домена в своей локальной базе данных. Если соответствующая запись найдена, то IP-адрес отправляется запрашивавшему узлу и процесс определения адреса заканчивается.

Если сервер DNS не имеет в локальной базе данных записи, соответствующей запрашиваемому имени, он может переадресовать запрос другому локальному или удаленному серверу DNS в зависимости от того, что определяется: имя узла или имя домена. Предположим, что второй сервер DNS имеет необходимую информацию. Она возвращается первому серверу DNS, который переправляет ее исходному компьютеру. Процесс определения имени заканчивается.

Допустим, например, что ваша компания зарегистрировала имя widgets.com и ваш администратор сети создал три поддомена в основном домене. Эти поддомены были названы marketing.widgets.com, accounting.widgets.com и admin.widgets.com. Вы работаете в отделе маркетинга, и вашей рабочей станции присвоено имя узла «Fido[1]». Следовательно, полное доменное имя вашей машины — fido.marketing.widgets.com. Предположим, что ваш компьютер настроен на использование сервера DNS при необходимости.

Вы хотите просмотреть Web-страницы на сервере budget в домене admin. Вы вводите адрес http://budget.admin.widgets.com в вашем броузере. Windows NT сначала сравнивает имя сервера, с которым вы пытаетесь соединиться, с собственным именем узла. Поскольку эти имена различны, производится просмотр файла HOSTS на локальном компьютере. Если TCP/IP в Windows NT не обнаруживает в файле HOSTS записи, соответствующей требуемому имени узла или FQDN, то она отправляет запрос на определение имени серверу DNS. Если сервер DNS находит запись, соответствующую требуемому имени узла, то он возвращает IP-адрес для budget.admin.widgets.com на ваш компьютер.

Теперь давайте предположим, что вы хотите установить соединение с узлом ftp.customer.com и что ваш локальный сервер DNS не имеет записи, соответствующей этому узлу. В этом случае сервер DNS должен переадресовать запрос другому серверу DNS, например, серверу DNS домена customer.com. Если этот сервер DNS имеет требуемую информацию, он отправляет ее вашему локальному серверу DNS, который, в свою очередь, отправляет информацию на ваш компьютер. Процесс определения имени на этом заканчивается.

Если сервер DNS возвращает неверный IP-адрес, процесс определения имени также заканчивается. В этом случае вам нужно связаться с вашим локальным администратором или администратором сервера DNS и попросить обновить запись.

Если сервер DNS не может определить IP-адрес и Windows NT получает отрицательный ответ, то производится проверка кэша имен NetBIOS. Если сервер DNS недоступен (не получено никакого ответа), то Windows NT попытается связаться с сервером с интервалами в 5, 10, 20, 40, 5, 10 и 20 секунд. По истечении общего времени в 1 минуту 50 секунд Windows NT либо сообщает об ошибке, либо продолжает процесс определения имени в зависимости от настроек вашей машины.

---

[1] Распространенное имя собаки (наподобие русского «Дружок» или «Шарик»); также — название международной любительской некоммерческой сети. — *Примеч. перев.*

Кэш имен NetBIOS

Если сервер DNS не в состоянии определить IP-адрес данного узла, то Windows NT проверяет локальный кэш имен NetBIOS в поисках нужного имени. Кэш имен NetBIOS на самом деле не содержит имен узлов, но, поскольку имена узлов и имена NetBIOS могут совпадать, кэш может содержать правильный адрес. Если совпадение найдено, имя считается определенным и процесс заканчивается. Если совпадений не найдено, Windows NT отправляет (если она настроена соответствующим образом) запрос серверу WINS.

Единственная причина, по которой имя может быть найдено в кэше имен NetBIOS, — недавнее определение имени или загрузка его в кэш из файла LMHOSTS.

Сервер WINS

Если в кэше имен NetBIOS не найдено совпадений и Windows NT настроена как клиент WINS, то система отправляет запрос серверу WINS. Сервер WINS весьма похож на сервер DNS — он отвечает за определение IP-адресов, соответствующих дружественным пользователям именам. Однако сервер WINS хранит имена NetBIOS, а не имена узлов.

Сервер WINS проверяет свою локальную базу данных в поисках нужного соответствия имя-адрес и, если находит его, сообщает найденный IP-адрес исходному узлу. Если сервер WINS не отвечает, Windows NT предпримет три попытки установить с ним связь.

Если WINS может определить IP-адрес нужного узла, процесс определения имени заканчивается. В противном случае TCP/IP производит широковещательный запрос в локальной сети.

Широковещательный запрос в локальной сети

Определение имен NetBIOS при помощи широковещательного запроса иначе называется «NetBIOS b-node resolution». Компьютер отправляет широковещательный запрос в локальную сеть. Каждый узел локальной сети обрабатывает этот запрос и определяет, не ему ли предназначен запрос. Если узел, получивший запрос, использует то имя, определение которого производится, то он создает ответный пакет, содержащий IP-адрес, и отправляет его запрашивавшему узлу. Если запрашивавший узел не получает ответа от какого-либо компьютера локальной сети после трех запросов, TCP/IP в Windows NT переходит к проверке файла LMHOSTS. Имена и службы NetBIOS могут регистрироваться, поддерживаться и освобождаться при помощи широковещательных запросов. Однако трафик, создаваемый этим процессом, сильно отражается на пропускной загрузке сети и вызывает затраты процессорного времени каждого компьютера локальной сети на обработку широковещательных сообщений. Это объясняет,

почему данный метод определения имен стоит на одном из последних мест в целом процессе.

Файл LMHOSTS

Файл LMHOSTS подобен файлу HOSTS, он является статическим текстовым файлом и используется на локальной системе для определения IP-адресов, соответствующих дружественным пользователю именам (NetBIOS). Этот файл хранится в каталоге *systemroot*\system32\drivers\etc локальной системы. Файл LMHOSTS должен создаваться и обновляться вручную и может редактироваться при помощи обычного текстового редактора. Мы обсудим файл LMHOSTS более подробно в главе 10, «Определение имен NetBIOS».

Если имя, соответствующее определяемому имени узла, найдено в файле LMHOSTS, то используется найденный IP-адрес и процесс определения имен заканчивается. Если имя не найдено, генерируется сообщение об ошибке и процесс определения имен также заканчивается. В таком случае вы должны вручную задать TCP/IP IP-адрес того узла, с которым вы хотите соединиться, или определить, какая часть процесса работает неверно.

Вопросы для подготовки к экзамену

Question 1

Which of the following is not a benefit of using host names to identify TCP/IP hosts?

- A. Host names are easier to remember than IP addresses.
- B. Alphanumeric host names can convey more meaning than plain numeric IP addresses.
- C. Host names allow you to assign several IP addresses to the same machine.
- D. The use of a host name to identify a machine allows the IP address and the location of the machine to be transparent to the end user.

Вопрос 1

Что не является преимуществом использования имен узлов для идентификации TCP/IP-узлов?

- A. Имена узлов проще запомнить, чем IP-адреса.
- B. Имена узлов, составленные из букв и цифр, могут быть более осмысленными, чем IP-адреса.
- C. Имена узлов позволяют назначить несколько IP-адресов одному компьютеру.
- D. Использование имен узлов для идентификации компьютеров позволяет IP-адресу и расположению компьютера быть прозрачными для конечного пользователя.

Лучший ответ на этот вопрос — C. Несколько имен узлов или псевдонимов могут быть присвоены одному и тому же TCP/IP-узлу, но имена узлов не позволяют вам присвоить несколько IP-адресов одному узлу. Ответы A, B и D описывают преимущества использования имен узлов для идентификации TCP/IP-узлов.

Question 2

Which of the following set of characters is not allowed for use in a valid host name?

- ○ A. A–Z
- ○ B. 0–9
- ○ C. a–z
- ○ D. &, !, *, _

Вопрос 2

Какой набор символов недопустимо использовать в именах узлов?

- ○ A. A–Z
- ○ B. 0–9
- ○ C. a–z
- ○ D. &, !, *, _

Правильный ответ — D. Допустимо использовать в имени узла символы A–Z, a–z, 0–9, а также дефис (–) и точку (.). Допустимое имя узла не может содержать специальных символов, таких как амперсанд, восклицательный знак, звездочка или символ подчеркивания.

Question 3

Which of the following statements about configuring a host name on a Windows NT machine are true? (Check all correct answers.)

- ☐ A. By default, the NetBIOS name of the machine is used as the host name.
- ☐ B. Any invalid characters in the NetBIOS name are converted to hyphens (–) in the host name.
- ☐ C. You must change the default host name (that is, the original NetBIOS name) to some name other than the name that is currently being used as the NetBIOS name.
- ☐ D. You can configure the host name and the DNS domain name in the DNS properties sheet of the TCP/IP properties.

Вопрос 3

Какие из следующих утверждений об установке имени узла в Windows NT верны? (Укажите все правильные ответы.)

- ❑ A. По умолчанию в качестве имени узла используется имя NetBIOS компьютера.
- ❑ B. Все недопустимые символы в имени NetBIOS преобразуются в дефисы (-) в имени узла.
- ❑ C. Вы должны изменить имя узла по умолчанию (которое является именем NetBIOS) *на некоторое имя, не используемое в качестве имени* NetBIOS.
- ❑ D. Вы можете установить имя узла и имя домена на вкладке свойств DNS окна свойств TCP/IP.

Правильные ответы на этот вопрос — A, B и D. По умолчанию Windows NT использует в качестве имени узла имя NetBIOS. Все недопустимые символы в имени NetBIOS преобразуются в дефисы в имени узла. Если вы хотите изменить имя узла, вы можете сделать это на вкладке DNS окна свойств TCP/IP. Ответ C неверен, поскольку не обязательно изменять устанавливаемое по умолчанию имя узла.

Question 4

Which of the following statements best describes a DNS domain?

- ○ A. A logical grouping of Windows hosts that all use the same security provider or PDC.
- ○ B. A logical grouping of Windows hosts.
- ○ C. A logical grouping of TCP/IP hosts.
- ○ D. A logical grouping of TCP/IP hosts that corresponds to a particular organization and name, and usually a particular group of IP addresses.

Вопрос 4

Какое из следующих утверждений наилучшим образом описывает домен DNS?

- ○ A. Логическая группа Windows-узлов, использующих один и тот же PDC или один и тот же узел для обеспечения политики безопасности.
- ○ B. Логическая группа Windows-узлов.
- ○ C. *Логическая группа* TCP/IP-*узлов.*
- ○ D. Логическая группа TCP/IP-узлов, соответствующих определенной организации и использующих определенную группу IP-адресов.

Правильный ответ на этот вопрос — D. Домен DNS представляет собой логическую группу компьютеров, имеющих один и тот же доменный суффикс. Эти компьютеры и пространство имен домена обычно контролируются одной организацией или меньшими группами внутри организации. Поскольку большинство организаций получают блок IP-адресов, эти доменные имена обычно соответствуют определенному набору IP-адресов. Ответ A неверен, поскольку он определяет домен Windows NT или NetBIOS, основываясь на политике безопасности. Ответ «b» неверен, поскольку он является просто менее четко выраженным ответом A. Ответ C — лучше, чем A или B, но он не так точен, как D.

Question 5

Which of the following commands will not result in the HOSTS file being accessed?

- A. PING
- B. Telnet
- C. FTP
- D. NET VIEW

Вопрос 5

Какая из следующих команд не приведет к просмотру файла HOSTS?

- A. PING
- B. Telnet
- C. FTP
- D. NET VIEW

Правильный ответ на этот вопрос — D, поскольку NET VIEW является одной из множества сетевых команд NetBIOS, используемых в Windows NT. Эта команда выводит список доступных ресурсов NetBIOS, таких как серверы и разделяемые диски. Команды PING, Telnet и FTP являются WinSock-приложениями, которые производят доступ к файлу HOSTS при определении заданного имени узла, если система настроена на использование этого файла.

Question 6

Which of the following statements are benefits provided by a DNS server? (Check *all correct answers*.)

- ❑ A. A DNS server provides for centralized administration of host names and domain names.
- ❑ B. A DNS server allows for the dynamic registration and release of host names as TCP/IP hosts come up and go down on the network.
- ❑ C. A DNS server is relatively easy to install, configure, and administer.
- ❑ D. A DNS server uses a distributed database to maintain access to a large number of host names and domain names.

Вопрос 6

Какие из следующих утверждений описывают преимущества использования DNS? (Укажите все правильные ответы.)

- ❑ A. Сервер DNS позволяет централизованно администрировать имена узлов и доменов.
- ❑ B. Сервер DNS обеспечивает возможность динамической регистрации и освобождения имен узлов при подключении и отключении TCP/IP-узлов от сети.
- ❑ C. Сервер DNS относительно просто установить, настроить и администрировать.
- ❑ D. Сервер DNS использует распределенную базу данных для обеспечения доступа к большому количеству имен узлов и доменов.

Правильные ответы на этот вопрос — A и D. Сервер DNS позволяет централизованно администрировать множество имен узлов и доменов, устраняя необходимость для каждого пользователя поддерживать собственный файл HOSTS. Серверы DNS используют распределенную базу данных для обеспечения доступа к очень большому количеству соответствий между именами узлов и доменов и IP-адресами. Ответы B и C неверны, поскольку серверы DNS весьма сложно настраивать и они должны поддерживаться специальным администратором. Microsoft DNS в настоящее время не поддерживает динамическую регистрацию имен узлов и IP-адресов.

Question 7

Using the default host name resolution order for Microsoft Windows NT, complete the following statement:

«After TCP/IP checks the local _____, the _____ is consulted. If it cannot resolve the host name, TCP/IP will next consult the _____.»

- A. host name; the LMHOSTS file; NetBIOS name cache
- B. HOSTS file; local DNS server; NetBIOS name cache
- C. DNS server, NetBIOS name cache; local host name
- D. NetBIOS name cache; WINS server; local HOSTS file

Вопрос 7

Считая, что определение имени узла происходит в порядке, заданном по умолчанию, вставьте слова в следующее предложение: «После того как TCP/IP произведет проверку локального _____, производится обращение к _____. Если нужный IP-адрес еще не найден, TCP/IP обратится к _____.»

- A. имени узла, файлу LMHOSTS, кэш имен NetBIOS
- B. файла HOSTS, локальному серверу DNS, кэш имен NetBIOS
- C. сервера DNS, кэшу имен NetBIOS, локальному имени узла
- D. кэша имен NetBIOS, серверу WINS, локальному файлу HOSTS

Правильный ответ на этот вопрос — B. Настройки Windows NT могут запретить выполнение одного или нескольких шагов при определении имени узла. Поэтому, на первый взгляд, несколько ответов кажутся верными. Однако только в ответе B шаги указаны в правильном порядке. Запомните, что по умолчанию определение имени производится в следующем порядке:

Имя локального узла > файл HOSTS > DNS > кэш имен NetBIOS > WINS > широковещательный запрос > LMHOSTS.

Ответ «a» неверен, поскольку после проверки имени локального узла TCP/IP обращается к файлу HOSTS. Ответ C неверен, поскольку по умолчанию TCP/IP проверяет имя локального узла до применения какого-либо другого метода определения имени. Ответ D неверен, поскольку по умолчанию файл HOSTS проверяется до любых попыток определения имени NetBIOS.

Question 8

Which of the following statements properly characterizes the HOSTS file? (Check all correct answers.)

- ❑ A. The HOSTS file is a simple text file that can be edited with any ASCII text editor.
- ❑ B. The HOSTS file must be located in the *systemroot*\system32 directory.
- ❑ C. The HOSTS file only needs to be updated when a machine is moved to another network, not when it simply receives a new IP address.
- ❑ D. The HOSTS file can map IP addresses to simple host names or FQDNs.

Вопрос 8

Какие из следующих утверждений о файле HOSTS верны? (Укажите все правильные ответы.)

- ❑ A. Файл HOSTS представляет собой обычный текстовый файл, который может редактироваться при помощи любого текстового редактора.
- ❑ B. Файл HOSTS должен находиться в каталоге *systemroot*\system32.
- ❑ C. Файл HOSTS должен обновляться при перемещении компьютера в другую сеть, но не тогда, когда компьютер просто получает новый IP-адрес.
- ❑ D. Файл HOSTS может указывать IP-адреса, соответствующие как просто именам узлов, так и FQDN.

Правильные ответы на этот вопрос — A и D. Файл HOSTS является обычным текстовым файлом, который может редактироваться любым текстовым редактором. В нем могут быть указаны IP-адреса, соответствующие как именам узлов, так и FQDN. Также один IP-адрес может соответствовать нескольким именам узлов. Ответ B неверен, поскольку по умолчанию файл HOSTS должен находиться в каталоге *systemroot*\system32\drivers\etc. Файл HOSTS обновляется при появлении новых узлов в сети, а не при перемещении компьютера. Следовательно, ответ «c» также неверен.

Дополнительная информация

Документ Microsoft Technical Information Network (TechNet), September, 97, PN99367 содержит множество статей об определении имен. Произведите поиск, используя ключевые слова «host name resolution», «HOSTS», «LMHOSTS» и «NetBIOS name cache».

Служба формирования имен узлов (DNS)

Термины, необходимые для понимания материала:

- DNS (Служба формирования имен узлов)
- BIND
- Пространство имен доменов
- Зона
- Мастер-сервер имен
- Основной сервер имен
- Дополнительный сервер имен
- Кэширующий сервер имен
- Рекурсивный запрос имени
- Итеративный запрос имени
- Обратный запрос имени

Приемы и знания, которыми вы должны овладеть:

- Установка DNS для Windows NT 4
- Настройка зон DNS
- Установка доменов DNS
- Создание записей DNS
- Построение in-addr.arpa доменов
- Настройка DNS для использования WINS

В этой главе вы узнаете, как служба формирования имен узлов может быть использована для определения имен узлов. Мы обсудим, как устанавливается DNS, дадим несколько советов по ее настройке и объясним некоторые из возможностей DNS. Вы также узнаете, как произвести интеграцию службы определения имен Интернета (WINS) и DNS; подробное описание WINS вы найдете в главе 12, «Служба определения имен Интернета (WINS)».

DNS: исследованная и объясненная

Служба формирования имен узлов (DNS) в настоящее время является основой определения имен в Интернете. Система доменов Интернета представляет собой всемирную иерархическую структуру, администрируемую организацией InterNIC (Internet Network Information Center, сетевой информационный центр Интернета).

Когда Интернет еще назывался ARPANet (Advanced Research Project Agency Network, Сеть агентства по перспективным научным разработкам) и состоял из небольшого количества компьютеров, определение имен не было проблемой; оно осуществлялось при помощи единственного компьютера в Стэнфордском научно-исследовательском институте. На этом компьютере хранился файл HOSTS, который в каждой строке содержал IP-адрес и соответствующие ему имена компьютеров. С ростом Интернета использование этого единственного текстового файла для определения имен стало неэффективным.

В конце концов была разработана служба формирования имен узлов — DNS. DNS обеспечивает похожий на использование файла HOSTS, но более эффективный метод определения IP-адресов. DNS не производит определение адресов при помощи составленных вручную файлов, а использует иерархическую базу данных имен, распределенную по нескольким компьютерам. Эта иерархическая и распределенная природа DNS более эффективна и проще управляема, чем один массивный текстовый файл HOSTS.

Совет

Можно добавить ссылки: Список RFC можно найти поадресу http://www.csl.sony.co.jp/cgi-bin/hyperrfc?rfc-index.txt; RFC 1034 и 1035 можно найти соответственно по адресам http://www.csl.sony.co.jp/cgi-bin/hyperrfc?rfc1034.txt и http://www.csl.sony.co.jp/cgi-bin/hyperrfc?rfc1034.txt.

BIND

BIND (Berkeley Internet Name Domain) — это спецификация DNS, разработанная в университете Беркли в Калифорнии. Эта реализация DNS была исходно создана для операционной системы 4.3BSD Unix.

BIND в настоящее время является наиболее популярной реализацией DNS; однако BIND не является официальной спецификацией Интернета и не поддерживается в RFC. Microsoft DNS основана на реализации BIND и является BIND-совместимой.

Windows NT поддерживает спецификацию BIND при помощи загрузочного файла BIND, находящегося в каталоге %systemroot%\system32\DNS. По умолчанию загрузочный файл не требуется для работы Windows NT или DNS. DNS использует значения, указанные в реестре Windows NT. Однако Windows NT будет использовать загрузочный файл, если вы укажете в реестре, что этот файл должен использоваться. Для настройки этого параметра вы должны отредактировать следующий ключ реестра: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters.

Для того чтобы разрешить использование загрузочного файла, просто удалите значение EnableRegistryBoot. После этого вы должны поместить загрузочный файл в каталог *systemroot*\system32\DNS. Дополнительную информацию о создании загрузочного файла вы можете найти, произведя поиск на Microsoft TechNet CD по ключевым словам «BIND boot file».

Внимание

Запомните, что загрузочный файл BIND делает Windows NT BIND-совместимой; однако BIND не описан в RFC.

Пространство имен доменов

Термин «пространство имен доменов» обозначает структуру и данные, созданные распределенной службой формирования имен узлов в Интернете. Эта иерархия имеет много уровней, и множество различных компьютеров отвечают за поддержку различных ее частей.

На корневом уровне иерархии находятся корневые серверы имен, поддерживаемые InterNIC. Большинство серверов DNS содержит в своих настройках IP-адреса этих корневых серверов. На следующем уровне иерархии расположены домены верхнего уровня, в том числе домены .com, .net, .org, .edu и несколько других суффиксов, обозначающих названия стран или типы поддоменов в домене. Например, microsoft.com является коммерческой организацией, как следует из суффикса .com (commercial). Поскольку Техасский университет — образовательное учреждение, то расположен в домене .edu (educational). Также существуют домены для стран, например, .uk для Великобритании (United Kingdom, Объединенное Королевство), .au для Авст-

ралии и т. п. Многие правительственные учреждения США используют домен .us (United States); однако эта практика не является общепринятой.

Под корневым уровнем и доменами верхнего уровня расположены другие домены. На рис. 9.1 изображена схема пространства имен доменов; это только малая часть всей картины.

В табл. 9.1 приведены некоторые суффиксы доменов, которые вы можете найти на рис. 9.1.

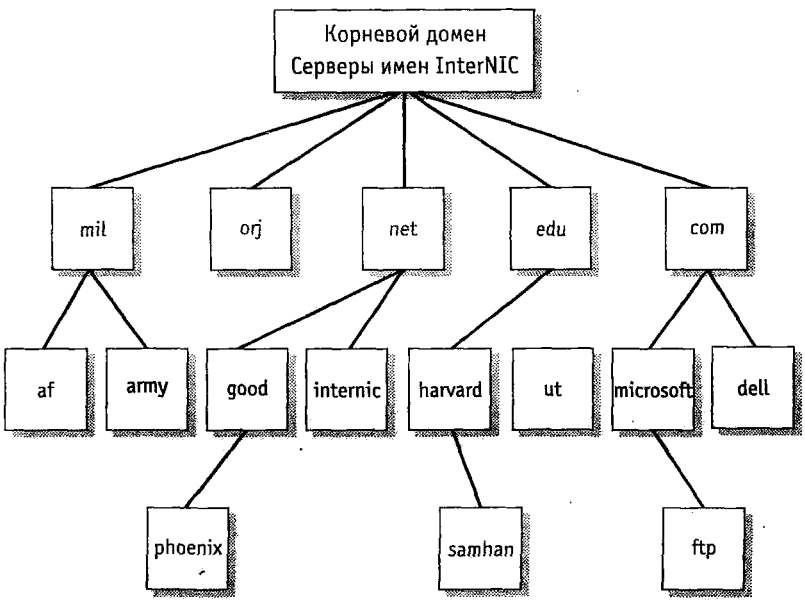


Рис. 9.1. Иерархия пространства имен доменов

Таблица 9.1. Распространенные суффиксы доменов

Суффикс домена	Тип
.com	Коммерческие организации
.edu	Образовательные учреждения
.gov	Правительство[1]
.int	Международные организации
.mil	Военные организации
.net	Общесетевые организации
.org	Некоммерческие организации

[1] Имеется в виду правительство США. — *Примеч. перев.*

В этой иерархии каждый отдельный компьютер представлен именем узла, которое располагается несколькими уровнями ниже корневого домена. Например, это может быть FTP-сервер Microsoft, имеющий имя ftp.microsoft.com, или компьютер, стоящий в сети производителя автомобилей из Остина в Техасе, названный product.aus-tx.saturn.com. Вне зависимости от того, какова длина имени, узел находится в иерархической структуре доменной системы имен. Такой тип имен называется полными доменными именами (FQDN, Fully Qualified Domain Name), поскольку они указывают полный путь к узлу в иерархии. Обратите внимание, что части FQDN становятся менее конкретными слева направо. В приведенном выше примере компьютер «product» находится в Остине, в Техасе в домене «saturn». Вы можете определить, что компьютер расположен в Остине в Техасе и принадлежит компании «Сатурн» (которая является коммерческой организацией). Если вы читаете имя слева направо, вы продвигаетесь от более конкретной информации к более общей. Однако при чтении IP-адреса для данного компьютера, предположим, 205.240.248.93, вы продвигаетесь от более общего к более конкретному. Например, адрес 205 принадлежит уровню домена, а 93 определяет конкретный компьютер в сети. Этот факт будет важен, когда мы будем обсуждать обратное определение имен.

Примечание

Имя product.aus-tx.saturn.com не является реально существующим и было придумано только для примера.

Определение имен

Определение имен при помощи DNS позволяет, аналогично определению имен при помощи файла HOSTS, преобразовать дружественные пользователю имена в IP-адреса, чтобы компьютеры могли взаимодействовать друг с другом по TCP/IP-сети. Однако определение имен при помощи DNS — более сложный процесс, чем просмотр обычного текстового файла. При использовании DNS клиенты обращаются к серверу DNS для определения имен. Сервер DNS пытается выполнить запрос на определение имени. Сервер DNS имеет возможность сбора дополнительной информации от других серверов DNS при выполнении запроса клиента.

При определении имен с помощью DNS компьютер-клиент, пытающийся определить имя, называется резольвером (resolver). Сервер, предоставляющий службы определения имен, называется сервером имен (name server). Сервер имен поддерживает список имен компь-

ютеров и соответствующих им IP-адресов. Записи в этом списке называются записями ресурсов (resource records).

Совет

Термин «резольвер» на самом деле относится к программному обеспечению, работающему на компьютере-клиенте и отправляющему запросы серверу имен.

Различные роли сервера имен

Сервер имен может играть одну или несколько из четырех различных ролей:

- Основной сервер имен отвечает за часть пространства имен доменов, называемого зоной. Информация, образующая зону, содержится в файле зоны. Файл зоны содержит соответствия между IP-адресами и именами узлов, а также прочую информацию, например записи, идентифицирующие почтовый сервер. Основной сервер имен — это сервер имен, который создает и поддерживает зону. Основной сервер имен также выполняет поступающие от клиентов запросы на определение имен.
- Дополнительный сервер имен содержит копию информации о зоне, которую он получает от основного сервера имен или другого дополнительного сервера имен. Это позволяет повысить отказоустойчивость зоны за счет создания избыточности информации. Например, если основной сервер выходит из строя, дополнительный сервер может продолжить определение имен, поскольку он содержит копию файла зоны. Дополнительный сервер имен снижает нагрузку на основной сервер имен, выполняя часть запросов на определение имен.
- Мастер-сервер имен (master name server) — это любой сервер имен, передающий информацию о зоне дополнительному серверу имен. Дополнительные серверы имен настраиваются так, что они обращаются к мастер-серверу за информацией о зоне.
- Кэширующий сервер имен делает только то, что следует из его названия, — кэширует запросы на определение имен. Единственное назначение такого сервера — увеличить эффективность процесса определения имен. Такой тип серверов не содержит постоянного списка узлов в зоне. Кэширующий сервер имен выполняет запросы, обращаясь к другим серверам имен. Однако после того, как кэширующий сервер выполнил запрос, результат запроса сохраняется в кэше, и, если клиент запрашивает адрес для имени, которое было недавно определено, сервер может немедленно возвратить клиенту требуемый адрес. Кэширующие серверы полезны при размещении на противоположном конце медленного канала связи, поскольк-

ку они могут отвечать на запросы клиентов, но не требуют передачи информации о зоне.

Определение при помощи серверов имен

Серверы имен используют не только собственные базы данных или кэши для выполнения запросов на определение имен — они также могут опрашивать другие серверы имен. Это позволяет работать иерархии доменного пространства имен по всему миру. Например, сервер имен в Австралии может определить имя узла в Северной Америке, обратившись к одному или нескольким серверам имен в Северной Америке.

При определении имен используются три типа запросов: рекурсивные (recursive), итеративные (iterative) и обратные (inverse).

Рекурсивные запросы

Рекурсивные запросы наиболее часто используются клиентами. Клиент (резолвер) нуждается в абсолютном определении имени, то есть запрашивает у сервера имен полный IP-адрес. Например, если клиент желает определить IP-адрес FTP-сервера Microsoft, он обращается к серверу имен примерно с таким вопросом: «Какой IP-адрес соответствует имени ftp.microsoft.com?» Если сервер имен не может дать клиенту полный ответ, он должен вернуть сообщение о том, что имя неизвестно.

Итеративные запросы

Итеративные запросы наиболее часто используются между серверами имен для частичного определения имен. Например, сервер имен может не знать целого IP-адреса узла ftp.microsoft.com, но он может знать IP-адрес сервера имен, отвечающего за домен microsoft.com. В этом случае определение имени происходит по частям. Исходный сервер имен выполняет часть работы, запрашивая сервер имен домена microsoft.com. Клиент получает полный адрес от сервера имен; однако исходный сервер имен не требует того же самого от вызываемых им серверов имен.

Обратные запросы

Что происходит, когда вы знаете IP-адрес и хотите узнать, какое имя узла ему соответствует? В этом случае вам также поможет DNS; однако для проведения такого поиска требуется создание специального домена, называемого in-addr.arpa. Домен in-addr.arpa поддерживает список соответствий имен IP-адресам. Особенностью этого списка является то, что IP-адреса записаны в нем в обратном порядке. Упомянутый в предыдущем разделе фиктивный адрес 205.240.248.93

придуманного узла product.aus-tx.saturn.com должен быть записан, как 93.248.240.205 — в том же порядке, как и имя узла.

Шаги процесса определения имени

Для того чтобы уяснить, как происходит определение имен при помощи DNS, *обратите внимание на следующий список шагов. Этот список* перечисляет шаги процесса определения имени ftp.microsoft.com после того, как клиент отправил рекурсивный запрос серверу имен.

1. Сервер имен проверяет кэш DNS и локальную базу данных в поиске соответствующего заданному имени IP-адреса. Если адрес не найден, производится запрос корневого сервера имен.
2. Сервер имен корневого уровня должен вернуть расположение сервера имен низшего уровня (например, microsoft.com).
3. Исходный сервер имен (из шага 1) подключается к серверу имен для домена microsoft.com и запрашивает имя узла ftp.microsoft.com.
4. После того как исходный сервер получил полный адрес требуемого узла, он отправляет его клиенту.

Кэширование и время жизни (TTL)

Когда сервер имен выполняет запрос, он помещает имя в кэш имен. Записи в кэше имен имеют определенное время жизни (Time To Live, TTL), чтобы предотвратить появление проблем с определением имен из-за старых записей, сохранившихся в кэше. Другими словами, вы не хотите, чтобы сервер имен вернул вам старый адрес ftp.microsoft.com, вы хотите свежую информацию.

Когда TTL истекает, запись удаляется из кэша. Клиенты также могут помещать записи в собственные кэши имен. Программное обеспечение на клиенте (резолвере) настраивается так, что оно использует то же значение TTL, что и сервер. Клиент также удаляет запись из кэша по истечении ее TTL.

Совет

Если IP-адреса в вашем домене редко изменяются, установите более высокое TTL для оптимизации процесса определения имен.

Установка и настройка DNS

В Windows NT DNS представляет собой сетевую службу и устанавливается на вкладке Services окна, открывающегося после двойного щелчка на значке Network панели управления. Просто нажмите кноп-

ку Add в окне диалога Services, выберите Microsoft DNS Server и нажмите кнопку OK (рис. 9.2). После этого вы должны вставить компакт-диск с дистрибутивом Windows NT Server 4 (или указать путь к файлам дистрибутива). После того как служба будет установлена, перезагрузите компьютер.

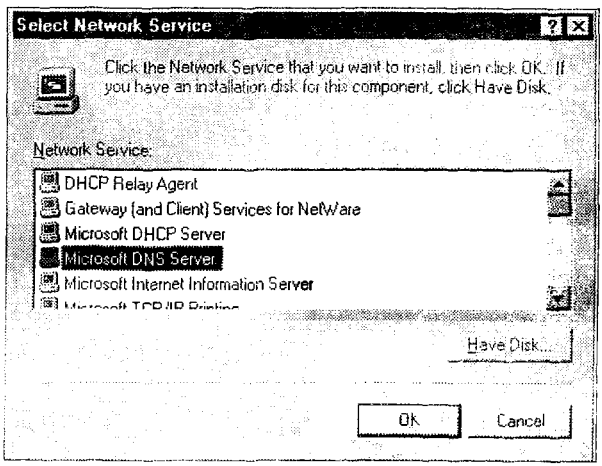


Рис. 9.2. Установка Microsoft DNS Server

После того как вы установите службу DNS, она появится в окне Services, открываемом из панели управления. Эта служба должна иметь статус «Started» и конфигурацию запуска «Automatic» (рис. 9.3).

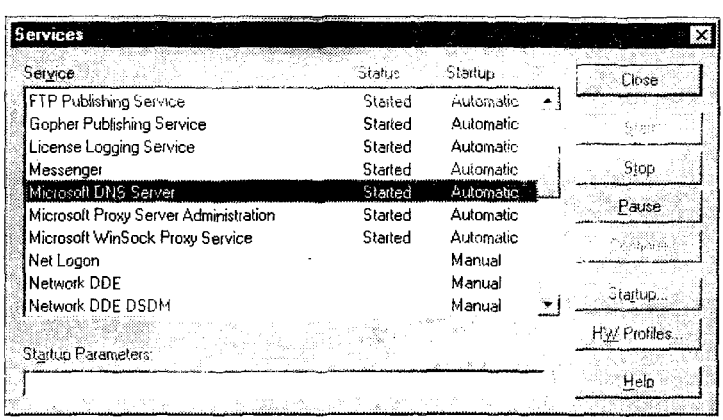


Рис. 9.3. Служба Microsoft DNS Server в окне диалога Services

Настройка доменов и зон

Прежде чем вы начнете настройку сервера имен, вы должны спланировать внутреннее строение всей вашей структуры имен. Обсуждение этого вопроса далеко выходит за рамки этой книги и сертификационного экзамена Microsoft. Вы можете узнать кое-что на эту тему из документа Microsoft TechNet «DNS and MS Windows NT 4.0».

После того как вы определите, какую структуру будете использовать для вашей части доменного пространства имен, вы должны настроить серверы, зоны и домены, находящиеся под вашим управлением. Процесс их создания объясняется в следующих параграфах.

Вы можете настроить ваш сервер DNS при помощи DNS Manager, который устанавливается в группу программ Administrative tools при установке сервера DNS. Когда вы первый раз открываете DNS Manager, он представляет собой фактически чистую доску. Чтобы добавить информацию о вашем сервере в базу данных, выберите в меню DNS команду New Server. Введите имя или IP-адрес вашего сервера и нажмите кнопку OK. После этого сервер должен появиться в списке Servers. Чтобы просмотреть иерархию, настроенную под этим сервером, дважды щелкните значок сервера и разверните дерево. По умолчанию новые серверы настраиваются как кэширующие серверы имен, поэтому под новым сервером вы увидите только один объект — кэш.

Если вы дважды щелкнете значок кэша, дерево раскроется дальше и вы увидите список серверов имен корневого уровня в правой панели DNS Manager. Эта информация берется из файла `CACHE.DNS`, который находится в каталоге `%systemroot%\system32\DNS`.

Совет

После того как ваш сервер DNS будет запущен, вы можете увидеть, как записи появляются в кэше и исчезают из него. Эти записи соответствуют обработке запросов на определение имен, выполняемой вашим сервером. Когда TTL записи в кэше истекает, запись исчезает.

Для продолжения настройки вашего сервера DNS вы должны создать зону, щелкнув правой кнопкой на значке, представляющем ваш сервер имен, и выбрать из контекстного меню команду New Zone (рис. 9.4).

Немедленно после этого вы увидите окно диалога Creating New Zone For. Для вашей исходной настройки выберите Primary и нажмите кнопку Next. Если вы потом захотите создать дополнительный сервер имен, вы должны ввести имя зоны и имя мастер-сервера имен. DNS импортирует при создании дополнительной зоны записи с мастер-сервера имен автоматически.

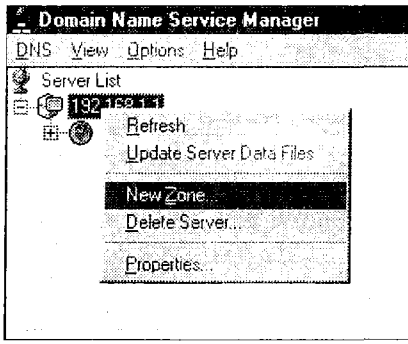


Рис. 9.4. Создание новой зоны

При создании основного сервера имен вы должны далее произвести настройку зоны. Введите имя домена, который вы создаете. Например, если ваш домен — hudlogic.com, введите в поле Zone Name hudlogic.com. Если вы нажмете клавишу Tab, то следующая часть будет заполнена автоматически. По умолчанию имя файла для вашего нового домена образуется добавлением расширения .DNS к имени домена. При этом создается файл в каталоге %systemroot%\system32\DNS. В предыдущем примере создаваемый по умолчанию файл будет называться HUDLOGIC.COM.DNS и находиться в каталоге C:\WINNT\system32\DNS (рис. 9.5). Для того чтобы завершить создание зоны, нажмите кнопку Next и затем Finish.

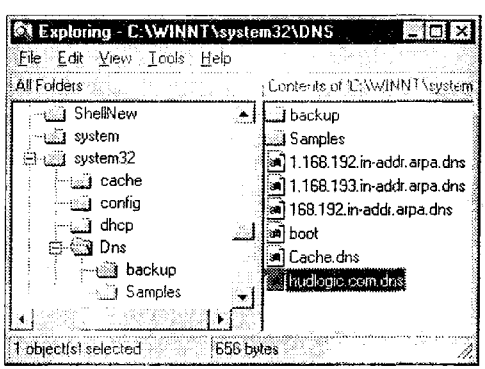


Рис. 9.5. Новая зона и файлы зоны в DNS Manager и создание этих файлов. Вид из Explorer

После того как вы настроили все зоны, которые вам нужны на этом сервере, вы можете добавить поддомены. Для этого щелкните правой кнопкой значок зоны и выберите команду New Domain из контекст-

ного меню. Затем введите в появившемся окне диалога имя поддомена и нажмите кнопку OK. Если вам нужно создать несколько уровней поддоменов, повторяйте этот процесс для каждого объекта вниз по иерархии.

Вы можете ввести записи ресурсов (resource records) в любой из доменов и поддоменов, которые вы создадите. Записи ресурсов — записи, содержащие имя узла и его IP-адрес. Для того чтобы создать запись ресурсов, щелкните правой кнопкой значок домена или поддомена, настройку которого вы хотите произвести, и выберите из контекстного меню команду New Record. Различные типы записей ресурсов, которые могут быть созданы в DNS, описаны в табл. 9.2.

Записи типа «A» — основной тип записей, содержащих соответствия между IP-адресом и именем, которые вы можете увидеть в файле HOSTS. «CNAME» указывает псевдоним для данного узла. Например, если вы хотите использовать имена superman.kryptonite.com и manofsteel.kryptonite.com для одного сервера, можете сделать второе имя псевдонимом для первого. На рис. 9.6 показано, как такая конфигурация выглядит в DNS Manager. Вы можете видеть, как определяются эти имена при использовании команды PING.

Таблица 9.2. Типы записей ресурсов

Тип записи	Описание
SOA	*Start Of Authority* — первая запись в файле базы данных зоны. Она определяет сервер имен, ответственный за зону
A	Записи, которые проецируют имя узла на IP-адрес
NS	Записи *Name Server* определяют другие серверы имен
CNAME	Записи *Canonical Name* определяют псевдонимы для имен узлов. Они позволяют установить соответствие между одним IP-адресом и несколькими именами узлов
MX	Записи *Mail eXchange* используются для указания маршрутизирующих почтовых серверов
PTR	Записи *Pointer* используются для определения имени по IP-адресу в зоне обратного поиска (in-addr.arpa)
WINS	Записи *WINS* позволяют указать серверы WINS
WINS-R	Записи *WINS-R* позволяют DNS использовать WINS для выполнения обратного определения имен

В следующих разделах типы записей PTR, WINS и WINS-R будут разобраны более подробно. Записи PTR используются для обратного определения имен, которое обсуждается в следующем разделе, «in-addr.arpa». Записи WINS и WINS-R обсуждаются в разделе «Интеграция DNS и WINS». Дополнительную информацию о различных ти-

пах DNS-записей вы можете получить из материалов, список которых приведен в конце главы.

Внимание

Если вы хотите создать псевдоним для имени узла, используйте запись типа CNAME.

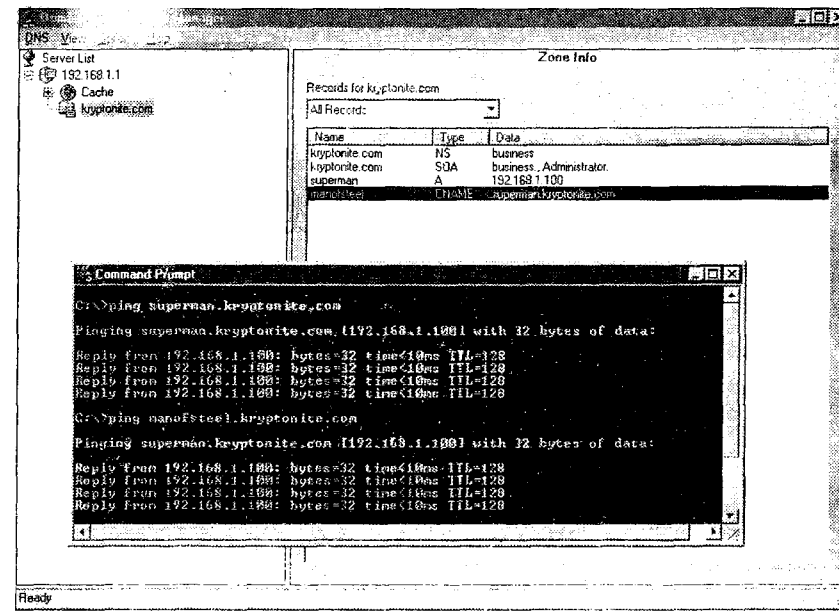


Рис. 9.6. Псевдонимы в окне DNS Manager и результаты команды PING после их создания

in-addr.arpa

Домен in-addr.arpa используется для обратного определения имен. Как упоминалось выше, обратное определение имен используется, когда у вас есть IP-адрес и вы собираетесь определить имя компьютера, имеющего этот IP-адрес. Точнее, это делает используемое вами программное обеспечение. Например, если у вас есть IP-адрес класса C 192.168.1.0, вы должны «перевернуть» часть 192.168.1 (получив 1.168.192) и дописать в конец in-addr.arpa. Итак, ваш in-addr.arpa-домен — 1.168.192.in-addr.arpa. Все, что вы должны сделать, — создать новую зону с таким именем.

Внимание

PTR-записи — это указатели на домен in-addr.arpa, которые используются для обратного определения имен.

Кроме того, PTR-записи в домене in-addr.arpa создаются автоматически при создании вами A-записей в прямой зоне. По умолчанию, когда вы вводите запись, флажок Create Associated PTR Record установлен (рис. 9.7).

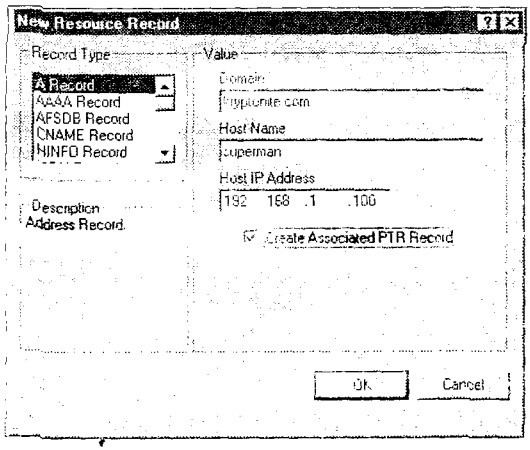


Рис. 9.7. Создание PTR-записи

Если по некоторым причинам автоматическое создание PTR-записи не удается — это происходит только в том случае, если вы не создали in-addr.arpa-домен, — вы можете создать запись вручную. Для этого щелкните правой кнопкой на значке домена in-addr.arpa и выберите в контекстном меню команду New Record. Затем выберите в качестве *типа записи PTR Record и введите IP-адрес узла и имя компьютера* (рис. 9.8).

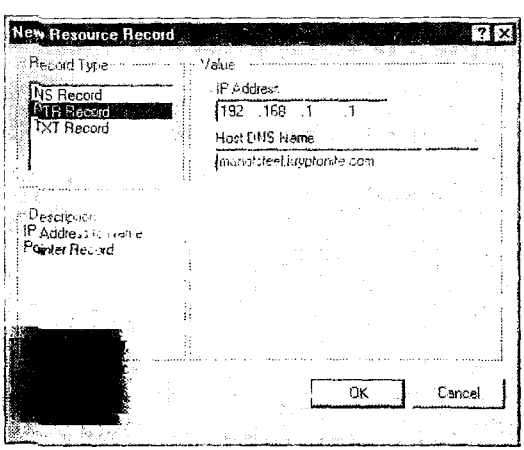


Рис. 9.8. Ручное создание PTR-записи в домене in-addr.arpa

Интеграция DNS и WINS

Ваш сервер DNS может быть настроен на использование для определения имен в числе других серверов сервера WINS. Сервер WINS может помочь серверу DNS в определении последней части FQDN (имени узла). Например, если ваш сервер имен пытается определить имя product.aus-tx.saturn.com, то сервер WINS может помочь в определении части product всего FQDN.

Совет

В главе 12, «Служба определения имен Интернета (WINS)», вы познакомитесь с процессом определения имен при помощи WINS. В настоящий момент вы должны понимать только то, что WINS является еще одним методом, позволяющим преобразовать имена компьютеров в IP-адреса. В этом разделе вы должны уделить основное внимание описанию записей ресурсов для использования WINS. WINS будет использоваться для определения только последней части полного доменного имени, эта часть также называется именем узла.

Чтобы разрешить использование WINS вашему серверу DNS, щелкните правой кнопкой мыши на значке, представляющем ваш домен (например, kryptonite.com), и выберите из контекстного меню пункт Properties. Откройте вкладку WINS Lookup и установите флажок Use WINS Resolution. Введите адрес сервера WINS, который будет использовать ваш сервер DNS при определении имен узлов; это создаст соответствующую WINS-запись в вашем домене (рис .9.9).

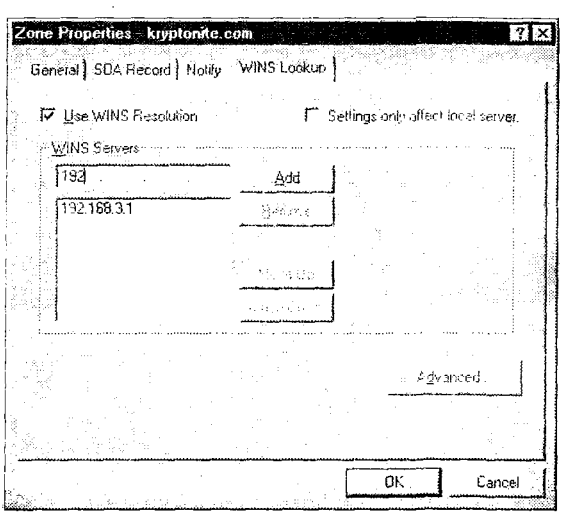


Рис. 9.9. Создание WINS-записи

После того как вы настроите зону для взаимодействия с сервером WINS, вы должны убедиться, что все остальные серверы имен, отвечающие за эту зону (иными словами, поддерживающие список имен в зоне), также настроены для взаимодействия с сервером WINS. В противном случае определение имен в вашем домене может работать от случая к случаю, что будет трудно выявить и устранить. На этой же вкладке вы также можете установить TTL для адресов, найденных при помощи WINS, нажав кнопку Advanced.

Внимание

Готовясь к экзамену Microsoft, убедитесь, что вы запомнили процесс интеграции DNS и WINS.

WINS и обратное определение имен

Хотя WINS и не предназначена для определения имени узла по его адресу, сервер DNS может быть настроен на использование сервера WINS для этой цели. Для того чтобы произвести такую настройку, щелкните правой кнопкой мыши значок домена in-addr.arpa для вашего узла и выберите в контекстном меню пункт Properties. Откройте вкладку WINS Reverse Lookup и установите флажок WINS Reverse Lookup. В окне диалога DNS Host Domain введите имя вашего домена DNS (например, kryptonite.com). Имя, которое вы введете, будет добавляться ко всем ответам WINS для этого домена перед возвратом имени клиенту.

DNS-уведомление

Microsoft-реализация DNS включает DNS-уведомление (DNS Notify), которое позволяет мастер-серверу информировать дополнительные серверы имен об изменениях в базе данных DNS. Мастер-сервер предлагает дополнительным серверам имен начать процесс переноса информации о зоне. Для того чтобы настроить DNS-уведомление, щелкните правой кнопкой значок, представляющий ваш домен, и выберите в контекстном меню пункт Properties. Откройте вкладку Notify и введите IP-адреса дополнительных серверов имен для вашей зоны. Если вы установите флажок Only Allow Access From Secondaries Included On Notify List, сервер имен будет доступен только для тех дополнительных серверов имен, которые указаны на вкладке Notify.

Внимание

При настройке дополнительных зон DNS вы должны поместить серверы в список DNS Notify, чтобы быть уверенными в том, что изменения базы данных на мастер-сервере будут реплицированы на дополнительных серверах имен.

DNS Round-Robin

DNS также может использоваться для распределения нагрузки в вашей сети. Например, Microsoft имеет несколько физических компьютеров, составляющих Web-узел Microsoft; когда вы подключаетесь к узлу Microsoft, вы не знаете, какой физический сервер вы на самом деле используете. Это возможно, поскольку DNS может выдавать для одного имени несколько IP-адресов. Если вы вводите одно и то же имя компьютера дважды, указав при этом различные IP-адреса, то DNS будет использовать эти адреса попеременно. Например, если вы вводите имя www.kryptonite.com дважды и задаете для него два различных IP-адреса, то DNS будет чередовать эти адреса при выполнении запросов на определение данного имени. На рис. 9.10 показаны результаты команды PING при подобной настройке DNS. Обратите внимание, что имя определяется как IP-адрес 192.168.1.100 в первый раз и как IP-адрес 192.168.3.1 в следующий. Такой режим работы DNS называется Round-Robin.

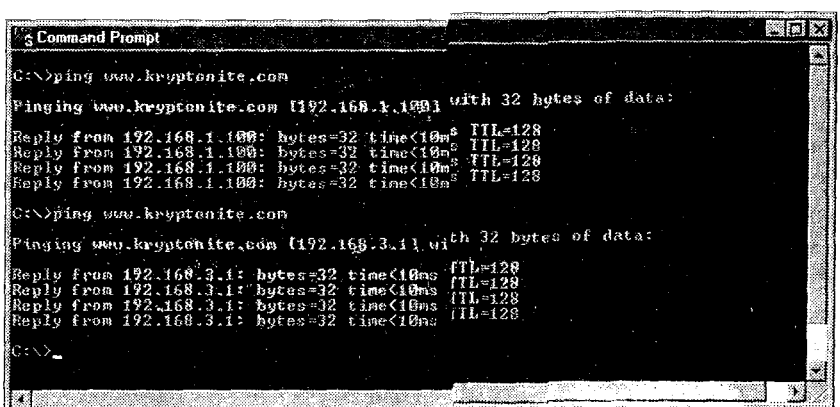


Рис. 9.10. Round-Robin

Внимание

Запомните, что при настройке DNS Round-Robin вы должны ввести одно имя компьютера несколько раз, указывая при этом различные IP-адреса. После этого DNS будет автоматически чередовать адреса из списка.

Настройка клиентов DNS (резольверов)

Настройка Microsoft Windows NT клиентов DNS исключительно проста; просто откройте вкладку Protocols окна диалога Network. Затем

дважды щелкните протокол TCP/IP для того, чтобы открыть окно его свойств, и откройте в этом окне вкладку DNS (рис. 9.11).

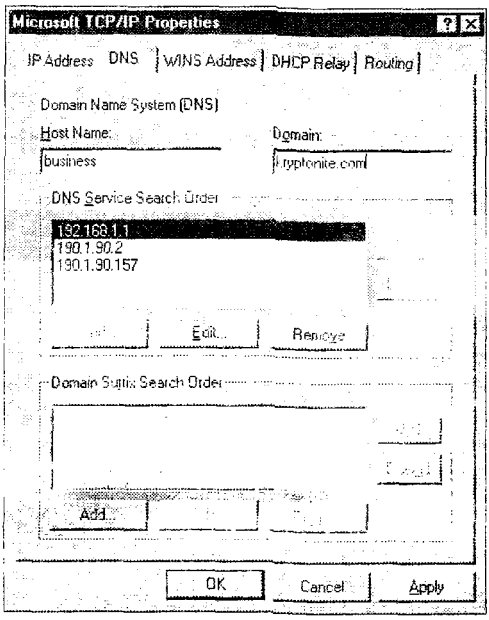


Рис. 9.11. Настройка клиента DNS

По умолчанию имя вашего узла совпадает с именем компьютера, заданным на вкладке Identification окна диалога Network. Вы также можете указать имя вашего домена (имя домена Интернета, а не имя домена Windows NT). В группе DNS Service Search Order введите IP-адреса серверов имен, которыми будет пользоваться клиент для определения имен. Обратите внимание, что вы можете установить порядок, в котором эти серверы будут опрашиваться. В разделе Domain Suffix Search Order вы можете установить порядок, в котором будет производиться поиск в доменах верхнего уровня. Например, вы можете ввести .com, .edu и .mil именно в таком порядке. Это будет означать, что домен .com будет опрашиваться до доменов .edu или .mil.

Поиск проблем с DNS при помощи NSLOOKUP

Серверы DNS работают не полностью автоматически; они требуют ручной настройки и поддержки, и иногда в них есть ошибки. Для поиска ошибок вы можете не изменять непосредственно ваши фай-

лы DNS или просматривать записи в DNS Manager, а воспользоваться утилитой NSLOOKUP.

Внимание

NSLOOKUP является утилитой командной строки, которая может использоваться для поиска ошибок в базе данных DNS.

NSLOOKUP — крайне полезная утилита, позволяющая отправлять запросы серверу DNS. Она работает даже с Unix-реализациями DNS. Вы можете запустить NSLOOKUP из командной строки, используя следующий синтаксис:

```
nslookup [-параметр ...] [компьютер | - [сервер]]
```

NSLOOKUP может работать в одном из двух режимов — интерактивном или не интерактивном. Если вам нужно произвести поиск только одной записи, вы найдете, что неинтерактивный режим удобнее. На рис. 9.12 показан результат работы этой команды в неинтерактивном режиме.

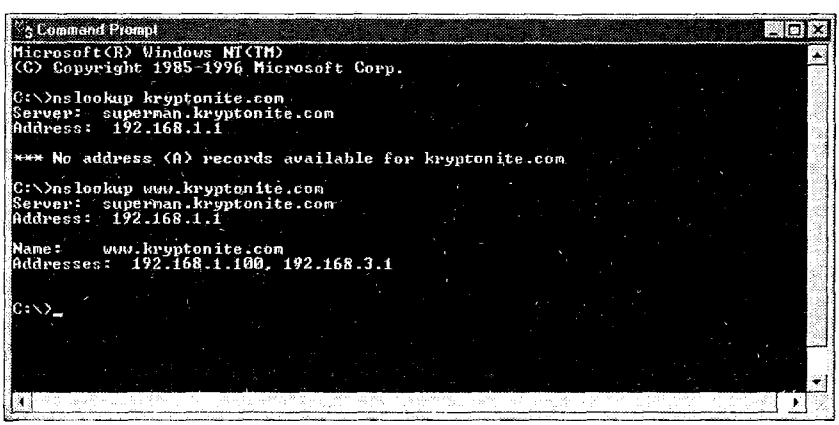


Рис. 9.12. Работа NSLOOKUP

Если вы вводите дефис (-) вместо имени компьютера, NSLOOKUP запускается в интерактивном режиме, в котором вы можете произвести несколько запросов. Если вы сомневаетесь в имени, которое вводите, используйте интерактивный режим и введите несколько запросов, один за другим, пока вы не найдете то, что ищете. Дальнейшую информацию об утилите NSLOOKUP вы можете найти в файле WINNT.HLP, который входит в поставку Windows NT 4. Вы также можете произвести поиск на Microsoft TechNet CD по ключевому слову «NSLOOKUP».

Вопросы для подготовки к экзамену

Question 1

Which method of host name resolution uses a single static text file to resolve Internet names? (Check the best answer.)

- A. Domain Name System.
- B. Domain Name Space.
- C. HOSTS.
- D. LMHOSTS.

Вопрос 1

Какой из методов определения имен узлов использует статический текстовый файл? (Выберите лучший ответ.)

- A. Служба формирования имен узлов (DNS).
- B. Пространство имен доменов.
- C. HOSTS.
- D. LMHOSTS.

Правильный ответ — C. Этот вопрос на самом деле проверяет знание вами истории методов определения имен в Интернете. Сложность этого вопроса заключается в том, что среди ответов указан файл LMHOSTS, который является статическим файлом. Однако файл LMHOSTS используется не для определения имен узлов, а для определения имен NetBIOS. Следовательно, ответ D неверен. Служба формирования имен узлов и пространство имен доменов ссылаются на распределенную систему определения имен, а не на статический текстовый файл. Следовательно, ответы A и B неверны.

Question 2

Which RFC explains the BIND specification?

- A. RFC 822
- B. RFC 883
- C. RFC 1542
- D. None

Вопрос 2

Какой из RFC описывает BIND?

- ○ A. RFC 822
- ○ B. RFC 883
- ○ C. RFC 1542
- ○ D. Никакой

Правильный ответ на этот вопрос — D. BIND не описан в RFC. BIND является преобладающим методом реализации DNS, но он не является официальным стандартом Интернета. Все остальные ответы, очевидно, неверны: RFC 822 и RFC 883 описывают доменную систему имен, и RFC 1542 описывает BOOTP и DHCP.

Question 3

Which of the following files contain DNS resource records for name resolution? (Check all correct answers.)

- ☐ A. CACHE.DNS.
- ☐ B. 12.122.205.IN-ADDR.ARPA.DNS.
- ☐ C. Boot file.
- ☐ D. HUDLOGIC.COM.DNS.

Вопрос 3

Какие из следующих файлов содержат записи ресурсов DNS, используемые для определения имен? (Укажите все правильные ответы.)

- ☐ A. CACHE.DNS.
- ☐ B. 12.122.205.IN-ADDR.ARPA.DNS.
- ☐ C. Загрузочный файл.
- ☐ D. HUDLOGIC.COM.DNS.

Правильные ответы на этот вопрос — A, B и D. Файл CACHE.DNS используется для указания вашему серверу имен корневых серверов InterNIC, которые используются для определения имен. Имя файла 12.122.205.IN-ADDR.ARPA.DNS показывает, что этот файл относится к адресу класса C 205.122.12.0 и используется для обратного определения имен. HUDLOGIC.COM.DNS — файл, содержащий записи ресурсов для определения имен в домене HUDLOGIC.COM. Загрузочный файл содержит информацию, используемую сервером DNS

только при его запуске. По умолчанию сервер Microsoft DNS не использует этот файл. Следовательно, ответ C неверен. Все другие файлы, перечисленные в этом вопросе, используются для определения имен.

Question 4

How do you enable DNS to allow it to call a WINS server in order to resolve a host name?

- A. Add an entry in the WINS database pointing to the DNS server.
- B. Check Enable DNS For Windows Resolution on the client computer.
- C. Add a WINS resource record to the zone and enable WINS resolution.
- D. In the name server properties, configure WINS Lookup.

Вопрос 4

Как вы можете настроить DNS на использование сервера WINS для определения имен узлов?

- A. Добавив в базу данных сервера WINS запись, указывающую на сервер DNS.
- B. Установив флажок Enable DNS For Window Resolution на компьютере-клиенте.
- C. Добавив запись ресурсов типа WINS в зону и разрешив определение имен при помощи WINS.
- D. При настройке DNS указав необходимую информацию на вкладке WINS Lookup в окне свойств DNS.

Правильный ответ — C. Вы должны быстро понять, что ответы A и B неверны. Вы не настраиваете WINS на использование DNS, вы настраиваете DNS на использование WINS. Следовательно, ответ A неверен. Второй ответ описывает настройку клиента WINS, позволяющую ему использовать FQDN, а не настройку сервера DNS для использования WINS. Последние два ответа могут вас слегка запутать. При настройке DNS вы должны произвести настройки WINS Lookup, однако они находятся не в окне свойств DNS; они находятся в окне свойств зоны; следовательно, ответ D неверен. На вкладке WINS Lookup вы должны установить флажок Use WINS Resolution и затем ввести IP-адрес сервера WINS. После того как вы произведете эти изменения, WINS-запись будет добавлена в зону.

Question 5

Which types of names can WINS resolve for DNS?

- A. Host
- B. FQDN
- C. Domain
- D. Root

Вопрос 5

В определении каких типов имен сервер WINS может помочь серверу DNS?

- A. Имен узла
- B. FQDN
- C. Имен домена
- D. Корневых имен

Правильный ответ на этот вопрос — A. Единственная трудность состоит в том, что, хотя сервер DNS определяет FQDN, он отправляет серверу WINS только часть FQDN — имя узла. Имена доменов и корневые имена не определяются сервером WINS, поскольку они находятся вне его поля зрения.

Question 6

Which type of query is used by a name server to navigate the Domain Name Space hierarchy to answer a name query from a resolver?

- A. Recursive
- B. Iterative
- C. Inverse
- D. WINS

Вопрос 6

Какой тип запросов используется сервером имен для перемещения по доменной системе имен при выполнении запроса на определение имени, поступившего от клиента?

- A. Рекурсивный запрос.
- B. Итеративный запрос.
- C. Обратный запрос.
- D. WINS.

Правильный ответ на этот вопрос — A. Рекурсивные запросы используются для абсолютного определения имени. Итеративные запросы используются для частичного определения имени; следовательно, ответ «b» неверен. Обратные запросы используются для определения имени узла по его IP-адресу; следовательно, ответ C неверен. WINS используется для определения части FQDN — имени узла. Итак, ответ D также неверен.

Question 7

Your company has configured seven different Internet-style domains for your network. You are responsible for the Southwestern domain. Which of the following could you implement to distribute the name resolution load of your domain? (Check all correct answers.)

- ❑ A. DNS Round-Robin.
- ❑ B. Secondary zone.
- ❑ C. Primary name server.
- ❑ D. Caching-only server.

Вопрос 7

Сеть вашей компании состоит из семи различных Интернет-доменов. Вы отвечаете за юго-западный домен. Что вы можете использовать для распределения нагрузки, создаваемой запросами на определение имен в вашем домене? (Укажите все правильные ответы)

- ❑ A. DNS Round-Robin.
- ❑ B. Дополнительную зону.
- ❑ C. Основной сервер имен.
- ❑ D. Кэширующий сервер имен.

Правильные ответы на этот вопрос — B и D. DNS Round-Robin не позволяет распределить нагрузку по определению имен. Это метод, используемый DNS для распределения нагрузки, создаваемой клиентами, на несколько серверов, при помощи определения одного имени в различные IP-адреса. Основной сервер имен не поможет вам, поскольку он будет производить обработку запросов на определение имен домена, отличного, от того, в котором вы работаете. Для распределения нагрузки вы можете настроить дополнительную зону или добавить кэширующий сервер имен в вашу существующую зону.

Question 8

Which record type allows the DNS server to call WINS for inverse name resolution?

- A. A
- B. CNAME
- C. WINS
- D. WINS-R

Вопрос 8

Какой тип записей позволяет серверу DNS вызывать WINS для обратного определения имен?

- A. A
- B. CNAME
- C. WINS
- D. WINS-R

Правильный ответ на этот вопрос — D. Единственный тип записи, позволяющий DNS вызывать WINS для обратного определения имен — WINS-R. Записи CNAME позволяют задавать псевдонимы; записи типа A используются для указания IP-адресов, соответствующих именам; и записи WINS указывают на серверы WINS, используемые при обычном определении имен.

Дополнительная информация

Произведите поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевые слова «DNS», «Domain Name System», «CACHE. DNS» и «DNS Zone».

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы должны найти статью, называющуюся «DNS and Windows NT 4.0», авторами которой являются Scott B. Suhy и Glenn Wood.

Документы RFC 822 и RFC 883 описывают DNS. Вы можете найти их по адресам http://ds.internic.net/rfc/rfc882.txt и http://ds.internic.net/rfc/rfc883.txt.

Определение имен NetBIOS

Термины, необходимые для понимания материала:

- Имя NetBIOS
- Файл LMHOSTS
- Регистрация имени
- Поиск имени
- Освобождение имени
- *Широковещательный B-запрос*
- WINS
- Типы запросов
- Просмотр сети

Приемы и знания, которыми вы должны овладеть:

- Понимание различных методов определения имен NetBIOS
- Определение типов приложений и служб, использующих имена NetBIOS
- Понимание процесса регистрации, поиска и освобождения имен NetBIOS
- Определение используемых Windows NT по умолчанию методов определения имен
- Определение разницы между определением имен NetBIOS и просмотром сети
- Поиск и устранение проблем, связанных с просмотром сети и определением имен NetBIOS

В этой главе мы обсудим имена NetBIOS и их использование при работе Windows в сети. Имена NetBIOS имеют назначение, похожее на назначение имен узлов, — они позволяют использовать дружественные пользователю имена для идентификации Windows-машин в сети. Однако имена NetBIOS используются для идентификации не только IP-узлов. Узлы, работающие под управлением Windows, используют NetBIOS для регистрации не только своих имен, но и сетевых файловых служб, сетевых служб печати и прочих сетевых служб Windows.

Имена NetBIOS: исследованные и объясненные

В главе 8, «Определение имен узлов», мы обсудили идентификацию и подключение к узлам с использованием имен узлов вместо IP-адресов. Имя узла обычно более понятно пользователю и его проще запомнить, чем IP-адрес. Эти дружественные пользователю имена также являются логическими идентификаторами узлов, не изменяющимися при смене по какой-либо причине IP-адресов узлов (например, при перемещении узла в другую подсеть).

Внимание

Для того чтобы хорошо понять имена NetBIOS, полезно сравнивать их с именами узлов — и наоборот. На протяжении этой главы мы будем сравнивать имена NetBIOS с именами узлов и пояснять различия в их функциональности. Знание сходств и различий между именами NetBIOS и именами узлов очень поможет вам при сдаче экзамена.

Имена NetBIOS

Каждый Windows NT-узел (и другие узлы, работающие под управлением Windows) получает имя NetBIOS при установке операционной системы. Это имя используется для однозначной идентификации компьютера в сети. Однако имена NetBIOS используются не только для обозначения узлов; они используются приложениями и процессами NetBIOS для взаимодействия с другими приложениями NetBIOS на удаленных узлах.

Имя NetBIOS состоит из 16 символов. Пользователь может определять первые 15 символов. Шестнадцатый символ зарезервирован под тип ресурса (тип имени, службы или группы, представляемой именем NetBIOS).

Предположим, к примеру, что рабочая станция HORTON под управлением Windows NT имеет три разделяемых каталога, доступных другим компьютерам сети: FUNNIES, DOCS и MEMOS. При загрузке эта рабочая станция отправляет в локальную сеть (или серверу WINS, если рабочая станция так настроена) сообщение с именами NetBIOS, которые она предполагает использовать, именем рабочей группы или домена, к которому она желает подключиться, и списком служб, которые она предоставляет. Имя компьютера и все службы получат при регистрации NetBIOS имя HORTON, но все эти имена будут использовать различные шестнадцатеричные значения для шестнадцатого символа.

Ниже приведен вывод команды NBTSTAT -N, показывающий, как может выглядеть таблица имен для HORTON. Мы обсудим эту и другие утилиты ниже в этой главе.

```
Node IpAddress: [192.168.0.1] Scope Id: [null]
NetBIOS Local Name Table
Name       Type          Status
HORTON     <00> UNIQUE   Registered
CORP       <00> GROUP    Registered
JAMES      <03> UNIQUE   Registered
HORTON     <20> UNIQUE   Registered
CORP       <1E> GROUP    Registered
```

В первой строке этой таблицы указано имя NetBIOS HORTON и указано, что это имя уникально. Шестнадцатеричное значение <00> означает, что данное имя NetBIOS является именем компьютера и зарегистрировано службой рабочей станции данного компьютера. CORP, второе имя NetBIOS в списке, является именем домена, в котором находится данный узел. Последний байт имени NetBIOS JAMES имеет шестнадцатеричное значение <03>, что означает, что это имя пользователя, работающего в настоящий момент на рабочей станции HORTON. Наконец, последний байт имени NetBIOS HORTON с шестнадцатиеричным значением <20> обозначает службу сервера, работающую на компьютере HORTON.

Для того чтобы понять, как могут использоваться имена NetBIOS, давайте предположим, что вы собираетесь смонтировать в качестве сетевого диска разделяемый каталог на компьютере HORTON. Вы открываете Windows NT Explorer, выбираете команду Map Network Drive, вводите G: в качестве диска и \\HORTON\memos в качестве имени сетевого ресурса. (Формат записи \\имя_компьютера\имя_ресурса из-

вестен как UNC — Universal Naming Convention — универсальное соглашение об именовании.)

Вашему компьютеру потребуется установить соединение со службой сервера на компьютере HORTON, чтобы получить доступ к разделяемому ресурсу. Используя широковещательный B-запрос (подробно обсуждаемый в одноименном разделе), ваша рабочая станция может отправить компьютеру HORTON запрос на определение его IP-адреса и подтверждения того, что на нем работает служба сервера.

Теперь, когда вы знаете, что такое имена NetBIOS и как они используются, давайте разберемся, как имена NetBIOS регистрируются и определяются в сети.

Регистрация, поиск и освобождение имен NetBIOS

Имя NetBIOS регистрируется в сети каждый раз при загрузке узла — в отличие от имени узла, которое определяется при помощи статического файла HOSTS или при помощи базы данных DNS. Имена NetBIOS узлов могут регистрироваться в локальной сети при помощи широковещательного сообщения или при помощи сервера WINS, что обеспечивает доступ к узлу всем остальным узлам целой сети.

Если узел не настроен на использование сервера WINS (сервера имен NetBIOS), то он отправляет в локальную сеть широковещательное сообщение с именем NetBIOS, которое он собирается использовать. Это широковещательное сообщение называется запросом на регистрацию имени NetBIOS. Все узлы локальной сети обрабатывают это сообщение с целью определить, не используют ли они уже регистрируемое имя. Если запрашиваемое имя уже используется одним из узлов сети, он отправляет отказ в регистрации данного имени. Это предотвращает инициализацию TCP/IP на исходном узле и генерирует сообщение об ошибке. Если имя не используется и ни один узел сети не отправляет отказа в регистрации, то производится инициализация TCP/IP на запрашивавшем узле, и загрузка продолжается.

Использование в сети сервера WINS устраняет необходимость широковещательных запросов, однако в целом процесс практически не изменяется. Вместо отправки широковещательного сообщения в локальную сеть клиент отправляет запрос на регистрацию имени непосредственно серверу WINS. Если сервер WINS еще не зарегистрировал это имя для использования другим узлом, он позволяет запрашивавшему узлу использовать указанное имя NetBIOS. Если сервер WINS находит запрашиваемое имя в своей базе данных, он отправ-

ляет сообщение узлу, использующему это имя в настоящий момент, с просьбой подтвердить использование имени. Если этот узел включен в сеть и работает нормально, он подтверждает использование имени, и узел, запрашивавший регистрацию, получает сообщение об ошибке. Если использование имени не было подтверждено, то сервер WINS позволяет запрашивавшему узлу использовать это имя.

Аналогично, процесс определения имен NetBIOS может происходить при помощи широковещательных запросов (используются B-запросы) или по схеме «точка-точка» (используется WINS). При определении IP-адреса, соответствующего имени NetBIOS, узел сначала проверяет свой кэш имен NetBIOS. Это область памяти, содержащая недавно определенные имена NetBIOS и соответствующие им IP-адреса. Если в кэше имен не найдено требуемого соответствия и узел не настроен на использование WINS, то он отправляет в локальную сеть широковещательный запрос на определение имени NetBIOS, называемый широковещательным B-запросом (b-node broadcast). Этот запрос получают и обрабатывают только компьютеры локальной сети, за исключением того случая, когда маршрутизаторы сети настроены на маршрутизирование пакетов на UDP-портах 137 и 138. Если компьютер локальной сети использует запрашиваемое имя, то он сообщает свой IP-адрес.

Внимание

Широковещательный B-запрос получают только узлы локальной сети, за исключением того случая, когда маршрутизаторы настроены на маршрутизирование пакетов на UDP-портах 137 и 138. Хорошо подумайте, прежде чем разрешить такую маршрутизацию, *поскольку это уменьшит пропускную способность сети.*

Если узел, которому требуется определить имя NetBIOS, настроен на использование сервера WINS, то, прежде чем пытаться отправить широковещательный запрос, он отправляет запрос на определение имени непосредственно серверу WINS. Сервер WINS проверяет свою базу данных и отправляет найденный IP-адрес непосредственно запрашивавшему узлу. Если сервер WINS не может определить требуемый IP-адрес, узел отправляет широковещательный запрос в локальную сеть. Если и это не помогает определить имя NetBIOS, то узел проверяет локальный файл LMHOSTS (если он настроен на это).

Наконец, в течение процедуры останова системы узел NetBIOS «освобождает» свое имя NetBIOS. Это означает, что он информирует сервер WINS или узлы локальной сети о том, что данное имя больше не используется и запросы, использующие это имя, не могут быть выполнены.

Клиент, использующий WINS, обычно устанавливает соединение с сервером WINS в течение останова системы и освобождает свое имя NetBIOS. Сервер WINS помечает в своей базе данных соответствующее имя NetBIOS как «освобожденное». Если после этого другой компьютер обратится за запросом на регистрацию этого имени, запрос будет удовлетворен. Однако если работа компьютера была завершена неправильно, то имя может остаться не удаленным из базы данных. Тогда, если новый узел запросит регистрацию этого имени, сервер WINS обратится к узлу-владельцу имени с просьбой подтвердить его использование. Если подтверждение не будет получено, то имени NetBIOS будет присвоен новый IP-адрес и запрос на его регистрацию будет удовлетворен. Такая ситуация может возникнуть, когда пользователь с переносным компьютером перемещается из одной подсети в другую.

Клиенты, которые не настроены на использование WINS, отправляют широковещательное сообщение об освобождении имени NetBIOS в локальную сеть. Это позволяет другим компьютерам локальной сети удалить имя из кэша имен NetBIOS.

Определение имен NetBIOS

IP-адрес, соответствующий имени NetBIOS, может быть определен одним из четырех способов: при помощи локального кэша имен NetBIOS, при помощи сервера WINS, при помощи широковещательного B-запроса и при помощи файла LMHOSTS. Если ни один из этих способов не дает результата, также производятся попытки определения имени при помощи файла HOSTS и при помощи сервера DNS.

Совет

Для запоминания порядка, в котором производится определение имен NetBIOS, можно воспользоваться мнемоническим правилом: «Как Вам Закупить Лишний Хороший Диск»[1]:

1. Кэш имен NetBIOS («К»).
2. WINS («В»).
3. Широковещательный B-запрос («З»).
4. Файл LMHOSTS («Л»).
5. Файл HOSTS («Х»).
6. DNS («Д»).

[1] В оригинале фраза выглядела как «Can We Buy Large Hard Drives» — cache, WINS, B-node broadcast, LMHOSTS, HOSTS, DNS. — *Примеч. перев.*

Кэш имен NetBIOS

Кэш имен NetBIOS представляет собой область памяти локального компьютера, в которой он хранит недавно определенные имена NetBIOS и соответствующие им IP-адреса. Каждая запись в кэше имеет свое значение TTL (времени жизни). Чем чаще используется имя из кэша, тем дольше оно в нем остается. Кэш — первое место, в котором Windows NT ищет IP-адрес, соответствующий имени NetBIOS.

Кэш имен также содержит записи из файла LMHOSTS. Записи в файле LMHOSTS, за которыми следует тег #PRE, загружаются в кэш при инициализации системы. Эти записи не имеют времени жизни. Они остаются в кэше до тех пор, пока кэш не будет очищен при помощи команды NBTSTAT -R или до выключения компьютера. Если службы и приложения NetBIOS на вашем компьютере часто осуществляют доступ к какому-либо компьютеру сети, разумно создать для этого компьютера постоянную запись в кэше.

Команда NBTSTAT имеет следующий синтаксис:

```
NBTSTAT [-a имя_узла] [-A IP-адрес] [-c] [-n] [-r]
[-R] [-s] [-S] [интервал]
```

Эта команда позволяет вам просматривать записи в кэше имен NetBIOS локального компьютера и манипулировать ими, а также просматривать таблицы имен на удаленных узлах. Параметры этой команды описаны в табл. 10.1.

Таблица 10.1. Параметры команды NBSTAT

Параметр	Описание
-a	Вывод таблицы имен удаленного узла; узел задается именем
-A	Вывод таблицы имен удаленного узла; узел задается IP-адресом
-c	Вывод кэша имен удаленного узла; узел задается IP-адресом
-n	Вывод локальных имен NetBIOS
-r	Вывод списка имен, определенных при помощи широковещательных запросов и при помощи обращений к серверу WINS
-R	Удаление всех записей из кэша с последующей перезагрузкой постоянных записей
-S	Вывод таблицы сеансов для данного IP-адреса
-s	Вывод таблицы сеансов, с преобразованием IP-адресов в имена узлов при помощи файла HOSTS
имя_узла	Имя удаленного узла
IP-адрес	IP-адрес в десятичной записи
Интервал	Непрерывный вывод указанной статистики через указанный интервал. Для прекращения работы нажмите Ctrl+C

WINS

Если узел не в состоянии определить имя NetBIOS, используя локальный кэш имен NetBIOS, и он настроен на использование хотя бы одного сервера WINS, то этот узел отправляет запрос на определение имени непосредственно серверу WINS.

Сервер WINS производит в своей базе данных поиск IP-адреса, соответствующего запрашиваемому имени NetBIOS. Если IP-адрес найден, то сервер отправляет его запрашивавшему узлу, который затем вносит его в свой локальный кэш имен NetBIOS. Если сервер WINS не находит требуемого адреса, то он сообщает об этом запрашивавшему узлу, и тот переходит к следующему шагу в определении имени NetBIOS.

Широковещательный B-запрос

Локальный узел отправляет в локальную сеть широковещательный B-запрос, если попытка определения имени NetBIOS при помощи сервера WINS не удалась. Каждый узел NetBIOS в локальной сети обрабатывает этот запрос, сравнивая имя NetBIOS в запросе с собственным. Если узел обнаруживает, что он использует запрашиваемое имя NetBIOS, он сообщает запрашивающему узлу свой IP-адрес.

Этот шаг в процессе определения имени NetBIOS обычно производится *после* попыток определения имени NetBIOS при помощи локального кэша имен и сервера WINS, поскольку сетевые широковещательные сообщения снижают пропускную способность сети и их обработка занимает процессорное время всех компьютеров. Поэтому широковещательные сообщения обычно распространяются в пределах локального сегмента сети и не пропускаются далее маршрутизаторами. Большинство маршрутизаторов не пропускают в другие сегменты широковещательные запросы на регистрацию, определение или освобождение имен NetBIOS. Для того чтобы такие сообщения проходили через маршрутизатор, он должен быть настроен на маршрутизацию пакетов на UDP-портах 137 и 138.

Вы можете использовать команду NBTSTAT -r для того, чтобы увидеть, какое количество имен NetBIOS определено при помощи широковещательных запросов и какое — при помощи WINS. Не путайте строчную r и прописную R! Параметр -r предназначен для вывода определенных имен, а -R вызывает очистку кэша.

Внимание

Познакомьтесь с различными функциями команды NBTSTAT. Хорошее знание этой команды и ее параметров необходимо для успешной сдачи экзамена.

Файл LMHOSTS

Если все перечисленные выше методы определения имени NetBIOS не привели к успеху, производится поиск в локальном файле LMHOSTS (если, конечно, компьютер настроен на его использование).

Файл LMHOSTS представляет собой обычный текстовый файл, подобный файлу HOSTS и используемый для определения IP-адресов, соответствующих именам NetBIOS. Файл LMHOSTS должен находиться в каталоге *systemroot*\system32\drivers\etc; вы можете найти в этом каталоге пример файла LMHOSTS под именем LMHOSTS.SAM. Файл LMHOSTS *содержит в каждой строке IP-адрес и имя NetBIOS, отделенное от IP*-адреса не менее чем одним пробелом. Кроме того, такие записи могут иметь специальное значение, если в конце строки есть один или несколько специальных тегов. Например, одна из строк файла LMHOSTS может выглядеть так:

```
192.168.0.1     BONGO       #PRE        #DOM:RESOURCE
```

Эта строка описывает имя NetBIOS BONGO. Тег #PRE указывает, что эта запись должна быть помещена в кэш имен NetBIOS при загрузке системы и находиться там постоянно. Тег #DOM, следующий далее, означает, что BONGO является контроллером домена RESOURCE.

В табл. 10.2 приведен список допустимых тегов, которые могут использоваться в файле LMHOSTS, и их значение.

Таблица 10.2. Теги, которые могут использоваться в файле LMHOSTS

Тег	Описание
#	Указывает, что далее в этой строке следует комментарий
#PRE	Указывает, что соответствующая запись должна быть помещена в кэш при загрузке системы
#DOM:имя_домена	Обозначает контроллер домена
#INCLUDE	Используется для указания файлов LMHOSTS на других узлах сети. Это позволяет централизованно поддерживать один файл LMHOSTS и использовать его на узлах сети.
#BEGIN_ALTERNATE	Используется для группировки нескольких тегов #INCLUDE
#END_ALTERNATE	Используется для указания конца блока, начатого тегом #BEGIN_ALTERNATE
#MH	Этот тег позволяет связать одно имя NetBIOS *с несколькими IP-адресами; используется для систем* с несколькими сетевыми интерфейсами.
#SG	Этот тег позволяет создавать специальные группы аналогично тегу #DOM

Файл LMHOSTS читается по одной строке от начала к концу до тех пор, пока не будет найдено нужное имя NetBIOS или пока не будет достигнут конец файла. Поэтому лучше иметь в этом файле как можно меньше строк. Чем меньше строк должно быть прочитано, тем быстрее будет идти процесс определения имен.

В связи с этим не стоит в качестве файла LMHOSTS использовать файл LMHOSTS.SAM с небольшими исправлениями. Этот файл, как вы увидите ниже, содержит множество комментариев и пояснений. Каждый из этих комментариев будет прочитываться системой при определении имен NetBIOS.

Вы должны разместить все строки, содержащие тег #PRE, ближе к концу файла LMHOSTS, поскольку эти записи постоянно содержатся в кэше имен NetBIOS после загрузки системы; нет необходимости читать их из файла каждый раз при определении имен — это будет только замедлять процесс. Если вы разместите такие записи в конце файла, то все другие записи будут читаться до того, как начнется чтение ненужных записей с тегом #PRE.

Давайте рассмотрим часть файла LMHOSTS.SAM[1]:

```
# Copyright (c) 1993-95 Microsoft Corp.
#
# Это - пример файла LMHOSTS, используемого
# Microsfot TCP/IP для Windows NT.
#
# Этот файл содержит соответствия между IP-адресами
# и Windows NT именами (именами NetBIOS). IP-адрес
# должен начинаться с первого символа строки;
# за ним должно быть помещено соответствующее
# имя компьютера. Адрес и имя
# компьютера должны быть разделены
# как минимум одним пробелом или
# символом табуляции. Символ "#"
# используется для обозначения начала комментария;
# исключения указаны ниже.

# Этот файл совместим с файлами Microsoft LAN
# Manager 2.x TCP/IP lmhosts и позволяет
# использовать следующие расширения:
#
#     #PRE
#     #DOM:<домен>
#     #INCLUDE <имя_файла>
```

[1] Комментарии в этом файле приведены в русском переводе. — *Примеч. перев.*

```
#       #BEGIN_ALTERNATE
#       #END_ALTERNATE

<Строки из исходного файла удалены>

#
# Ключевые слова #BEGIN_ALTERNATE и #END_ALTERNATE
# позволяют сгруппировать несколько строк #INCLUDE
# в один блок. При успешном включении одного из
# указанных файлов считается успешно
# выполненным весь блок

< Строки из исходного файла удалены>

# 102.54.94.123 popular   #PRE #основной сервер
# 102.54.94.117 localsrv #PRE #необходим для INCLUDE
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE

< Строки из исходного файла удалены>

# Обратите внимание, что при каждом определении
# имени считывается весь файл, включая комментарии,
# поэтому сведите их количество к минимуму для
# увеличения производительности системы. По этой
# причине не рекомендуется просто добавлять новые
# записи в конец этого файла.
```

Вы можете добавить собственные записи, такие как адреса контроллеров доменов, адреса высокопроизводительных рабочих станций, к которым вы часто подключаетесь, или расположение центрального файла LMHOSTS в вашей сети, — в конец этого файла или в новый файл. Вот пример того, как может выглядеть файл LMHOSTS:

```
128.131.98.225 PDC1             #DOM:ACCOUNTS
# Контроллер домена
128.131.98.91  WORKSTATION1   #PRE
# Этот адрес будет автоматически
# помещен в кэш при загрузке
#BEGIN_ALTERNATE
     #INCLUDE \\SERVER8\public\LMHOSTS
     #INCLUDE \\SERVER9\public\LMHOSTS
#END_ALTERNATE
```

Файл HOSTS и DNS

Если не удалось определить имя NetBIOS при помощи одной из служб определения имен NetBIOS, TCP/IP для Windows NT может (если система настроена на это) обратиться к файлу HOSTS и серверу DNS. Это поможет в определении имени NetBIOS только в том случае, если имя узла и его имя NetBIOS совпадают.

Типы запросов NetBIOS на основе TCP/IP

Реализация TCP/IP фирмой Microsoft использует все упомянутые выше методы для определения имен NetBIOS и, как правило, именно в том порядке, в котором они обсуждались в этой главе. Однако последовательность может изменяться в зависимости от настройки конкретного компьютера.

В следующих разделах мы обсудим различные комбинации методов определения имен, которые может использовать Microsoft TCP/IP.

B-запрос

B-запрос[1] использует широковещательные сообщения в локальной сети для регистрации, поиска и освобождения имен. Если узел не может быть найден в кэше имен NetBIOS или достигнут при помощи широковещательного сообщения в локальной сети, имя NetBIOS не может быть определено. Этот метод фактически не требует настройки для правильной работы, но создает значительный трафик в сети.

Улучшенный B-запрос

Это конфигурация по умолчанию Windows-компьютеров, *не* настроенных на использование WINS для определения имен NetBIOS. Улучшенный B-запрос является измененной версией B-запроса и позволяет компьютеру проверить локальный файл LMHOSTS, если широковещательный запрос не помог определить имя NetBIOS.

P-запрос

Службы P-запроса[2] при использовании служб имен NetBIOS целиком полагаются на связь типа «точка-точка». Если имя NetBIOS не найдено в кэше, этот метод определения имен требует от клиента установления непосредственного соединения с сервером имен NetBIOS

[1] Broadcast — широковещательный. — *Примеч. перев.*

[2] Point — точка. — *Примеч. перев.*

(обычно — с сервером WINS). Этот метод определения имен сильно снижает широковещательный трафик в сети, но не обеспечивает отказоустойчивости на случай сбоя в работе сервера WINS.

M-запрос

M-запрос[1], еще называемый смешанным запросом, является комбинацией B-запроса и P-запроса. Сначала производится проверка кэша имен. Если имя не найдено в кэше, узел отправляет широковещательный B-запрос в локальную сеть. Если это не помогает определить имя NetBIOS, узел отправляет запрос непосредственно серверу WINS (серверу имен NetBIOS).

Этот метод определения имен обеспечивает некоторую избыточность, но он не позволяет снизить широковещательный трафик в сети. Компьютер, использующий M-запрос, всегда отправляет широковещательный запрос перед тем, как отправить запрос серверу WINS.

H-запрос

По умолчанию Windows или Windows NT, настроенная на использование сервера WINS, использует H-запрос[2]. H-запрос использует и широковещательные сообщения, и непосредственное соединение с сервером для определения имен WINS, — как и M-запрос, но в обратном порядке.

Узел, использующий H-запрос, сначала проверяет кэш имен NetBIOS. Если имя не найдено в кэше, узел отправляет запрос серверу WINS. Если сервер WINS не может определить имя WINS, отправляются до трех широковещательных запросов в локальную сеть. Компьютер может быть настроен так, чтобы при неудаче в определении имени методом широковещательных запросов выполнялась проверка файла LMHOSTS и/или файла HOSTS, а также отправлялся запрос серверу DNS.

Такой метод определения имен является наиболее предпочтительным, поскольку сервер WINS, обращение к которому отправляется до того, как будет произведен широковещательный запрос, обычно имеет нужную информацию. Это позволяет значительно уменьшить объем широковещательного трафика в сегментах сети. Если, по каким-либо причинам, сервер WINS недоступен или не в состоянии определить имя, узел может использовать широковещательный запрос и файл LMHOSTS для определения имени.

---

[1] Mixed — смешанный. — *Примеч. перев.*

[2] Hybrid — гибридный. — *Примеч. перев.*

Использование NetBIOS на основе TCP/IP для просмотра сети

Windows NT имеет возможность просматривать сетевые ресурсы. Просмотр позволяет определить наличие ресурсов NetBIOS в сети и использовать их впоследствии, не имея изначально информации об их расположении.

Просмотр возможен, поскольку NetBIOS обычно размещает списки просмотра для каждой сети на специальном компьютере, называемом сервером просмотра (master browser). Список просмотра представляет собой список доступных сетевых ресурсов NetBIOS для конкретного сегмента сети. Каждый сегмент сети имеет свой сервер просмотра или резервный сервер просмотра (local backup browser), поддерживающий список просмотра для данного сегмента. Эти серверы отправляют списки просмотра через регулярные интервалы основному серверу просмотра домена. Основной контроллер домена (PDC) чаще всего является основным сервером просмотра для своего домена. Этот компьютер отвечает за объединение списков, полученных от серверов просмотра отдельных сегментов, в один список просмотра. Полученный список затем пересылается резервному серверу просмотра каждого сегмента. Таким образом, каждый локальный или резервный сервер просмотра владеет списком всех доступных на настоящий момент ресурсов NetBIOS во всей сети.

Каждый сервер просмотра определяется при помощи процесса, называемого выборами. Выборы в сети могут происходить в различное время. Победитель выборов определяется исходя из версии и типа операционной системы, используемой на компьютере. Обычно победителем является компьютер, использующий последнюю версию программного обеспечения, поскольку такой компьютер имеет больше сведений о работе с различными операционными системами, которые могут встретиться в сети. Например, Windows NT Workstation 4 выиграет у Windows 95, а Windows NT Server 3.51 проиграет Windows NT Server 4.0.

Предыдущий пример предполагает возможность передачи информации через маршрутизаторы. В сетях Windows существует несколько способов обойти ограничение NetBIOS на работу в одном локальном сегменте. WINS, файл LMHOSTS, специально настроенные маршрутизаторы могут обеспечивать использование службы имен NetBIOS в маршрутизируемом доменном окружении.

WINS позволяет каждому узлу NetBIOS в маршрутизируемой сети регистрировать и определять имена при помощи непосредственных

запросов по типу «точка-точка». Каждый компьютер регистрирует себя на сервере WINS при инициализации TCP/IP, и каждый узел или сервер просмотра может непосредственно обратиться к серверу WINS. Поскольку эти запросы отправляются на конкретный IP-адрес, то наличие маршрутизаторов не играет никакой роли.

Файл LMHOSTS может использоваться сервером просмотра (контроллером домена) каждой подсети для определения IP-адреса основного сервера просмотра домена при отправке ему списков просмотра. Основной сервер просмотра домена затем посылает общий список ресурсов NetBIOS локальным серверам просмотра. Этот направленный обмен информацией не зависит от наличия или отсутствия маршрутизаторов.

Наконец, в небольшой маршрутизируемой сети, содержащей ограниченное количество узлов NetBIOS, маршрутизаторы могут быть настроены на ретрансляцию пакетов NetBIOS, Это фактически позволяет всем узлам работать так, как если бы они находились в одной локальной сети. Однако в больших сетях такой подход вызовет падение производительности сети.

Разрешение проблем с именами NetBIOS

Первый шаг в разрешении проблемы в системе определения имен NetBIOS — убедиться, что проблема связана именно с определением имен. Другими словами, следует убедиться, что проблема связана не с просмотром.

То, что компьютер или ресурс не может быть найден в локальном списке просмотра — таком, как Network Neighbourhood, — еще не означает, что узел недоступен или что существует проблема в определении соответствующего имени. Возможно, просто резервный сервер просмотра в одном из сегментов сети временно неисправен, что приводит к появлению ошибочного списка просмотра для всей сети.

Когда компьютер включается и загружает операционную систему, он анонсирует свое появление в сети. Изначально эти анонсы отправляются в сеть каждую минуту, потом их частота постепенно снижается до одного раза в двенадцать минут. Эти сообщения используются сервером просмотра для определения того, что ресурс еще доступен. Сервер просмотра поддерживает список ресурсов для компьютера, пока тот не пропустит три очередных объявления. Это позволяет скомпенсировать возможные сбои в сети. Итак, после того как компьютер включен и проработал значительное время, а потом был отключен от сети, его ресурсы останутся в списке сервера просмотра

еще 36 минут. Резервные серверы просмотра опрашивают основной сервер просмотра домена каждые 15 минут. Следовательно, отказавший ресурс может находиться в списках ресурсов резервных доменов до 51 минуты.

Быстрее всего можно определить природу проблемы, попытавшись подключить желаемый ресурс, используя UNC ресурса, а не Network Neighbourhood. Например, попробуйте непосредственно подключить ресурс \\TOTO\kansas вместо того, чтобы искать его в Network Neighbourhood.

Если вы не в состоянии получит доступ к ресурсу и таким образом, то попробуйте использовать утилиту PING, указав IP-адрес компьютера, с которым вы хотите соединиться, чтобы убедиться, что он работает и подключен к сети. Если вы получаете ответ, переходите к определению того, какая часть процесса определения имен работает неверно.

Если ваш компьютер настроен на использование сервера WINS, но не использует файл LMHOSTS и вы пытаетесь определить имя из другого сегмента сети, попробуйте использовать PING с адресом сервера WINS. Если сервер WINS недоступен по какой-либо причине, то вы должны разрешить использование другого метода определения имен, например файла LMHOSTS.

Если вы используете файл LMHOSTS, то должны проверить, не совершили ли вы одну из часто встречающихся при использовании этого файла ошибок. Имя узла, с которым вы пытаетесь соединиться, может отсутствовать в этом файле, или же IP-адрес узла мог измениться.

Возможно, в файле LMHOSTS содержится более одного соответствия имени данного узла и IP-адреса. Запомните, что в этом случае будет использоваться только первое из них, вне зависимости от того, правильный ли указан в нем IP-адрес. Используйте возможность поиска в вашем текстовом редакторе для устранения повторяющихся записей одного имени NetBIOS в файле LMHOSTS.

Наконец, проверьте, что файл LMHOSTS имеет правильное имя и расположен в правильном каталоге. Многие текстовые редакторы по умолчанию добавляют к имени файла расширение .TXT. Это приводит к тому, что Windows NT не в состоянии открыть файл LMHOSTS, поскольку он имеет имя LMHOSTS.TXT. Кроме того, имя должно быть именно LMHOSTS, а не LMHOST.

Вопросы для подготовки к экзамену

Question 1

You have just received a new Windows NT Workstation and you seem to be having trouble mapping a drive to another Windows NT host that resides on a remote network. Your network does not currently have a WINS server providing NetBIOS name resolution. Which of the following files should you modify to enable Windows NT to correctly resolve the name of the Windows host to which you are trying to connect?

- A. HOSTS
- B. LMHOSTS
- C. HOST
- D. LMHOST

Вопрос 1

Вы только что получили новую Windows NT Workstation, и по всей видимости существуют проблемы при подключении сетевого диска другого Windows NT-узла, находящегося в удаленном сегменте сети. Ваша сеть в настоящий момент не имеет сервера WINS, обеспечивающего определение имен NetBIOS. Какой из следующих файлов вы должны изменить, чтобы Windows NT могла правильно определить IP-адрес удаленного Windows-узла, с которым вы пытаетесь установить соединение?

- A. HOSTS
- B. LMHOSTS
- C. HOST
- D. LMHOST

Правильный ответ на этот вопрос — B. Файл LMHOSTS является тем файлом, который вы должны изменить, чтобы Windows NT могла правильно определить IP-адрес удаленного узла, с которым вы пытаетесь установить соединение. Запомните, что как файл HOSTS, так и файл LMHOSTS могут содержать несколько записей каждый. Поэтому в их названии последняя буква — «S», означающая в английском языке множественное число.

Question 2

Which of the following applications is not a NetBIOS application or command? (Check all correct answers.)

- A. net use \\server2\share1.
- B. Windows NT FTP client.
- C. Windows NT Telnet client.
- D. Windows NT Explorer.

Вопрос 2

Какие из следующих приложений не являются приложениями или командами NetBIOS?

- ❑ A. net use \\server2\share1.
- ❑ B. FTP-клиент Windows NT.
- ❑ C. Telnet-клиент Windows NT.
- ❑ D. Windows NT Explorer.

Правильные ответы на этот вопрос — B и C. FTP и Telnet являются приложениями Windows Sockets. Команда NET и Windows NT Explorer были разработаны для доступа к другим Windows-компьютерам сети, использующим Windows NT Workstation, Server или Windows 95. Следовательно, эти приложения основаны на NetBIOS. Запомните, что TCP/IP-приложения разрабатывались для обеспечения взаимодействия между всеми типами TCP/IP-узлов и используют программный интерфейс Sockets; таковы программы PING, FTP, Telnet и Gopher. Приложения Windows, такие как Windows Explorer, User Manager и команда NET, хотя и позволяют использовать TCP/IP, разрабатывались для обеспечения связи между Windows-платформами и, следовательно, являются приложениями NetBIOS. Этот вопрос помечен как сложный, поскольку вы должны внимательно прочитать его — требуется выбрать приложения, *не являющиеся* приложениями NetBIOS.

Question 3

Mary would like to ensure that each workstation within her department has an updated LMHOSTS file and make sure that each file is in the correct location on the local machine. If Mary adds a new, preloaded (#PRE) NetBIOS name to each LMHOSTS file that she edits, which of the following commands will enable her to test whether or not the file is located in the correct directory and is being used for resolution?

- ○ A. NETSTAT -r, followed by NBTSTAT -d
- ○ B. NBTSTAT -r, followed by NBTSTAT -c
- ○ C. NETSTAT -R, followed by NBTSTAT -d
- ○ D. NBTSTAT -R, followed by NBTSTAT -c

Вопрос 3

Марии нужно убедиться, что каждая рабочая станция в ее отделе имеет обновленный файл LMHOSTS и что этот файл на каждой машине расположен в надлежащем каталоге. Мария добавила новую предзагружаемую (#PRE) запись в каждый из файлов LMHOSTS. Какую команду она может использовать для проверки того, что файл находится в нужном каталоге и используется для определения имен?

- A. NETSTAT -r, потом NBTSTAT -d
- B. NBTSTAT -r, потом NBTSTAT -c
- C. NETSTAT -R, потом NBTSTAT -d
- D. NBTSTAT -R, потом NBTSTAT -c

Правильный ответ на этот вопрос – D. NBTSTAT (утилита NetBIOS) позволяет вам очистить кэш имен NetBIOS, задав параметр -R. После того как кэш имен будет очищен и перезагружен из файла LMHOSTS, вы можете использовать команду NBTSTAT -c (c – cache) для просмотра содержимого кэша имен NetBIOS. Присутствие добавленной предзагружаемой (#PRE) записи в кэше свидетельствует о том, что файл LMHOSTS находится в нужном каталоге и используется для определения имен NetBIOS.

Команда NETSTAT -r не выводит информацию о NetBIOS. Она используется для вывода локальной таблицы маршрутизации (наподобие команды ROUTE print). Параметр -r выводит статистику регистрации и определения имен NetBIOS, а также методов, использованных для определения имен (WINS или широковещательный запрос). Утилита NBTSTAT не имеет документированного параметра -d. Следовательно, ответы, содержащие этот параметр, неверны.

Question 4

You have just taken a job with a company that would like to convert its current network operating system to Windows NT. The company has four subnets on its TCP/IP network, each of which will have its own Backup Domain Controller (BDC), except for the subnet on which the PDC will reside. The company would like to allow browsing across the entire network without needing to implement WINS. How should you modify the LMHOSTS file so that this is possible?

- A. Create an entry in the LMHOSTS file on the PDC for each of the BDCs and use #DOM.
- B. Create an entry in the LMHOSTS file on each BDC for the PDC and use #DOM.
- C. Create a HOSTS file for each subnet on the network and place these files on each client.
- D. This is not possible.

Вопрос 4

Вы получили работу в компании, которая собирается заменить свою сетевую операционную систему на Windows NT. Компания имеет TCP/IP-сеть, состоящую из четырех подсетей, каждая из которых содержит свой собственный резервный контроллер домена (BDC), за исключением подсети, в которой находится основной контроллер домена (PDC). Компания хочет, чтобы был возможен просмотр всей сети без реализации WINS. Как вы должны изменить файл LMHOSTS, чтобы выполнить эти требования?

- A. Создать в файле LMHOSTS на PDC для каждого BDC, используя тег #DOM.
- B. Создать запись в файле LMHOSTS на каждом BDC для PDC, используя тег #DOM.
- C. Создать файл HOSTS для каждой подсети и поместить его на каждый узел сети.
- D. Это невозможно.

Правильный ответ на этот вопрос — B. По умолчанию BDC выбирается сервером просмотра для подсети, если в этой подсети нет PDC. Добавив соответствие между IP-адресом и именем NetBIOS в файл LMHOSTS (и использовав тег #DOM для указания того, что это контроллер домена), вы можете настроить каждый из BDC/серверов просмотра на отправку списка доступных ресурсов основному серверу просмотра домена — PDC. PDC затем объединяет полученные из каждой подсети списки и возвращает созданный список ресурсов всей сети каждому BDC для использования в локальных подсетях. Это позволяет каждой подсети иметь информацию о компьютерах, доступных для просмотра во всей сети компании.

Question 5

Which of the following statements are potential problems that can occur when using the LMHOSTS file? (Check all correct answers.)

- A. The LMHOSTS file is not in the root directory of system drive.
- B. The LMHOSTS file has been saved with an incorrect name or extension.
- C. The entry in question has been misspelled or entered incorrectly.
- D. Two different entries exist for the same NetBIOS name, and the one that occurs first in the list is incorrect.

Вопрос 5

Какие из следующих утверждений описывают потенциальные проблемы, которые могут возникнуть при использовании файла LMHOSTS? (Укажите все верные ответы).

- ❑ A. Файл LMHOSTS не находится в корневом каталоге системного диска.
- ❑ B. Файл LMHOSTS сохранен под неверным именем или имеет неверное расширение.
- ❑ C. Запись в файле написана с ошибкой.
- ❑ D. Существуют две различные записи для одного имени NetBIOS, и та из них, которая встречается первой, неверна.

Правильные ответы — B, C и D. Ответ B верен, поскольку при редактировании файла LMHOSTS возможно сохранить его под неверным именем, например LMHOST, или сохранить его с расширением, например, .SAM или .TXT. Правильное имя этого файла — LMHOSTS. Опечатки и ошибки при вводе часто встречаются при редактировании текстовых файлов, таких как файл LMHOSTS. Следовательно, ответ C также верен. Ответ D верен, поскольку файл LMHOSTS считывается от начала к концу по одной строке. Когда запись, соответствующая нужному имени, найдена, процесс определения имен NetBIOS заканчивается, вне зависимости от того, имеются ли в файле еще записи, соответствующие данному имени. Эта проблема чаще всего возникает в тех случаях, когда должен поддерживаться файл LMHOSTS большого размера. Ответ A неверен, поскольку файл LMHOSTS должен находиться в каталоге %systemroot%\system32\drivers\etc, а не в корневом каталоге диска, содержащего системные файлы.

Question 6

Curtis works for a local state agency that does not use WINS for NetBIOS name resolution. Instead, each client on the network copies a master LMHOSTS file from a central server during the logon process. After having a number of problems with the current PDC (MIS4) of the HR domain, Curtis decides to promote one of the BDCs (Payroll2) to PDC status and take the former PDC offline. What change must Curtis make to the master LMHOSTS file in order for each client to be able to contact the new PDC?

- ○ A. 128.131.24.122 #PRE Payroll2 #DOMAIN: HR
- ○ B. 128.131.24.122 HR: #DOM #PRE
- ○ C. 128.131.24.122 Payroll2 #PRE #DOM: HR
- ○ D. 128.131.24.122 Payroll2 #DOM

Вопрос 6

Николай работает в муниципальном учреждении, в сети которого не используется WINS для определения имен NetBIOS. Вместо этого каждый клиент копирует файл LMHOSTS с центрального сервера в течение процесса входа в сеть. После многократного устранения неполадок, возникающих на существующем PDC (MIS4, домен HR), Николай решил перевести один из существующих BDC (Payroll2) в статус PDC, а прежний PDC отключить. Какие изменения Николай должен произвести в главном файле LMHOSTS, чтобы каждый клиент мог взаимодействовать с новым PDC?

- A. 128.131.24.122 #PRE Payroll2 #DOMAIN:HR
- B. 128.131.24.122 HR:#DOM #PRE
- C. 128.131.24.122 Payroll2 #PRE #DOM:HR
- D. 128.131.24.122 Payroll2 #DOM

Правильный ответ на этот вопрос — C. Основной файл LMHOSTS должен содержать соответствие между IP-адресом и именем NetBIOS для компьютера, который будет новым PDC. Однако эта запись в файле LMHOSTS должна содержать тег #DOM для указания того, что данный компьютер является основным контроллером домена. Тег #PRE необязателен — он позволяет указать, что данная запись должна постоянно находиться в кэше имен NetBIOS. Ответ A неверен, поскольку имя компьютера должно следовать сразу после его IP-адреса. Ответ B неверен, поскольку не задано имя компьютера и имя домена помещено перед тегом #DOM, а не после него. Ответ D также неверен (хотя очень похож на правильный — в этом заключается сложность вопроса), поскольку в нем не указано имя домена, контроллером которого является Payroll2.

Question 7

The following are the first four steps of the NetBIOS name resolution process:

1. b-node broadcast
2. WINS
3. NetBIOS name cache
4. LMHOSTS

Which of the following options places these steps in the correct (default or hybrid node) order?

- A. 3, 2, 1, 4
- B. 3, 1, 4, 2
- C. 2, 3, 1, 4
- D. 1, 2, 3, 4

Вопрос 7

Ниже приведены четыре первых шага процесса определения имен NetBIOS:

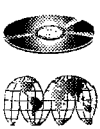
1. Широковещательный B-запрос
2. WINS
3. Кэш имен NetBIOS
4. LMHOSTS

В каком порядке по умолчанию выполняются эти шаги?

- A. 3, 2, 1, 4
- B. 3, 1, 4, 2
- C. 2, 3, 1, 4
- D. 1, 2, 3, 4

Правильный ответ на этот вопрос — A. По умолчанию Windows NT, настроенная на использование как минимум, основного сервера WINS, применяет H-запрос. Это означает, что сначала производится проверка кэша имен NetBIOS, а затем отправляется запрос серверу WINS. Если сервер WINS не может определить запрашиваемое имя, исходный узел отправляет широковещательный B-запрос в локальную сеть для того, чтобы обнаружить компьютер, владеющий данным именем. Если на этот запрос не получено ответа, то производится поиск в файле LMHOSTS (если компьютер настроен на его использование).

Дополнительная информация



Произведите поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевые слова «NetBIOS Name Resolution», «NetBIOS names», «LMHOSTS and 4.0», «NetBIOS name cache» и «WINS».

Протокол динамической конфигурации узла (DHCP)

Термины, необходимые для понимания материала:

- DHCP-аренда
- DHCP-ретрансляция
- Контекст DHCP
- Зарезервированный клиент

Приемы и знания, которыми вы должны овладеть:

- Понимание процесса DHCP-аренды
- Понимание процесса продления аренды
- Понимание того, как DHCP-ретрансляция используется в маршрутизируемых сетях

Протокол динамической конфигурации узла (DHCP) был разработан для того, чтобы устранить очевидный недостаток TCP/IP: отсутствие возможности централизованного управления IP-адресами. DHCP является расширением протокола BOOTP, который использовался ранее для динамического выделения IP-адресов. В этой главе мы обсудим роль DHCP в настройке узлов и управлении сетью, а также то, что вам потребуется о нем знать на экзамене.

DHCP: исследованный и объясненный

DHCP был разработан IETF (Internet Engineering Task Force) для того, чтобы обеспечить надежный метод динамического выделения IP-адресов, который бы позволил упростить начальную настройку клиентских компьютеров и снизить нагрузку на администратора сети. DHCP полностью описан в RFC 1533, RFC 1534, RFC 1541 и RFC 1542; он обеспечивает автоматическую установку IP-адреса и маски подсети, а также может передавать адрес шлюза по умолчанию и адреса одного или нескольких серверов DNS или WINS.

DHCP контролируется сервером DHCP, который выполняет запросы клиентов и отвечает за то, чтобы в сети не было повторяющихся IP-адресов. В сети может содержаться неограниченное количество серверов DHCP, однако, если используется более одного сервера, каждому серверу должен быть выделен свой список IP-адресов. Если эти списки совпадают или перекрываются, то опасность появления в сети совпадающих IP-адресов сводит на нет все преимущества DHCP.

На первый взгляд, DHCP может показаться простейшим способом настройки клиентов, однако имеются некоторые подводные камни. В табл. 11.1 указаны положительные и отрицательные стороны реализации DHCP.

Таблица 11.1. DHCP: плюсы и минусы

Плюсы	Минусы
Легко реализуем	Трудно отследить, какому компьютеру принадлежит какой адрес
Централизованная настройка снижает количество возможных ошибок	Крайне сложно реализуем при наличии брандмауэров
Компьютеры могут перемещаться	Пользователи с новыми компьютерами могут вручную настроить системы, выбрав адрес, который был выделен динамически
Входит в состав большинства операционных систем Microsoft	Не *все* операционные системы поддерживаются

DHCP: аренда и ее продление

Когда клиент для своей настройки использует DHCP, он арендует у сервера IP-адрес на определенное время, подобно аренде помещения. Когда вы подписываете договор на аренду помещения, вы получаете право использовать его в течение определенного периода времени. Когда срок аренды подходит к концу, вы можете либо продлить аренду, либо сообщить о том, что вы освободите помещение по истечении срока. DHCP-аренда работает примерно так же. Когда срок аренды IP-адреса подходит к концу, клиент может продлить аренду — как это происходит, мы обсудим ниже. Процесс аренды IP-адреса состоит из четырех шагов.

На первом шаге, называемом «запрос аренды», клиент отправляет широковещательное сообщение в сеть. Поскольку клиент еще не имеет собственного IP-адреса, в пакете указан адрес 0.0.0.0 в качестве адреса отправителя и адрес 255.255.255.255 в качестве адреса получателя. Отправляемый пакет называется DHCP-запросом и содержит имя NetBIOS клиента, которое будет использовано на втором шаге. Если сервер DHCP не отвечает, клиент повторяет широковещательное сообщение три раза, через интервалы в 9, 13 и 16 секунд. Если ответ все еще не получен, клиент начинает повторять DHCP-запросы каждые 5 минут до тех пор, пока не получит ответ. Пока ответ не получен, инициализация TCP/IP не завершена и взаимодействие с другими TCP/IP-узлами невозможно.

Второй шаг называется «предложением аренды». На этом шаге серверы DHCP, имеющие свободные IP-адреса, отвечают на широковещательный запрос клиента. Отправляемые ими пакеты содержат IP-адрес и маску подсети, которые клиент может использовать, период аренды (в часах) и IP-адрес сервера. Когда сервер делает предложение, он временно резервирует адрес, чтобы не предложить его другому узлу, избегая отправки одинаковых адресов различным клиентам.

Следующий шаг называется «выбором аренды». Название немного неточно, поскольку клиент просто принимает первое полученное им предложение, после чего отправляет подтверждение. Это широковещательное сообщение не содержит информации об IP-адресе отправителя, но содержит адрес сервера DHCP, предложение которого принято. Все другие серверы DHCP при этом отменяют сделанные ими предложения.

Последний шаг называется «подтверждением аренды». Если все идет по плану, сервер выделяет клиенту данный IP-адрес и отправляет DHCPACK-сообщение (подтверждение) клиенту, после чего клиент устанавливает полученную им информацию об IP-адресе. Однако иногда сервером отправляется сообщение DHCPNACK (отказ в под-

тверждении) — например, если клиент запрашивает свой старый IP-адрес, но он уже был выделен кому-то еще.

Итак, вы получили в аренду IP-информацию. Что теперь с ней делать? И, более важно, что делать, когда срок аренды подойдет к концу? Ну, все не так плохо, как вы могли подумать. Поскольку клиент не хочет менять настройки, когда истекает 50 процентов срока аренды, он отправляет DHCP-запрос на аренду серверу DHCP. Если сервер DHCP доступен и не имеет причин отказать в выполнении запроса, он отвечает подтверждением аренды, обновляя настройки и переустанавливая время аренды. Однако, если по каким-либо причинам сервер не в состоянии удовлетворить запрос, он отправляет сообщение о том, что аренда не будет продлена. Ничего страшного: у клиента остается 50 процентов срока аренды, чтобы еще раз попытаться продлить аренду, — что он и делает, когда истекает 87,5 процентов срока. В отличие от запроса, отправляемого по истечении половины срока аренды, на этот запрос может ответить любой сервер DHCP. Однако если клиент не получает сообщения DHCPACK от сервера, то весь процесс получения аренды начинается сначала.

Как вы понимаете, иногда аренда прекращается. Однако в наиболее логичный момент — когда клиентский компьютер выключается, — этого не происходит, поскольку компьютер попытается возобновить аренду того же адреса при повторном включении. Если клиентский компьютер выключен и время аренды истекло, аренда прекращается и сервер DHCP снова может использовать данный IP-адрес. Аренда также может быть прекращена пользователем вручную при помощи команды `IPCONFIG /RELEASE`, которая будет обсуждаться ниже в разделе «Утилита IPCONFIG».

Планирование и реализация DHCP в вашей сети

Как мы упоминали в начале главы, использование DHCP связано с некоторыми проблемами. Ниже приведен список вопросов, ответы на которые вы должны знать, чтобы использовать DHCP в вашей сети.

- **Сколько клиентов будет использовать DHCP?** Это важный вопрос, от ответа на который зависит конфигурация и производительность сервера. Microsoft рекомендует использовать не менее двух серверов DHCP, настроенных на резервирование друг друга. Если один из серверов выйдет из строя, работа сети не остановится.
- **Какую операционную систему будут использовать клиенты?** Почти все операционные системы Microsoft поддерживают DHCP, включая Windows 3.5x и выше, Windows 95, Windows for Work-

groups (с TCP/IP-32), LAN Manager 2.2 (для DOS, но не для OS/2) и Microsoft Network Client 3.0 для DOS.

- **Будет ли использоваться DHCP для назначения адресов шлюза по умолчанию, сервера DNS или WINS?** Прежде чем начать установку DHCP в сети, вы должны знать, какая информация будет распространяться сервером DHCP.
- **Сколько подсетей будут использовать DHCP?** Если все клиенты, которые будут использовать DHCP, находятся в одной подсети, настройка сервера несложна; однако, если сервер обслуживает несколько подсетей, требуется также произвести настройку маршрутизаторов.
- **Вовлечены ли в процесс маршрутизаторы, и если да, то могут ли они производить ретрансляцию широковещательных BOOTP-сообщений?** Если маршрутизаторы не имеют возможности ретрансляции BOOTP-сообщений, то вы должны поместить отдельный сервер DHCP в каждую подсеть.

Примечание

Запомните, что DHCP основан на BOOTP. Маршрутизаторы настраиваются не на поддержку DHCP, а на поддержку протокола BOOTP, на котором основан DHCP.

Установка

Любой Windows NT Server, не являющийся DHCP-клиентом, может быть сервером DHCP. Установка службы DHCP замечательно проста и использует ту же процедуру, что и установка всех других компонен-

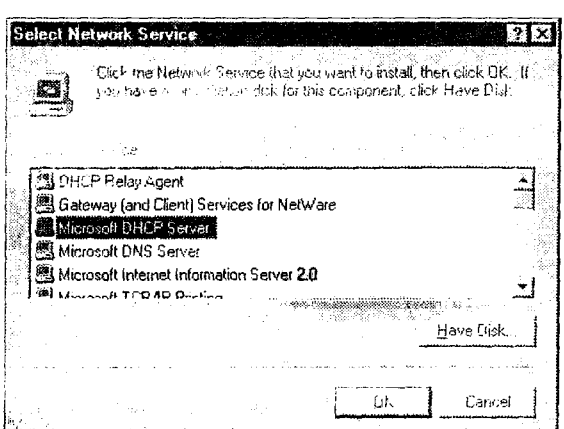


Рис. 11.1. Выберите Microsoft DHCP Server из списка доступных служб

тов Windows NT Server. В окне Control Panel дважды щелкните на значке Network, откройте вкладку Services и нажмите кнопку Add. Появится список доступных служб, как показано на рис. 11.1. Выберите Microsoft DHCP Server и нажмите кнопку OK.

Вам будет предложено ввести путь к файлам Windows NT Server. Введите путь и нажмите кнопку Continue. После этого Windows NT произведет копирование нужных файлов. Появится окно диалога, сообщающее вам, что для всех сетевых адаптеров, использовавших ранее DHCP, нужно указать статический IP-адрес (рис. 11.2).

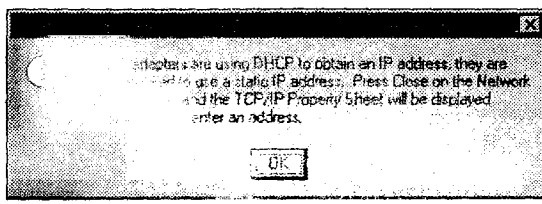


Рис. 11.2. Для интерфейсов сервера DHCP должны быть указаны статические IP-адреса

Нажмите кнопку Close, чтобы завершить копирование файлов. Для того чтобы служба DHCP начала работу, вы должны перезагрузить компьютер; нажмите кнопку Yes для того, чтобы перезагрузить компьютер немедленно. После завершения перезагрузки, для того чтобы DHCP начал выполнять запросы, требуется настроить контекст DHCP. Оставшаяся настройка DHCP обсуждается далее в этой главе.

DHCP-ретрансляция

Если ваша сеть содержит маршрутизаторы между сервером DHCP и DHCP-клиентами, эти маршрутизаторы должны иметь возможность ретрансляции DHCP- (BOOTP-) пакетов. Эта возможность часто называется просто DHCP-ретрансляцией, и ее наличие или отсутствие сильно влияет на процесс настройки DHCP.

Внимание

DHCP-ретрансляция часто встречается в вопросах экзамена Microsoft. Запомните: для того чтобы DHCP-ретрансляция работала, маршрутизатор должен быть настроен на ретрансляцию BOOTP-пакетов.

Не удивительно, что компьютер под управлением Windows NT 4 может работать в качестве агента ретрансляции DHCP. Чтобы разрешить эту возможность, откройте вкладку DHCP relay в окне TCP/IP Properties (рис. 11.3) и укажите IP-адреса одного или нескольких серверов DHCP.

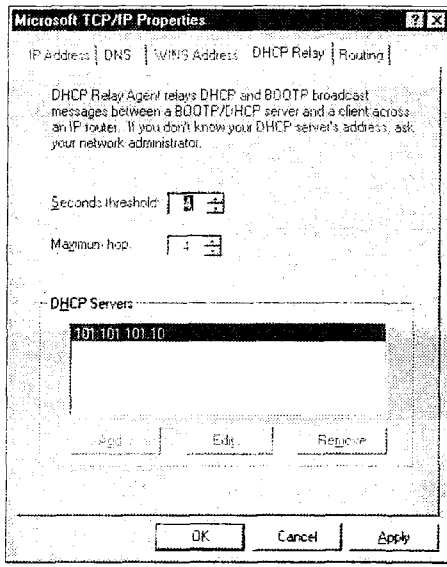


Рис. 11.3. Настройка DHCP-ретрансляции

Контекст

Контекст DHCP — это блок IP-адресов, которые сервер может назначать клиентам. Сервер DHCP должен иметь как минимум один контекст. На рис. 11.4 показано окно Create Scope, одно из окон DHCP Manager.

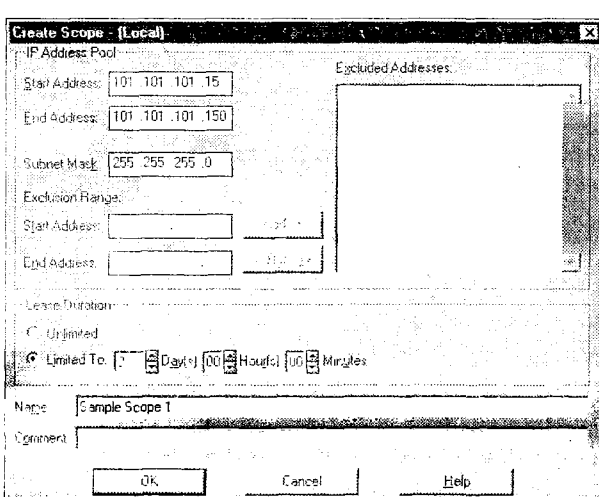


Рис. 11.4. DHCP Manager: окно Create Scope

Чтобы создать контекст, запустите DHCP Manager, находящийся в разделе Administrative Tools (Common) меню Start, выберите сервер DHCP, для которого вы хотите создать контекст, и затем выберите в меню Scope команду Create. После ввода информации в окне Create Scope нажмите кнопку OK. Вам будет задан вопрос — хотите ли вы активировать контекст; нажмите кнопку Yes. После этого контекст будет помечен значком: желтой светящейся лампочкой, указывающей, что он активирован.

Параметры контекста

Каждый созданный контекст имеет некоторое количество параметров, которые можно установить при помощи меню DHCP Options в окне DHCP Manager, как показано на рис. 11.5.

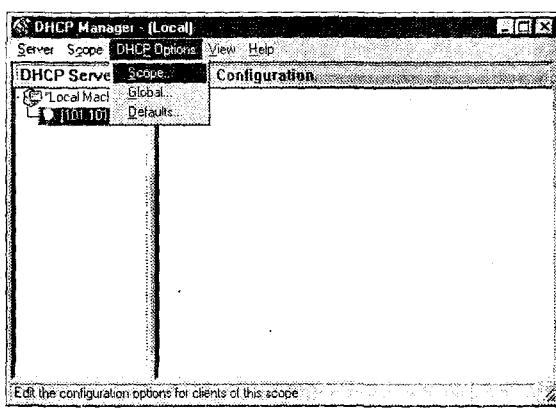


Рис. 11.5. Параметры контекста DHCP устанавливаются при помощи DHCP Manager

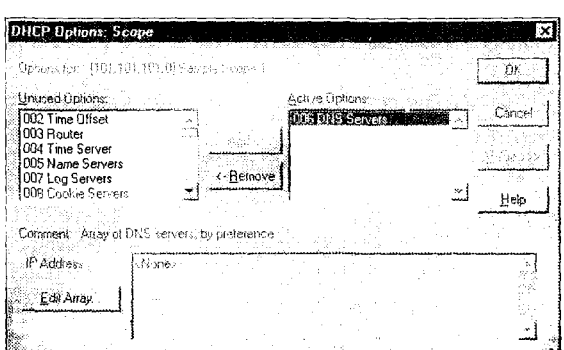


Рис. 11.6. Параметры контекста DHCP

Эти параметры определяют настройки, передаваемые клиенту при выполнении DHCP-запроса. Например, для того чтобы передавать для определенного контекста адрес сервера DNS, выберите в списке «006 DNS Servers» и нажмите кнопку Add для активации этого параметра. Нажмите кнопку Value, чтобы вывести нижнюю часть окна (рис. 11.6).

Для того чтобы ввести адреса серверов DNS, нажмите кнопку Edit Array. Откроется окно, показанное на рис. 11.7.

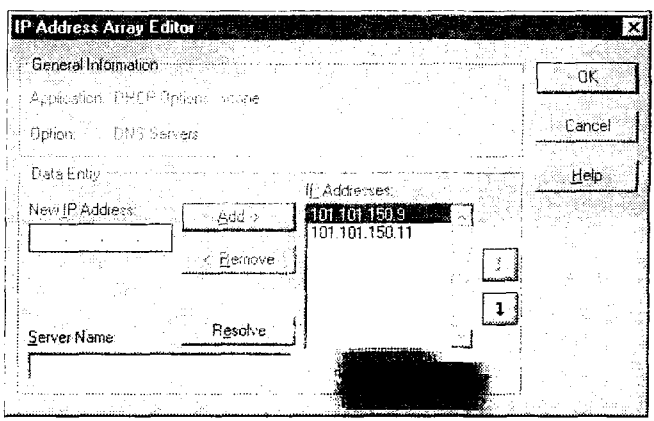


Рис. 11.7. Адреса серверов DNS, передаваемые DHCP-клиентам, настраиваются при помощи установки параметров контекста

Глобальные параметры

Глобальные параметры сервера DHCP совпадают с доступными параметрами контекста; однако эти параметры, как следует из их названия, *глобальные*. Каждый клиент, вне зависимости от контекста, получит информацию, указанную при помощи этих параметров. Обратите внимание, что параметры контекста имеют приоритет над глобальными параметрами.

Резервирование клиентов

Иногда определенный адрес должен быть зарезервирован для определенного клиента, например, если клиент работает через брандмауэр. Если установлено резервирование клиента, то этот клиент, когда бы он ни обратился с DHCP-запросом, получает один и тот же IP-адрес. На рис. 11.8 показано окно Add Reserved Clients, которое можно открыть из DHCP Manager, выделив контекст и выбрав из меню Scope команду Add Reservations.

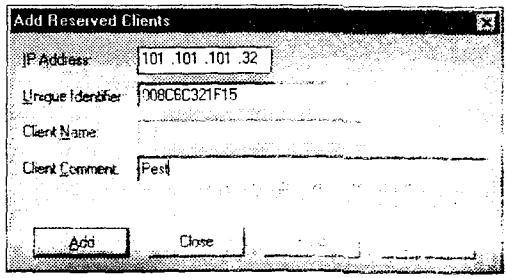


Рис. 11.8. Резервирование клиентов позволяет всегда присваивать определенному клиенту один и тот же адрес

Поле Unique Identifier — это то, что позволяет работать механизму резервирования клиентов. В этом поле должен быть указан аппаратный адрес сетевой карты клиента. Неправильная установка этого значения может привести к неверной работе резервирования клиентов, поэтому будьте внимательны при вводе адреса. Если вы сомневаетесь, используйте команду IPCONFIG /ALL на клиенте, для того чтобы определить его аппаратный адрес. Если в сети имеется несколько серверов DHCP, на вех серверах должна быть установлена одинаковая информация о резервировании клиентов.

Утилита IPCONFIG

Утилита IPCONFIG может быть запущена на любом Microsoft-клиенте (для Windows 95 введите winipcfg). Она выводит ценную информацию, а также позволяет вручную продлевать или прекращать DHCP-аренду. На рис. 11.9 показан вывод утилиты IPCONFIG по умолчанию.

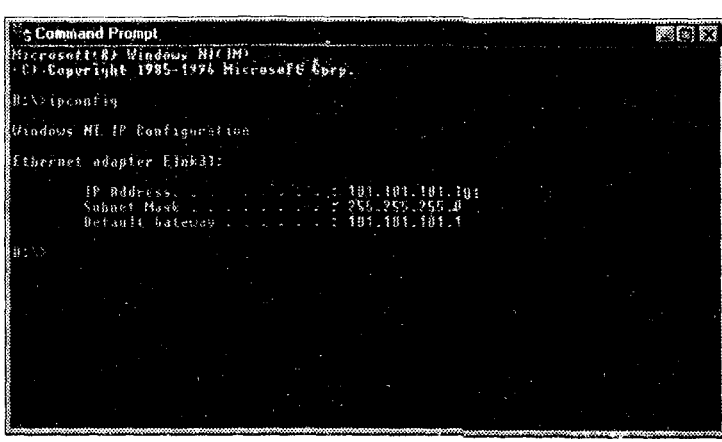


Рис. 11.9. По умолчанию IPCONFIG выводит только IP-адрес, маску подсети и шлюз по умолчанию для данного сетевого адаптера

Однако вы можете вывести при помощи IPCONFIG более подробную информацию, использовав ключ /ALL. Этот ключ позволяет для каждого сетевого интерфейса, помимо выводимой по умолчанию информации, получить еще и имя узла, адреса серверов DNS, тип запроса NetBIOS, используется ли для данного интерфейса DHCP, а также аппаратный адрес интерфейса. Пример вывода команды IPCONFIG/ALL показан на рис. 11.10.

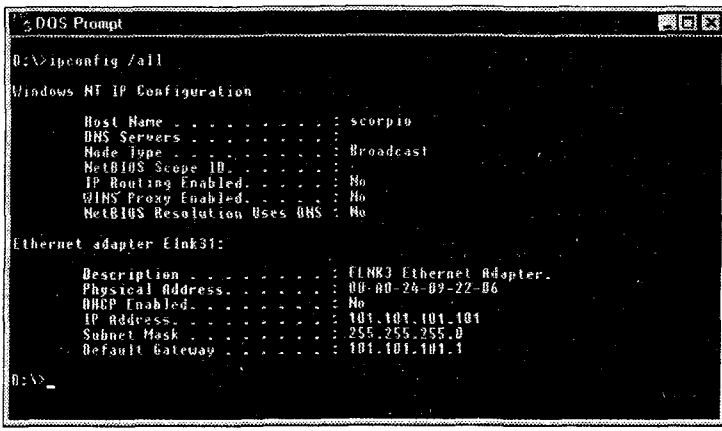


Рис. 11.10. Вывод команды IPCONFIG/ALL

IPCONFIG может использоваться для того, чтобы вручную продлить или прекратить DHCP-аренду. Команда IPCONFIG/RENEW указывает системе провести попытку продления аренды. Эта команда особенно удобна в случае, если сервер должен быть остановлен на некоторое время.

Как упоминалось выше, клиент не прекращает аренду автоматически по завершении работы. Утилита IPCONFIG позволяет вам завершить DHCP-аренду при помощи ключа /RELEASE. Эта команда часто используется перед перемещением компьютера в другую сеть. После использования команды IPCONFIG/RELEASE IP-адрес немедленно становится доступен для назначения его другим компьютерам. Когда клиент будет включен в новую подсеть, он запросит новый адрес.

Администрирование базы данных DHCP

База данных DHCP управляется так же, как и большинство других баз данных в Windows NT. Вы можете резервировать, восстанавливать и сжимать базу данных DHCP вручную. Вы должны поддерживать вашу базу данных, страхуясь от ее сбоя или отказа жесткого диска.

По умолчанию служба сервера DHCP резервирует базу данных после 60 минут неактивности. Файлы помещаются в каталог *\%systemroot%*

system32\dhcp\backup\Jet; содержимое подраздела реестра \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Configuration сохраняется в каталоге \%*systemroot*%\system32\dhcp\backup под именем DHCPCFG. Интервал и путь резервирования могут быть изменены в разделе реестра \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Одним из важнейших достоинств службы сервера DHCP является возможность автоматического восстановления поврежденной базы данных DHCP – конечно, если существует резервная копия. Вы также можете восстановить базу данных DHCP вручную, использовав один из двух следующих методов:

- Установите значение параметра RestoreFlag раздела реестра \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters равным 1и перезагрузите компьютер. База данных будет восстановлена с резервной копии.
- Скопируйте содержимое каталога \%*systemroot*%\system32\dhcp\backup\Jet в каталог \%*systemroot*%\system32\dhcp и перезагрузите компьютер.

Как и для большинства баз данных Windows NT, для сжатия базы данных DHCP может использоваться утилита JETPACK. Вы должны остановить службу DHCP перед запуском JETPACK. Для того чтобы сжать базу данных DHCP с использованием JETPACK, выполните следующие шаги:

1. Из командной строки перейдите в каталог \%*systemroot*%\system32\dhcp.
2. Введите команду JETPACK DHCP.MDB temp.MDB. Вместо имени temp можете использовать все что угодно, поскольку этот файл скоро будет переименован.
3. Переименуйте файл temp.MDB при помощи команды REN temp.MDB DHCP.MDB.
4. Перезапустите сервер DHCP при помощи Service Manager.

Вопросы для подготовки к экзамену

Question 1

Which of the following are benefits of using DHCP? (Check all correct answers.)

- ❑ A. Dynamic NetBIOS name registration.
- ❑ B. Dynamic IP configuration.
- ❑ C. Less chance of human error.
- ❑ D. Centralized IP name resolution.

Вопрос 1

Что является преимуществом использования DHCP? (Укажите все правильные ответы.)

- ❑ A. Динамическая регистрация имен NetBIOS.
- ❑ B. Динамическая настройка IP.
- ❑ C. Уменьшение вероятности ошибки администратора.
- ❑ D. Централизованное определение IP-имен.

Правильные ответы на этот вопрос — B и C. Одной из основных причин использования DHCP является возможность динамической настройки узлов (отсюда и название DHCP — Dynamic Host Configuration Protocol). Поскольку настройка централизована на сервере, вероятность человеческой ошибки уменьшается. DHCP не имеет отношения к регистрации имен NetBIOS, хотя адреса серверов WINS и могут выдаваться клиентам при помощи DHCP. Следовательно, ответ A неверен. Централизованное определение IP-имен выполняется при помощи DNS, а не DHCP. Следовательно, ответ D также неверен.

Question 2

What is the order of the DHCP lease process?

- ○ A. Request, Acknowledgment, Offer, Selection.
- ○ B. Request, Offer, Selection, Acknowledgment.
- ○ C. Request, Offer, Election, Selection.
- ○ D. Request, Election, Selection, Acknowledgment.

Вопрос 2

В каком порядке происходит процесс DHCP-аренды?

- ○ A. Запрос, подтверждение, предложение, выбор.
- ○ B. Запрос, предложение, выбор, подтверждение.
- ○ C. Запрос, предложение, выборы, выбор.
- ○ D. Запрос, выборы, выбор, подтверждение.

Правильный ответ на этот вопрос — B: запрос, предложение, выбор, подтверждение. Если вы вспомните, как происходит процесс, это станет хорошо понятно. В ответе A указан неверный порядок, и, следовательно, этот ответ неверен. В процессе DHCP-аренды нет понятия «выборы». Следовательно, ответы C и D неверны.

Question 3

A DHCP-enabled client is moved from Subnet A to Subnet B. After the move, the user complains that he is no longer able to use TCP/IP. What is the possible cause for this problem?

- A. The client did not terminate its lease before the computer was moved.
- B. DHCP cannot support multiple subnets.
- C. The client's WINS configuration is incorrect.
- D. The router between Subnet A and Subnet B is not able to forward BOOTP broadcasts.

Вопрос 3

DHCP-клиент был перемещен из подсети A в подсеть Б. После перемещения пользователь сообщил, что он больше не может использовать TCP/IP. Что может быть причиной проблемы?

- A. Клиент не завершил DHCP-аренду перед перемещением компьютера.
- B. DHCP не может поддерживать несколько подсетей.
- C. Настройка WINS на клиенте ТО ЖЕ неверна.
- D. Маршрутизатор не может ретранслировать широковещательные BOOTP-сообщения.

Лучший ответ на этот вопрос – D. Запомните, что маршрутизатор должен поддерживать широковещательные BOOTP-сообщения, если сервер и клиент DHCP находятся в разных подсетях. Вне зависимости от того, завершил ли клиент DHCP-аренду, процесс аренды будет начат заново при загрузке компьютера после перемещения его в другую подсеть. Следовательно, ответ A неверен. Как видно из правильного ответа, DHCP может поддерживать несколько подсетей. Следовательно, ответ B неверен. Настройка WINS имеет отношение только к определению имен NetBIOS, но не к основным операциям TCP/IP. Следовательно, ответ C неверен.

Question 4

Which of the following are functions of IPCONFIG? (Check all correct answers.)

- ❑ A. Renew DHCP lease.
- ❑ B. View WINS configuration.
- ❑ C. Release DHCP lease.
- ❑ D. Request DHCP lease.

Вопрос 4

Какие функции позволяет выполнять утилита IPCONFIG? (Укажите все правильные ответы.)

- ❑ A. Продление DHCP-аренды.
- ❑ B. Просмотр настройки WINS.
- ❑ C. Завершение DHCP-аренды.
- ❑ D. Запрос DHCP-аренды.

Правильные ответы на этот вопрос — A, B и C. Вы можете управлять DHCP-арендой при помощи ключей /RENEW и /RELEASE. С помощью ключа /ALL можно посмотреть настройки WINS. Однако, вы не можете начать процесс запроса DHCP-аренды. Следовательно, ответ D неверен. Ответ B неверен, потому что утилита IPCONFIG не предоставляет доступ к такой информации

Question 5

Which of the following utilities can be used to administer the DHCP database?

- ○ A. IPCONFIG
- ○ B. JETPACK
- ○ C. DHCP Manager
- ○ D. Network applet

Вопрос 5

Какая из следующих утилит используется для администрирования базы данных DHCP?

- ○ A. IPCONFIG
- ○ B. JETPACK
- ○ C. DHCP Manager
- ○ D. Приложение Network

Правильный ответ на этот вопрос — B. Утилита JETPACK используется для сжатия базы данных DHCP. IPCONFIG используется для просмотра конфигурации и продления или завершения DHCP-аренды, но не для администрирования базы данных. DHCP Manager может использоваться для изменения базы данных, но под администрированием обычно понимают резервирование, восстановление и сжатие, а не управление (в этом и состоит сложность вопроса). Приложение Network используется для установки DHCP, но на этом его использование заканчивается.

Дополнительная информация

Раздел о DHCP Microsoft TechNet, September, 97, PN99367, содержит исчерпывающую информацию и может ответить на любые ваши вопросы.

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы можете произвести поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевое слово «DHCP».

Служба определения имен Интернета (WINS)

Термины, необходимые для понимания материала:

- Статическая запись
- «Толкающий» партнер
- «Тянущий» партнер
- Сервер имен NetBIOS
- Прокси-агент WINS

Приемы и знания, которыми вы должны овладеть:

- Установка WINS
- Настройка клиентов WINS
- Настройка «толкающих»/«тянущих» партнеров
- Сжатие базы данных WINS

В этой главе вы узнаете, как установить WINS. Вы также познакомитесь с параметрами настройки клиентов и серверов, с настройкой избыточности серверов WINS и с интеграцией не-WINS клиентов в WINS-окружение. Вы также научитесь администрировать и поддерживать базу данных WINS.

WINS: исследованная и объясненная

WINS — это сервер имен NetBIOS, входящий в состав Windows NT Server 4. Метод работы WINS отличается от методов определения имен, которые мы рассматривали выше (DNS, файлы HOSTS и LMHOSTS), поскольку является динамической, или автоматической, службой определения имен. Сервер WINS на самом деле собирает имена и IP-адреса клиентов, работающих в сети. Когда клиенту WINS необходимо определить IP-адрес другого компьютера сети, он просто обращается к серверу WINS за определением имени.

Наиболее очевидное преимущество использования WINS — уменьшение широковещательного трафика в сети. Без WINS определение и регистрация имен в сети Microsoft выполняются при помощи широковещательных сообщений:

- Когда компьютер включается в сеть, он анонсирует свое имя NetBIOS при помощи широковещательного сообщения. Если машины с таким именем нет в сети, данный компьютер закрепляет его за собой и получает возможность общаться с другими компьютерами.
- Когда компьютер пытается установить NetBIOS-соединение с другим компьютером — например, при выполнении команды net send для отправки сообщения на машину-адресат, — он отправляет широковещательный запрос с именем NetBIOS адресата, запрашивая IP-адрес компьютера с таким именем. После получения ответа устанавливается соединение и сообщение отправляется.
- При правильном завершении работы компьютера он отправляет широковещательное сообщение, освобождая имя NetBIOS.

Как работает WINS?

Процесс работы WINS будет проще понять, если мы его разделим на три части: регистрация имени, определение имени и освобождение имени. Эти части описаны ниже и иллюстрированы на рис. 12.1.

- **Регистрация имени NetBIOS.** При инициализации клиента WINS он отправляет сообщение серверу WINS, запрашивая регистрацию его имени и IP-адреса. Клиент получает определенное время — TTL (время жизни), и имя регистрируется на сервере WINS. Когда

некоторая часть времени жизни проходит, клиент пытается продлить время жизни для своего имени NetBIOS.

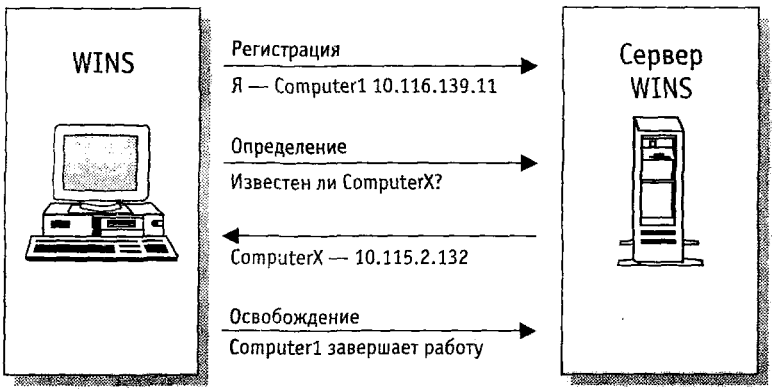


Рис. 12.1. Процесс работы WINS

- **Определение имени NetBIOS.** Когда клиент WINS пытается установить соединение с каким-либо компьютером, он отправляет сообщение серверу WINS, запрашивая определение имени. Сервер WINS возвращает IP-адрес требуемого узла.
- **Освобождение имени.** При корректном завершении работы клиент отправляет сообщение серверу WINS, освобождая свое имя NetBIOS. Имя помечается в базе данных сервера WINS, указывая, что TTL для этой записи равняется нулю. После того как имя освобождено, оно доступно для использования другим компьютером.

Планирование и реализация WINS-окружения

При планировании установки WINS в вашей сети вы должны ответить на следующие вопросы:

- **Все ли компьютеры могут использовать WINS?** Большинство систем, которые могут работать в сети Microsoft и используют продукты Microsoft, могут быть настроены на использование WINS. Если в вашей сети имеются компьютеры, не поддерживающие WINS, вы можете внести в базу данных сервера WINS статические записи для этих клиентов. Это позволит клиентам WINS определять имена не-WINS клиентов. Однако не-WINS клиенты не смогут использовать базу данных WINS для определения имен. Вы должны будете обеспечить для них альтернативный способ определения имен, такой как файл HOSTS, сервер имен DNS или про-

кси-агент WINS. Прокси-агенты WINS обсуждаются ниже в разделе «Прокси-агенты WINS».

- **Сколько серверов WINS необходимо установить?** Серверы WINS в состоянии производить около 1500 регистраций и 4500 определений имен в минуту; пессимистическая оценка показывает, что вы должны иметь сервер WINS и резервный сервер WINS для каждых 1000 клиентов. Если один из серверов WINS откажет, ваши пользователи могут заметить некоторое уменьшение производительности, но определение имен по-прежнему будет работать.
- **Состоит ли сеть из отдельных далеко расположенных друг от друга частей, связанных с использованием технологий глобальных сетей, таких как T1 или ATM?** Если ваша сеть использует технологии глобальных сетей, вы должны задуматься о размещении сервера WINS в каждой из частей. Это позволит определять имена NetBIOS локально, без выхода в глобальную сеть.

Установка и настройка сервера WINS

Только Windows NT Server может быть сервером WINS. Установка службы WINS похожа на установку любой другой сетевой службы для Windows NT(рис. 12.2). Для настройки Windows NT Server на работу в качестве сервера WINS, выполните следующие шаги:

1. Щелкните правой кнопкой на значке Network Neighbourhood и выберите в контекстном меню команду Properties. Откроется окно диалога Network.
2. Откройте вкладку Services и нажмите кнопку Add.

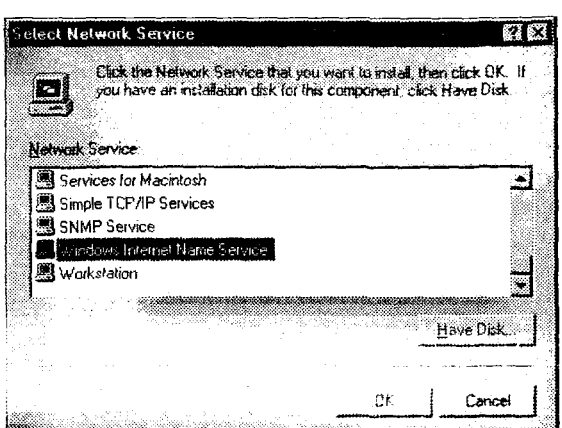


Рис. 12.2. Установка сервера WINS

3. Выберите Windows Internet Name Service из списка служб. Введите путь к установочным файлам Windows NT Server и нажмите кнопку OK.
4. Нажмите кнопку Close.
5. Перезагрузите компьютер, когда вам будет это предложено.

После того как система перезапустится, в подменю Administrative tools будет добавлена программа WINS Manager. WINS готова к использованию. Никакая дальнейшая настройка не требуется для того, чтобы WINS могла функционировать, но, чтобы работа WINS была более успешной, все-таки может понадобиться произвести некоторые настройки.

Администрирование WINS

Для настройки базы данных WINS может использоваться программа WINS Manager. Для того чтобы запустить ее, выберите команду Start ➤ Programs ➤ Administrative Tools (Common) ➤ WINS Manager.

Когда WINS Manager будет запущен в первый раз, вы должны увидеть ваш сервер WINS и связанную с ним статистику. Аналогично DHCP Manager, WINS Manager может быть использован для удаленного администрирования нескольких серверов. Для того чтобы добавить серверы WINS в WINS Manager, выберите в меню Server команду Add WINS Server. Введите имя или IP-адрес сервера WINS, который вы хотите добавить, когда вам будет предложено это сделать, и нажмите кнопку OK. Сервер WINS должен появиться в списке. Для того чтобы удалить сервер WINS из списка, выделите сервер в окне WINS Manager и выберите в меню Server команду Delete WINS Server, затем подтвердите удаление, нажав кнопку OK.

База данных WINS

Для того чтобы посмотреть на базу данных WINS, выберите команду Mappings ➤ Show Database. Окно диалога Show Database (рис. 12.3) содержит существующие на настоящий момент записи и позволяет использовать несколько способов для поиска в базе данных. В окне Mappings вы можете видеть, какие записи активны и какие являются статическими, а также срок годности каждой записи. Справа в окне Mappings расположен столбец, озаглавленный Version ID. Число, указанное в этом столбце, используется партнером репликации для определения того, какие изменения в базе данных произошли последними. Если вы хотите создать заново всю базу данных WINS, нажмите кнопку Delete Owner для удаления всех записей.

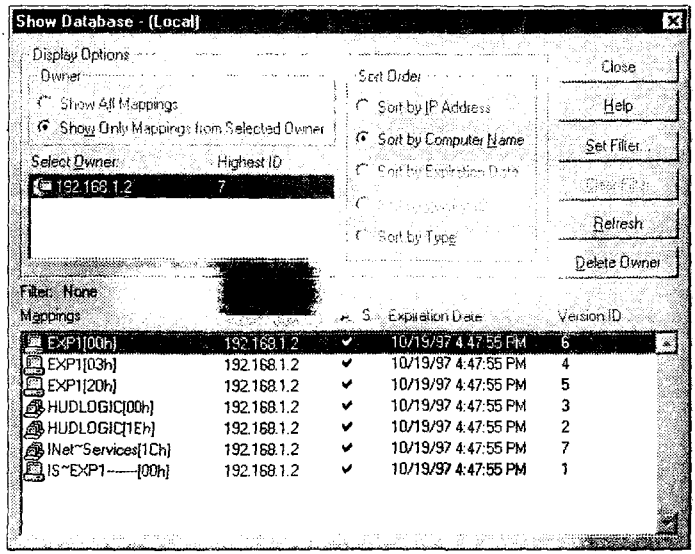


Рис. 12.3. Просмотр базы данных WINS

Сборка мусора

Меню Mappings содержит команду Initiate Scavenging, позволяющую удалять записи из базы данных WINS. Этот процесс называется сборкой мусора, он обеспечивает проверку записей базы данных и их владельцев. Записи, срок действия которых истек или у которых нет владельца, удаляются из базы данных. Сборка мусора производится сервером WINS автоматически. Для того чтобы установить временные интервалы (рис. 12.4), выберите в меню Server команду Configuration. Вы можете установить следующие интервалы:

- **Renewal Interval.** Это максимальный промежуток времени, в течение которого имя NetBIOS считается зарегистрированным. В Windows NT Server 4 он по умолчанию равен 144 часам (6 суток). После этого клиент должен перерегистрировать имя на сервере WINS, в противном случае имя будет считаться освобожденным.
- **Extinction Interval.** Освобожденное имя сохраняется в базе данных, чтобы его не понадобилось вводить заново, если клиент WINS пытается зарегистрировать его. По умолчанию, когда истек промежуток в шесть суток с момента, как имя стало освобожденным, оно уже считается «вымершим», означает, что оно будет скоро удалено из базы данных. Вы можете установить промежуток, через который имя становится «вымершим», в часах, минутах и секундах.
- **Extinction Timeout.** Этот временной интервал задает, как долго имя хранится в базе данных после того, как оно стало «вымершим».

По умолчанию «вымершие» имена находятся в базе данных еще шесть суток.

- **Verify Interval.** Этот интервал определяет, как долго сервер WINS позволяет записям из другой базы данных WINS (партнера репликации) оставаться активными в собственной базе данных. По истечении этого времени записи должны быть проверены.
- **Pull Parameters/Push Parameters.** Эти группы элементов управления используются для настройки работы с партнерами репликации WINS (которые описываются в следующем разделе).

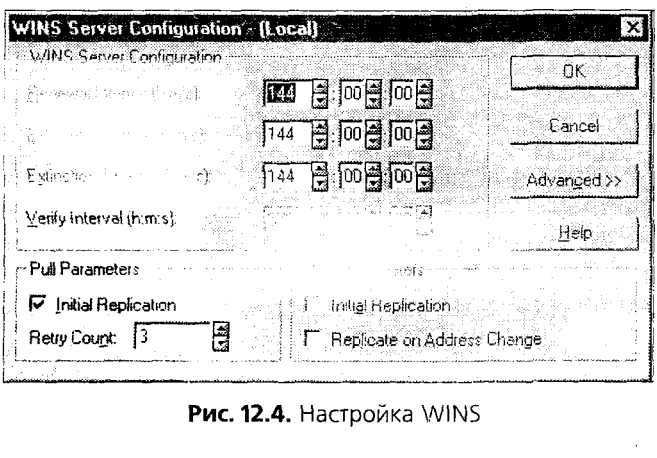


Рис. 12.4. Настройка WINS

Чтобы получить более подробную информацию о настройках, нажмите кнопку Help в окне WINS Server Configuration.

Партнеры репликации WINS

Серверы WINS обычно устанавливаются парами для обеспечения избыточности. При отказе одного из серверов определение имен будет по-прежнему возможно, что снижает влияние отказа на пользователей. Серверы WINS могут быть настроены на взаимное обновление своих баз данных, позволяющее всем серверам WINS иметь идентичную информацию.

Сервер WINS, настроенный как «толкающий», отправляет свою базу данных партнеру. Отправка базы данных происходит после фиксированного количества изменений в ней. Сервер WINS, настроенный как «тянущий», запрашивает у партнера изменения в их базах данных через фиксированный интервал времени. Сервер WINS может быть настроен как «толкающий» партнер, «тянущий» партнер или как и «толкающий» и «тянущий» партнер одновременно, что позволяет

синхронизировать его базу данных с базой данных другого сервера WINS (рис. 12.5).

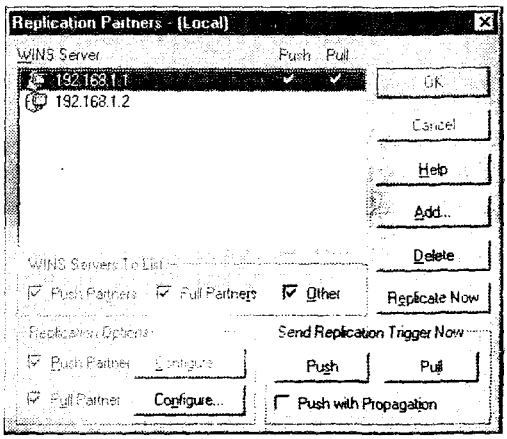


Рис. 12.5. Окно диалога Replication Partners

Внимание

Microsoft рекомендует настраивать «тянущих» партнеров по обе стороны медленного канала связи между частями глобальной сети. Это позволит вам контролировать, когда изменения в базе данных передаются через канал связи. «Толкающие» партнеры рекомендуются для использования только в быстрых локальных сетях.

В окне диалога Replication Partners вы можете произвести различные настройки. Если вы установите флажок Push With Propagation, то после того, как ваш сервер отправит изменения в своей базе данных партнеру, он предложит партнеру передать изменения в его базе данных всем его партнерам. Вы можете больше узнать об этом и других параметрах, нажав кнопку Help в окне диалога Replication Partners.

Резервирование базы данных

База данных WINS использует ядро Microsoft Access. Аналогично базе данных DHCP, резервная копия базы данных WINS может быть создана при помощи WINS Manager. Резервные копии определенных имен и TTL соответствующих записей должны производиться систематически, чтобы база данных могла быть восстановлена в случае ее повреждения. Процесс резервирования базы данных должен быть начат вручную, но после того, как вы произведете резервирование, оно будет автоматически повторяться каждые 24 часа. Для того чтобы начать резервирование базы данных WINS, выполните следующие шаги:

1. Откройте WINS Manager.
2. В меню Mappings выберите команду Backup Database.
3. Выберите каталог, в который вы хотите поместить резервную копию.
4. Установите флажок Incremental Backup, для того чтобы архивировались только изменения по сравнению с последней резервной копией. В противном случае будет выполнено резервное копирование всей базы данных.
5. Нажмите кнопку OK.

При повреждении базы данных она будет автоматически восстановлена. Вы также можете произвести форсированное восстановление баз данных, выбрав в меню Mappings окна WINS Manager команду Restore Database.

Сжатие при помощи JETPACK

Программное обеспечение Microsoft Windows NT Server 4 настроено на автоматическое сжатие базы данных WINS, однако вы можете сжать ее вручную. База данных должна быть сжата, если ее размер становится более 30 Мбайт. Чтобы определить размер базы данных WINS, просмотрите свойства файла WINS.MDB в каталоге %systemroot%\system32\wins.

Для того чтобы сжать базу данных вручную, используйте утилиту JETPACK. Синтаксис ее таков:

```
jetpack wins.mdb временное_имя.mdb
```

Совет

При использовании утилиты JETPACK вы должны перейти в каталог *systemroot*\system32\wins. Остановите WINS перед сжатием базы данных. Запустите WINS заново, после того как сжатие будет завершено.

Настройка клиентов WINS

После того как серверы WINS настроены, вы должны настроить клиентов на их использование. Это может быть выполнено как непосредственно на клиентском компьютере, так и централизованно — на сервере DHCP.

На клиенте, работающем под управлением Windows 95 или Windows NT, щелкните правой кнопкой мыши значок Network Neighbourhood. В окне диалога Network откройте вкладку Protocols и дваж-

ды щелкните на протоколе TCP/IP. Откроется окно диалога TCP/IP Properties. Откройте вкладку WINS Address (рис. 12.6). В поле Primary WINS Server введите IP-адрес сервера WINS. Если доступны два сервера, добавьте запись в поле Secondary WINS Server.

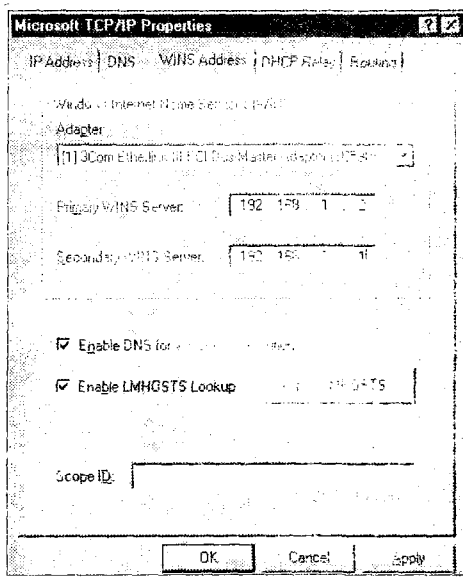


Рис. 12.6. Настройка клиентского компьютера на использование WINS

Если в сети используется DHCP, откройте DHCP Manager и введите информацию о сервере WINS в качестве информации по умолчанию, глобальной информации или информации для контекста (рис. 12.7).

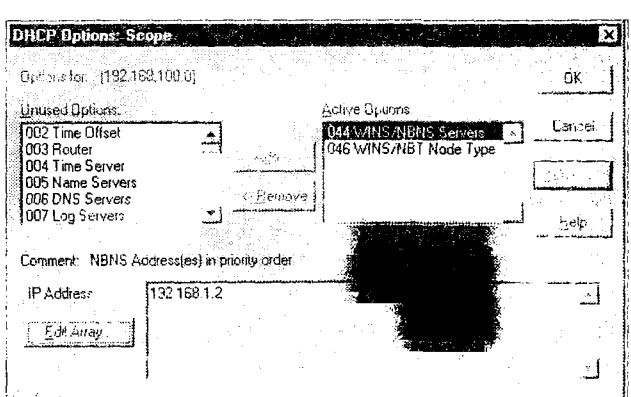


Рис. 12.7. Настройка WINS при помощи DHCP

WINS может быть настроен в любой из этих областей в зависимости от того, как устроена сеть. Необязательная информация — 044 NBNS и 046 Node type. После того как DHCP будет настроен на использование WINS, клиенты DHCP станут клиентами WINS после завершения работы и последующего получения нового IP-адреса.

Прокси-агенты WINS

Windows NT-компьютер может быть настроен как прокси-агент WINS, что позволяет ему переправлять широковещательные запросы на определение имени не-WINS клиентов серверу WINS. В действительности прокси-агент WINS — это способ использования сервера WINS не-WINS клиентами. Процесс определения имени происходит следующим образом:

1. Не-WINS клиент отправляет широковещательный запрос на определение имени в локальный сегмент сети.
2. Прокси-агент WINS получает этот широковещательный запрос.
3. Прокси-агент WINS переправляет запрос на определение имени серверу WINS.
4. Сервер WINS отвечает на запрос прокси-агента WINS.
5. Прокси-агент WINS переправляет ответ сервера WINS не-WINS клиенту.

Прокси-агенты WINS нужны только в тех подсетях, в которых нет сервера WINS. Если не-WINS клиент отправляет широковещательный запрос на определение имени в сегмент, в котором есть сервер WINS, то сервер WINS отвечает на этот запрос (рис. 12.8). Если ваши маршрутизаторы ретранслируют широковещательные сообщения (на UDP-портах 137 и 138), то прокси-агент WINS также не нужен. Однако настройка маршрутизаторов на ретрансляцию широковещательных сообщений не рекомендуется, поскольку это приводит к увеличению сетевого широковещательного трафика.

Любой компьютер, работающий под управлением Microsoft Windows NT 4, может быть настроен как прокси-агент WINS. Для этого откройте раздел реестра:

```
HKEY_Local_Machine\System\CurrentControlSet\Services\NetBT\Parameters
```

Затем установите значение параметра EnableProxy в 1. После этого закройте редактор реестра и перезагрузите компьютер, чтобы разрешить службу WINS-прокси.

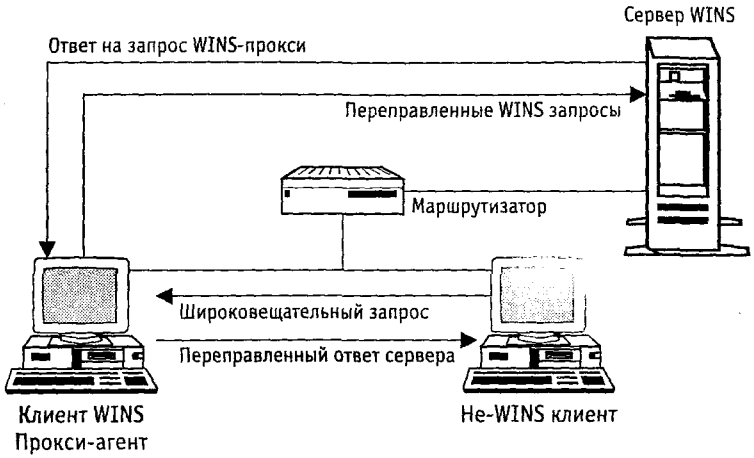


Рис. 12.8. Процесс работы WINS-прокси

Внимание

Вы не должны устанавливать в подсети более двух прокси-агентов WINS; *в противном случае это может привести к тому, что сетевой* трафик превысит приемлемую границу; каждый прокси-агент WINS ретранслирует все широковещательные запросы на определение имени, которое он получает.

Вопросы для подготовки к экзамену

Question 1

Which of the following are benefits of using WINS? (Check all correct answers.)

- ❑ A. Dynamic NetBIOS name registration.
- ❑ B. Dynamic IP configuration.
- ❑ C. Reduction in broadcast traffic.
- ❑ D. Increase in network throughput capacity.

Вопрос 1

Что является преимуществом использования WINS? (Укажите все правильные ответы.)

- ☐ A. Динамическая регистрация имен NetBIOS.
- ☐ B. Динамическая настройка IP.
- ☐ C. Уменьшение широковещательного трафика.
- ☐ D. Увеличение пропускной способности сети.

Правильные ответы на этот вопрос — A и C. WINS предоставляет службу динамической (автоматической) регистрации имен NetBIOS, а также службы их определения и освобождения. Кроме того, WINS снижает широковещательный трафик в сети, поскольку клиенты WINS вместо широковещательных запросов при определении имен используют сервер WINS. Однако за динамическую настройку IP отвечает DHCP, а не WINS. Следовательно, ответ B неверен. Ответ D неверен, поскольку для увеличения пропускной способности сети обычно требуется замена аппаратного обеспечения, и она ничего общего не имеет с WINS или определением имен.

Question 2

Which utility is used to back up the WINS database?

- ○ A. JETPACK
- ○ B. WINS Manager
- ○ C. DHCP Manager
- ○ D. Server Manager

Вопрос 2

Какая утилита используется для создания резервной копии базы данных WINS?

- ○ A. JETPACK
- ○ B. WINS Manager
- ○ C. DHCP Manager
- ○ D. Server Manager

Правильный ответ на этот вопрос — B, WINS Manager. JETPACK используется не для создания резервной копии базы данных, а для ее сжатия. Следовательно, ответ A неверен. DHCP Manager может использоваться для настройки клиентов DHCP на использование WINS, но он не предназначен для создания резервной копии базы данных

WINS. Следовательно, ответ C неверен. Server Manager используется для управления серверами в вашей сети, но он не имеет возможности создания резервной копии базы данных WINS. Следовательно, ответ D неверен.

Question 3

You manage a network of 1,500 Microsoft clients, all configured to use DHCP. You have been asked to implement WINS on your network for NetBIOS name resolution. What is the easiest way to configure these client computers to use WINS?

- A. Configure the DHCP server with options 44 WINS/NBNS and 46 WINS/NBT.
- B. Configure the DHCP server with option 44 WINS/NBNS only.
- C. Configure the DHCP server with option 46 WINS/NBT only.
- D. Configure each client with the address of the WINS server manually.

Вопрос 3

Вы управляете сетью, содержащей 1500 Microsoft-клиентов, настроенных на использование DHCP. Вам требуется реализовать в вашей сети WINS для определения имен NetBIOS. Каков простейший способ настройки клиентов на использование WINS?

- A. Настройка сервера DHCP с параметрами 44 WINS/NBNS и 46 WINS/NBT.
- B. Настройка сервера DHCP только с параметром 44 WINS/NBNS.
- C. Настройка сервера DHCP только с параметром 46 WINS/NBT.
- D. Ручная настройка адреса сервера WINS на каждом из клиентов.

Правильный ответ на этот вопрос — A. В сети 1500 компьютеров, так что вы не хотите бегать и настраивать компьютеры-клиенты вручную, раз уж вы используете DHCP. Вы не можете добавить параметр 44 без параметра 46 на сервере DHCP.

Question 4

You have been asked to configure WINS name resolution for all of the computers on your network. There are two WINS servers on your network that reside on the same subnet. Your routers are not configured to forward NetBIOS name broadcasts. If you have six total subnets on your entire IP network, with a mixture of WINS and non-WINS clients, how many WINS Proxy servers must you configure to complete the objective, and where?

- A. Six: one on each subnet.
- B. Five: one on each subnet that does not have a WINS server.
- C. One WINS Proxy Agent.
- D. Two WINS Proxy Agents on the same subnet as the WINS servers.

Вопрос 4

Вам требуется настроить определение имен при помощи WINS для всех компьютеров вашей сети. В вашей сети уже имеются два сервера WINS, находящихся в одной подсети. Ваши маршрутизаторы не настроены на ретрансляцию широковещательных запросов на определение имен NetBIOS. Ваша сеть состоит из шести подсетей, в которых имеются как WINS-клиенты, так и не-WINS клиенты. Сколько WINS-прокси серверов вы должны установить и где?

- A. Шесть: по одному в каждой подсети.
- B. Пять: по одному в каждой подсети, не содержащей сервера WINS.
- C. Один прокси-агент WINS.
- D. Два прокси-агента WINS в той же подсети, что и сервера WINS.

Правильный ответ на этот вопрос — B. Вы должны настроить по одному прокси-агенту WINS в каждой подсети, не содержащей сервера WINS. Вам не нужен прокси-агент WINS в подсети, содержащей оба ваших сервера WINS. Следовательно, ответ A неверен. Другие предлагаемые варианты не обеспечивают определение имен для всех компьютеров во всей сети, поскольку не-WINS клиенты имеются во всех подсетях вашей сети.

Question 5

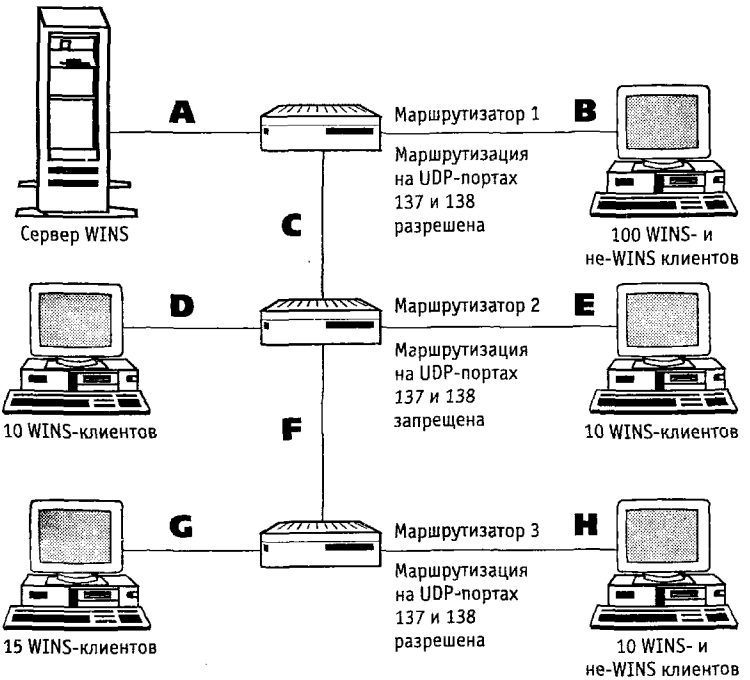
You have been asked to provide dynamic name resolution for your entire network. Your network is configured as shown in the following graphic. What is the minimum number of WINS Proxy Agents you require and where would you put them?

- A. None.
- B. Two, one for segment H and one for segment B.
- C. Seven, one for each segment except segment A.
- D. One for segment H.

Вопрос 5

Вам требуется обеспечить динамическое определение имен для всей сети. Ваша сеть имеет строение, показанное на приведенной иллюстрации. Какое наименьшее количество прокси-агентов WINS вам понадобится и где они должны быть размещены?

- A. Ни одного.
- B. Два: один в сегменте H и один в сегменте B.
- C. Семь: по одному в каждом сегменте, кроме A.
- D. Один в сегменте H.



Правильный ответ на этот вопрос – D. Только сегмент H требует прокси-агент WINS. Если вы думаете, что правильный ответ – A, то посмотрите снова на маршрутизатор 2. Он не пропускает широковещательные запросы от не-WINS клиентов в сегменте H к серверу WINS в сегменте A. Сегмент B не нуждается в прокси-агенте WINS, поскольку маршрутизатор 1 будет ретранслировать широковещательные запросы в сегмент A. Только сегменты B и H содержат не-WINS клиенты, поэтому только эти сегменты являются кандидатами на установку в них прокси-агента WINS.

Дополнительная информация

Microsoft TechNet, September, 97, PN99367, содержит множество статей об IP-адресации и масках подсетей. Проведите поиск по ключевым словам «WINS», «Windows Internet Name Service», «NetBIOS Name Server» и «WINS replication partners».

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы можете произвести поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевые слова «WINS», «WINS replication» и «WINS database».

Коммуникации

Термины, необходимые для понимания материала:

- NETSTAT
- NBTSTAT
- Telnet
- FTP
- LPR
- LPQ
- REXEC
- RCP
- RSH
- IIS
- Демон

Приемы и знания, которыми вы должны овладеть:

- Использование утилит, входящих в состав операционных систем Microsoft, для получения статистической информации об IP
- Понимание назначения каждого ключа каждой утилиты

Как неоднократно говорилось на протяжении этой книги, TCP/IP имеет массу достоинств, делающих реализацию этого набора протоколов в сети привлекательной. Не последним из этих достоинств является межплатформенная совместимость. В этой главе мы рассмотрим Microsoft-реализацию TCP/IP. Мы обсудим некоторые доступные утилиты, Microsoft IIS (Internet Information Server, информационный сервер Интернета) и печать при помощи TCP/IP.

IP-утилиты Microsoft

Среди стандартных TCP/IP-утилит, таких как FTP и PING, Microsoft включает в состав своих операционных систем две программы, которые позволяют наблюдать за состоянием TCP/IP в данной системе. Эти программы, NETSTAT и NBTSTAT, могут выводить ценную информацию, особенно полезную при поиске и устранении неисправностей.

NETSTAT

Утилита NETSTAT выводит статистику для протоколов (TCP, IP, ICMP или UDP) и информацию об IP-соединениях. Команда NETSTAT имеет следующий синтаксис:

```
netstat [-a] [-e] [-n] [-s] [-p протокол]
[-r] [интервал]
```

На рис. 13.1 приведен пример вывода команды NETSTAT -a.

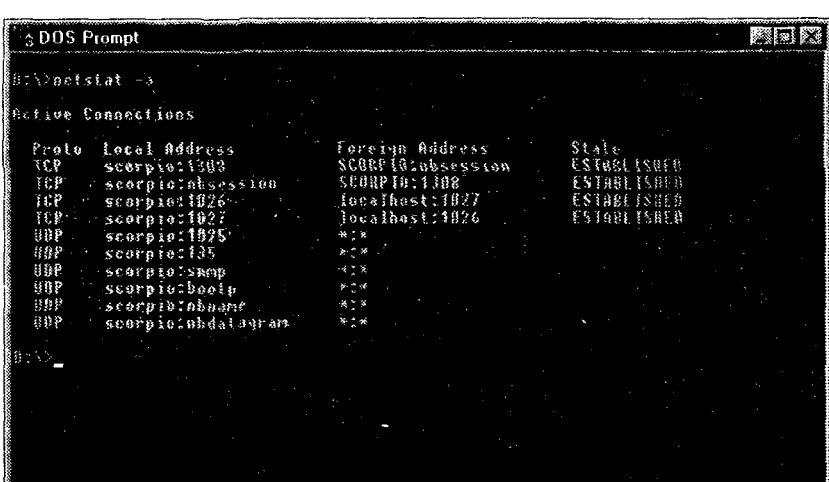


Рис. 13.1. Команда NETSTAT -a выводит информацию обо всех соединениях

В табл. 13.1 приведены ключи, которые могут быть использованы с командой NETSTAT, и их описание.

Таблица 13.1. Утилита Microsoft NETSTAT

Ключ	Описание
-a	Вывод информации о всех соединениях и всех портах, на которых компьютер ожидает соединения
-e	Вывод информации об Ethernet
-n	Вывод информации в числовой форме, без попыток определения имен
-s	Вывод подробной статистики для протоколов. Этот ключ может использоваться вместе с -p для получения статистики по определенному протоколу
-p протокол	Вывод информации о соединениях с использованием данного протокола. Параметр протокола может принимать значения TCP и UDP. Если использован ключ -s, то возможно также использовать значения ICMP и IP
-r	Вывод таблицы маршрутизации для компьютера
интервал	Постоянный вывод информации с интервалом в указанное количество секунд. Для завершения работы программы нажмите Ctrl+C

NBTSTAT

Утилита NBTSTAT выводит статистическую информацию для NetBIOS на основе TCP/IP. На рис. 13.2 приведен пример вывода команды NBTSTAT -n, которая выводит локальную таблицу имен NetBIOS.

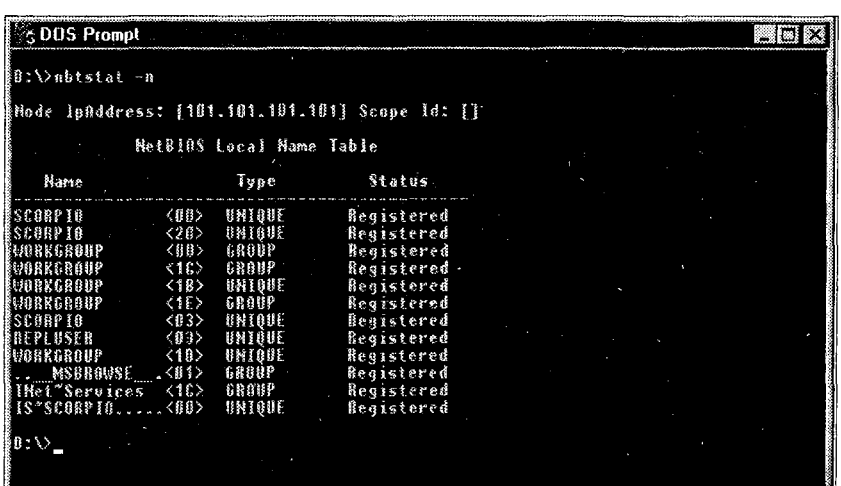


Рис. 13.2. Команда NBTSTAT может быть использована для вывода записей локальной таблицы имен NetBIOS

В табл. 13.2 приведены ключи, которые могут быть использованы с командой NBTSTAT. Важное отличие между NETSTAT и NBTSTAT заключается в том, что команда NETSTAT может быть выполнена без указания каких-либо ключей, а NBTSTAT требует как минимум одного ключа.

Таблица 13.2. Утилита Microsoft NBTSTAT

Ключ	Описание
-a имя_удаленной _системы	Вывод таблицы имен NetBIOS удаленной системы, заданной ее именем
-A IP-адрес	Вывод таблицы имен удаленной системы, заданной ее IP-адресом
-c	Вывод содержимого локального кэша имен NetBIOS с выводом IP-адреса для каждого имени
-n	Вывод локальной таблицы имен NetBIOS
-r	Вывод количества имен, определенных при помощи широковещательных запросов и при помощи WINS
-R	Очистка кэша имен NetBIOS с последующим помещением в него предзагружаемых записей из файла LMHOSTS
-s	Вывод списка сеансов с данным компьютером на настоящий момент и их состояния. Выводятся имена компьютеров, определенные по их IP-адресам
-S	Вывод списка сеансов с данным компьютером на настоящий момент и их состояния. Выводятся не имена компьютеров, а их IP-адреса
интервал	Постоянный вывод информации с интервалом в указанное количество секунд. Для завершения работы программы нажмите Ctrl+C

Краткое описание других утилит

Другие утилиты, перечисленные в этом разделе, подобны программам, входящим в состав большинства реализаций TCP/IP. Они используются для эмуляции удаленного терминала (Telnet), удаленного выполнения программ (REXEC), удаленного копирования файлов (RCP) и удаленного выполнения команд при помощи интерпретатора командной строки (RSH). В каждом случае, чтобы команда работала, на сервере должен быть запущен соответствующий демон. Демон — это программа, которая работает постоянно, ожидая и выполняя запросы для какой-либо службы. Например, если на Unix-компьютере запущен демон Telnet, пользователи Windows 95 имеют возможность доступа к этой системе. Если демон не запущен, возможность доступа отсутствует. Windows NT предоставляет только клиентские приложения для этих команд, но не серверы.

Telnet

Telnet — очень полезное приложение, эмулирующее удаленный терминал и использующее свой собственный транспортный протокол, определенный в RFC 854. Этот протокол работает на уровне приложения модели TCP/IP. Целью разработки Telnet было обеспечить взаимодействие между любым узлом и любым терминалом. Вы можете использовать эмуляцию одного из терминалов VT-100, VT-52 или TTY. Telnet чаще всего используется для межплатформенного доступа. Например, вместо того чтобы устанавливать непосредственное соединение между PC и маршрутизатором, администратор может использовать Telnet и работать фактически с терминалом на маршрутизаторе. Это означает, что управление маршрутизатором может осуществляться с рабочего места администратора. Другой пример использования Telnet — пользователь Windows NT, которому требуется управлять VMS-компьютером. Пользователь может открыть терминальный сеанс при помощи Telnet, что позволит обойтись без непосредственного подключения к VMS-системе.

Чтобы использовать Telnet для соединения с удаленной системой, введите команду Telnet IP-адрес_удаленного_узла. Когда соединение с удаленной системой будет установлено, вам будет предложено ввести имя пользователя и пароль. Если вы введете команду Telnet, не указав адрес удаленной системы, откроется окно программы Telnet. Выберите в меню Connect команду Remote System, как показано на рис. 13.3

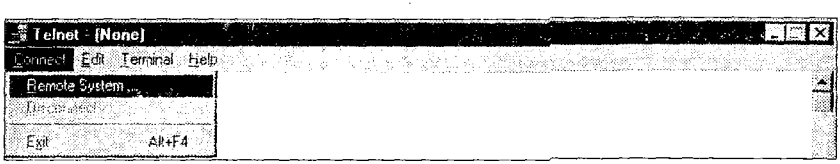


Рис. 13.3. Чтобы установить Telnet-соединение, выберите команду Remote System из меню Connect

REXEC (удаленное выполнение)

Утилита REXEC позволяет запустить процесс на удаленном компьютере, на котором работает служба сервера REXEC. REXEC производит аутентификацию пользователей и запускает процесс, только если были введены правильные имя пользователя и пароль. Команда REXEC имеет следующий синтаксис:

```
REXEC узел [-l имя_пользователя] [-n] команда
```

Параметры команды REXEC описаны в табл. 13.3.

Табл. 13.3 Параметры REXEC

Параметр	Описание
узел	Имя или IP-адрес узла, на котором должен быть запущен процесс
-l имя_пользователя	Имя пользователя, которое будет использовано при аутентификации на удаленном компьютере
-n	Переназначение стандартного ввода REXEC в NULL
команда	Команда, которая должна быть выполнена на удаленной системе

RCP (удаленное копирование)

RCP — утилита, похожая на FTP. Она позволяет копировать файлы с одного TCP/IP-узла на другой. Разница заключается в том, что RCP не производит аутентификацию пользователя. Имя пользователя должно быть указано в файле Unix-системы «.rhosts». Когда демон запущен, он производит чтение файла и обеспечивает подключение для указанных в этом файле пользователей. RCP имеет следующий синтаксис:

```
RCP [-a | -b] [-h] [-r]
[узел[.пользователь]:]источник
[узел[.пользователь]:]путь\назначение
```

Параметры RCP описаны в табл. 13.4.

Таблица 13.4. Параметры RCP

Параметр	Описание
-a	Файлы будут передаваться в текстовом (ASCII) режиме. Это — значение по умолчанию
-b	Файлы будут передаваться в двоичном (бинарном) режиме
-h	Копировать файлы, имеющие атрибут **hidden**
-r	Рекурсивное копирование: копируются все подкаталоги и все содержащиеся в них файлы указанного каталога. Источник и назначение должны быть каталогами
узел	Локальный или удаленный узел. Если узел задан своим IP-адресом, должно быть указано имя пользователя
пользователь	Указывает имя пользователя
источник	Указывает файлы для копирования
путь\назначение	Указывает путь для размещения копируемых файлов относительно домашнего каталога пользователя

RSH (Удаленный интерпретатор командной строки)

RSH — утилита, подобная REXEC. Она позволяет пользователю выполнить команду на удаленной системе. Однако RSH не требует регистрации пользователя в удаленной системе. Как и RCP, так и RSH использует файл «.rhosts». Одно из обычных применений RSH — запуск компилятора в Unix-системе. RSH имеет следующий синтаксис:

```
RSH узел [-l имя_пользователя] [-n] команда
```

В табл. 13.5 описаны параметры, используемые RSH.

Таблица 13.5. Параметры RSH

Параметр	Описание
узел	Имя или IP-адрес узла, на котором должен быть запущен процесс
-l имя_пользователя	Имя пользователя, которое будет использовано при аутентификации на удаленном компьютере
-n	Переназначение стандартного ввода RSH в NULL
команда	Команда, которая должна быть выполнена на удаленной системе

Службы информационного сервера Интернета

Microsoft IIS (Internet Information Server, информационный сервер Интернета) имеет совершенно отдельный набор классов и тестов. Вам следует знать, как он устанавливается и что делают его службы. IIS входит в состав Windows NT Server 4. Версия с урезанным набором возможностей, называемая Peer Web Server, входит в состав Windows NT Workstation 4. Также имеется версия для Windows 95, имеющая имя Personal Web Server for Windows 95. В соответствии с нашими целями, мы уделим основное внимание IIS.

Вы можете подумать, что IIS, как и любая другая сетевая служба, устанавливается из приложения Network. Это не так. После установки операционной системы на рабочем столе появится значок установки IIS. Однако, как и большинство людей, вы, скорее всего, удалили этот значок немедленно после установки NT. В таком случае вам следует знать, что программа установки IIS находится в каталоге *Systemroot*\system32 и называется INETINS.EXE.

После ее запуска вы увидите обычный экран установки программы. Нажмите кнопку OK, чтобы перейти к следующему шагу установки (рис. 13.4), на котором вы можете выбрать, какие компоненты IIS

устанавливать. Стандартный IIS Manager работает как приложение на Windows NT-компьютере, но также доступна HTML-версия — Internet Service Manager (HTML). Выберите, какие программы устанавливать, и нажмите OK.

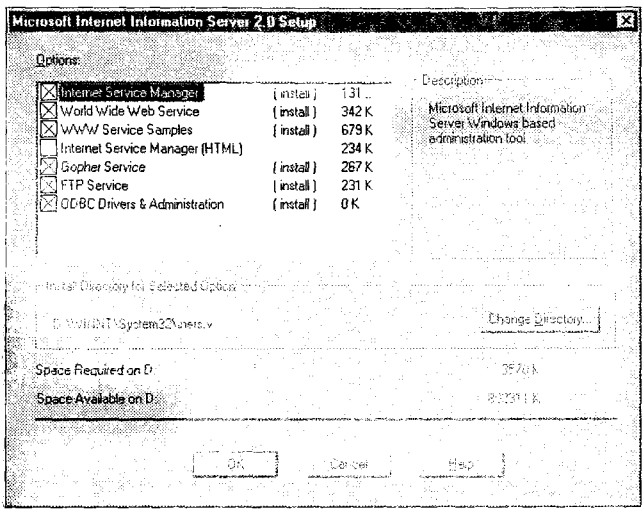


Рис. 13.4. Выбор устанавливаемых компонентов Microsoft Internet Information Server

На следующем шаге вам будет предложено указать каталоги для хранения общедоступных файлов каждой из служб, как показано на рис. 13.5. После того как вы укажете каталоги, нажмите OK. Начнется процесс установки IIS.

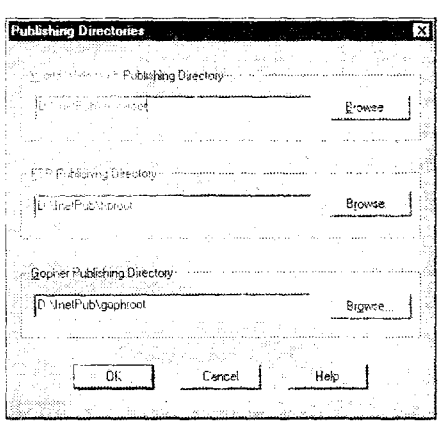


Рис. 13.5. Каждая служба имеет свой каталог для хранения общедоступных файлов

Если процесс установки не может определить имя домена для данного компьютера, вам будет предложено ввести его, чтобы быть уверенным, что Gopher работает правильно. Затем нажмите кнопку OK. Когда вам будет предложено, выберите, какие драйверы ODBC вы хотите установить, и нажмите кнопку OK. После завершения установки также нажмите кнопку OK.

Все службы управляются при помощи IIS Manager, показанного на рис. 13.6. Эта программа может быть запущена из раздела Programs меню Start. Чтобы произвести настройку какой-либо из служб, дважды щелкните на соответствующей строке. Вы также можете выделить службу и выбрать команду Service Properties в меню Properties.

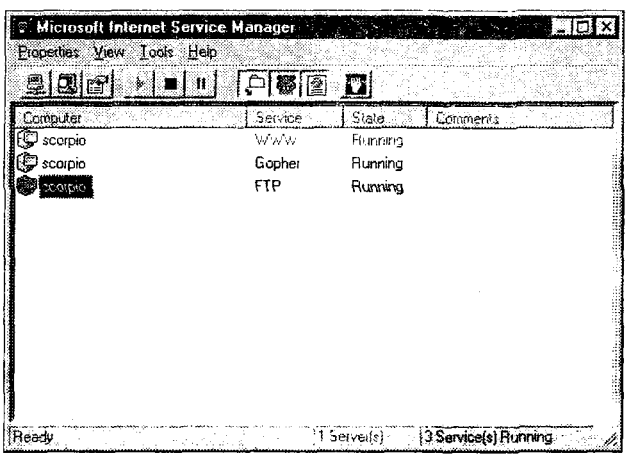


Рис. 13.6. Internet Service Manager используется для просмотра и настройки служб IIS

FTP

Служба FTP в IIS позволяет Windows NT Server играть роль сервера FTP. На рис. 13.7 показана вкладка Services окна FTP Service Properties. На этой вкладке вы можете произвести наиболее важную настройку службы FTP.

Вы можете настроить следующие параметры:

- **TCP Port** (вкладка Service). Номер TCP/IP-порта, используемого для управления передачей файлов. *Не* является хорошей идеей экспериментировать с этим параметром.
- **Connection Timeout** (вкладка Service). Интервал, в течение которого соединение может оставаться неактивным без его закрытия.
- **Allow Anonymous Connections** (вкладка Service). Сервер FTP может быть настроен на использование анонимных соединений.

Поля Username и Password позволяют указать имя пользователя и пароль для установления анонимного соединения.

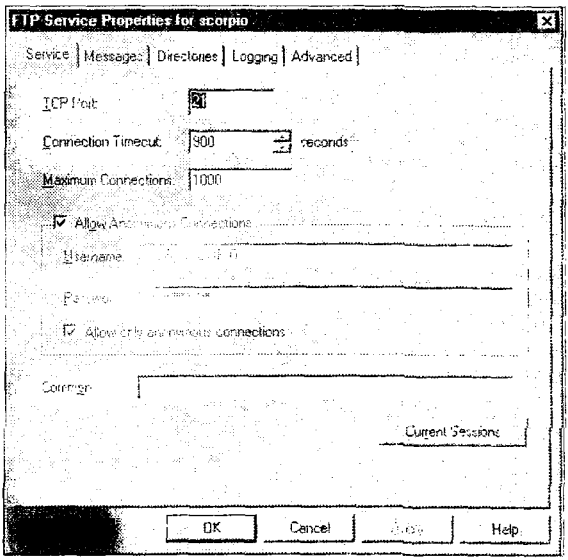


Рис. 13.7. Окно FTP Service Properties позволяет настроить службу FTP

- **Allow only anonymous connections** (вкладка Service). Этот флажок позволяет разрешить серверу использовать только анонимные соединения.
- **Вкладка Messages.** На этой вкладке могут быть указаны сообщения, выдающиеся пользователю при установлении и закрытии соединения, а также при превышении максимально допустимого числа открытых соединений.
- **Вкладка Directories.** На этой вкладке вы можете указать, к каким каталогам будут иметь доступ пользователи, установившие FTP-соединение с сервером.
- **Вкладка Logging.** На этой вкладке может быть создан и настроен файл журнала. Ведение журнала может автоматически производиться в SQL/ODBC базе данных.
- **Вкладка Advanced.** Настройки на этой вкладке могут использоваться для разрешения или запрета доступа одному компьютеру или целому блоку IP-адресов.

Gopher

Gopher — основанная на меню программа, позволяющая просматривать информацию без знания ее точного расположения. Она позво-

ляет вам производить поиск в списках ресурсов и отправляет найденный материал вам. Она также интегрирована с программами FTP и Telnet при помощи меню, что упрощает работу с ресурсами. Раньше Gopher широко использовалась для просмотра информации на серверах. Однако с ростом Всемирной паутины многие серверы Gopher умерли быстрой и безболезненной смертью.

Настройка службы Gopher идентична настройке службы FTP за одним исключением: для Gopher можно задать имя и адрес электронной почты администратора, которые сообщаются пользователям в качестве контактной информации.

WWW

Служба Всемирной паутины (служба WWW) предоставляет пользователям возможность просмотра HTML-документов. Серверы, использующие протокол HTTP для передачи HTML-документов, составляют большую часть того, что мы называем Интернетом. WWW может предоставлять информацию для просмотра как в интрасети, так и в Интернете. На рис. 13.8 показана вкладка Service окна WWW Service Properties.

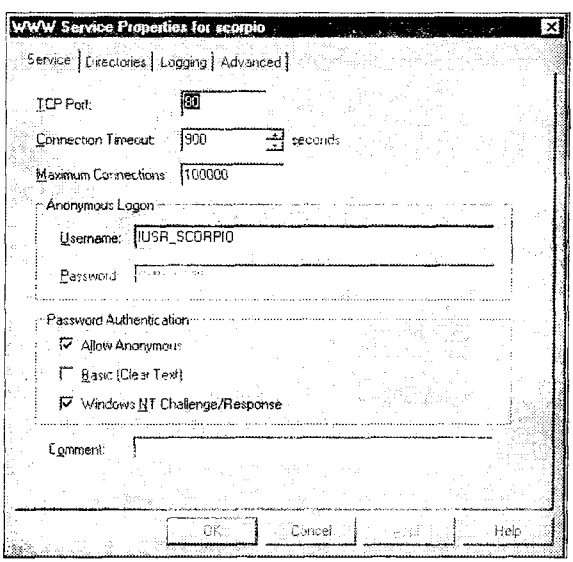


Рис. 13.8. Вкладка Service окна WWW Service Properties

Обратите внимание, что настройка этой службы аналогична настройке служб FTP и Gopher. Однако служба WWW может поддерживать

несколько виртуальных доменов, в то время как FTP поддерживает только одно имя домена, служба WWW также имеет следующие способы проверки пароля:

- Allow Anonymous (разрешить анонимное подключение).
- Basic (Clear Text) (простейший, обычный текст).
- Windows NT Challenge/Response (Windows NT протокол Challenge/Response).

TCP/IP-печать

В состав Windows NT Workstation 4 и Windows NT Server 4 входят три утилиты, обеспечивающие работу функций печати в смешанных Unix/Windows сетях. Чтобы использовать эти утилиты, вы должны загрузить службу печати Microsoft TCP/IP при помощи вкладки Services окна Network.

Установка NT TCP/IP-принтера (LPDSVC)

После того как служба печати TCP/IP будет установлена, TCP/IP-компьютер, такой как Unix-система, может выводить документ на принтер, подключенный к Windows NT. Эта служба также называется LPD (Line Printer Daemon, демон строчного принтера). LPD получает запросы на печать от LPR-клиентов (Line Printer Remote, удаленное управление принтером). LPR-клиенты — это, как правило, Unix-системы, однако программное обеспечение для работы LPR входит в большинство реализаций TCP/IP.

LPR

Windows NT устанавливает LPR-клиента одновременно со службой печати TCP/IP. Как мы упоминали ранее, LPR-клиенты отправляют запросы на печать серверам LPD. В этом случае Windows NT в состоянии отправить задание на печать Unix-системе (или другой системе), на которой работает LPD. Команда LPR вызывается из командной строки и имеет следующий синтаксис:

```
LPR -S сервер -P принтер [-C класс] [-J задание]
[-o параметр] [-x] [-d] файл
```

Список параметров LPR приведен в табл. 13.6.

Таблица 13.6. Параметры LPR

Параметр	Описание
-S сервер	Имя узла или IP-адрес компьютера, предоставляющего службу LPD
-P принтер	Имя очереди печати на сервере
-C класс	Класс задания для вывода на титульной странице
-J задание	Имя задания для вывода на титульной странице
-o параметр	Тип отправляемого на печать файла. По умолчанию — текстовый (ASCII). Используйте -o l для вывода бинарных файлов (файлов в формате Postscript).
-x	Указывает на необходимость совместимости с SunOS 4.1.x и более ранними
-d	Указывает, что файл данных должен быть отправлен первым
файл	Имя локального файла для печати

LPQ

Утилита LPQ используется для вывода информации о состоянии удаленной очереди печати. Например, после того как вы, использовав LPR, поставили задание в очередь печати, можете использовать команду LPQ, чтобы определить, было уже задание обработано или оно еще ожидает печати. LPQ также вызывается из командной строки и имеет следующий синтаксис:

```
LPQ -S сервер -P принтер -l
```

Параметры команды LPQ приведены в табл. 13.7.

Таблица 13.7. Параметры LPQ

Параметр	Описание
-S сервер	Имя узла или IP-адрес компьютера, предоставляющего службу LPD
-P принтер	Имя очереди печати на сервере
-l	Указывает на необходимость вывода подробной информации

Вопросы для подготовки к экзамену

Question 1

Which of the following commands can be used to execute a command on a remote system? (Check all correct answers.)

- ❑ A. RCP
- ❑ B. RSH
- ❑ C. REXEC
- ❑ D. RPD

Вопрос 1

Какие из следующих команд могут быть использованы для выполнения команды на удаленной системе? (Укажите все правильные ответы.)

- ❑ A. RCP
- ❑ B. RSH
- ❑ C. REXEC
- ❑ D. RPD

Правильные ответы на этот вопрос — B и C. Как RSH (удаленный интерпретатор командной строки), так и REXEC (удаленное выполнение команды) могут использоваться для исполнения команды на удаленной системе. Однако запомните, что для REXEC нужен пароль. RCP копирует файлы, и только. Следовательно, ответ A неверен. RPD — несуществующая команда. Следовательно, ответ D неверен.

Question 2

Which of the following will display the NetBIOS names that have been resolved via broadcast or WINS?

- ○ A. NETSTAT -R
- ○ B. NBTSTAT -R
- ○ C. NETSTAT -r
- ○ D. NBTSTAT -r

Вопрос 2

Какая из следующих команд покажет, какое количество имен NetBIOS определено при помощи широковещательных запросов, а какое — при помощи WINS?

- A. NETSTAT -R
- B. NBTSTAT -R
- C. NETSTAT -r
- d. NBTSTAT -r

Правильный ответ на этот вопрос — D, NBTSTAT -r. Запомните, что параметры -R и -r имеют для NBTSTAT различный смысл, а для NETSTAT — нет. Команда NBTSTAT -R вызовет очистку кэша и его перезагрузку из файла LMHOSTS, в то время как команда NETSTAT -R (или -r) выведет таблицу маршрутизации TCP/IP.

Question 3

Which of the following utilities is used to monitor printing on a remote Unix system?

- A. LPD
- B. LPQ
- C. LPR
- d. LPS

Вопрос 3

Какая из следующих утилит может использоваться для проверки состояния очереди печати на удаленной Unix-системе?

- A. LPD
- B. LPQ
- C. LPR
- d. LPS

Правильный ответ на этот вопрос — B. Запомните, что LPQ используется для проверки очереди (Queue) печати на удаленной системе. LPD — это демон, позволяющий печать с удаленных систем. Следовательно, ответ A неверен. LPR используется для отправки задания на удаленную систему. Следовательно, ответ C неверен. LPS — выдуманная команда, не имеющая никакого отношения к TCP/IP. Следовательно, ответ D неверен.

Question 4

Which of the following are services of IIS? (Check all that supply.)

- ❑ A. FTP
- ❑ B. LPD
- ❑ C. NETSTAT
- ❑ D. Gopher

Вопрос 4

Какие из следующих служб являются службами IIS? (Укажите все правильные ответы.)

- ❑ A. FTP
- ❑ B. LPD
- ❑ C. NETSTAT
- ❑ D. Gopher

Правильные ответы на этот вопрос – A и D. IIS включает службы FTP, Gopher и WWW. LPD входит в состав службы печати TCP/IP. Следовательно, ответ B неверен. NETSTAT входит в состав операционной системы NT. Следовательно, ответ C неверен.

Question 5

Which of the following utilities provide file transfer capabilities in a TCP/IP environment? (Check all that apply.)

- ❑ A. FTP
- ❑ B. RCP
- ❑ C. Telnet
- ❑ D. RSH

Вопрос 5

Какие из следующих утилит позволяют производить пересылку файлов в TCP/IP-сетях? (Укажите все правильные ответы.)

- ❑ A. FTP
- ❑ B. RCP
- ❑ C. Telnet
- ❑ D. RSH

Правильные ответы на этот вопрос — A и B. FTP является системой для передачи файлов с проверкой имени пользователя и пароля, в то время как команда RCP копирует файлы с или на удаленную систему, используя имена пользователей, указанные в файле «.rhosts». Telnet является программой эмуляции терминала и не предоставляет возможностей пересылки файлов. Следовательно, ответ C неверен. Команда RSH позволяет выполнить команду на удаленной системе, но не позволяет производить пересылку файлов. Следовательно, ответ D неверен.

Дополнительная информация

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы можете произвести поиск на компакт-диске TechNet (или на его версии в сети, доступной на www.microsoft.com), используя ключевые слова «NETSTAT», «NBTSTAT», «IIS», «LPR» и «LPD».

Реализация службы SNMP

Термины, необходимые для понимания материала:

- Запрос комментариев (RFC)
- Get-запрос
- Set-запрос
- Захват
- Назначение захвата
- База данных управляющей информации (MIB)
- Имена сообщества
- Агенты
- Диспетчеры
- Консоль диспетчера

Приемы и знания, которыми вы должны овладеть:

- Определение сообществ агентов и диспетчеров
- Планирование реализации SNMP
- Понимание того, как связаны процессы захвата и аутентификации
- Определение разницы между Get-запросом и Set-запросом
- Разрешение проблем, связанных с SNMP

В состав Windows NT входит служба SNMP, обеспечивающая возможность централизованного администрирования NT-компьютеров. Вопросы на эту тему входят как в экзамен по TCP/IP, так и в другие экзамены Microsoft, такие как NT Server 4 и NT Server 4 на предприятии. На связанные с SNMP вопросы не так уж сложно ответить, но вы должны иметь в виду, что в реальной жизни SNMP — очень быстро развивающаяся технология. В первых разделах этой главы мы исследуем SNMP, подробно обсудим базы данных управляющей информации (Management Information Base, MIB) и перейдем к реализации SNMP фирмой Microsoft. После этого мы предложим вашему вниманию обзор установки и настройки Microsoft SNMP и закончим обсуждением работы с SNMP. Мы советуем вам внимательно проработать вопросы для подготовки к экзамену в конце главы для достижения наилучшего результата.

SNMP: исследованный и объясненный

Простой протокол управления сетью (Simple Network Management Protocol, SNMP) — это несложный набор протоколов, разработанных для упрощения управления сетью. Когда в 70-х годах сети стали приобретать все более важное значение, они были еще небольшими и редко соединенными друг с другом. Но с ростом размеров и сложности сетей, а также с появлением каналов связи между различными сетями стал крайне нужен стандартный набор протоколов для наблюдения за сетями и управления ими. Итак, в 80-х годах в качестве «временной затычки» появился SNMP, который должен был исчезнуть с появлением более развитых инструментов. SNMP изначально разрабатывался как временная мера для обеспечения взаимодействия между различными типами сетей, но ничего лучшего не появилось, так что SNMP версии 2 все еще широко распространен и ожидается появление версии 3.

Запрос комментариев

Сетевые протоколы описываются IETF в сериях RFC (Request for Comments, запрос комментариев). RFC представляют собой группу документов, описывающих стандарты TCP/IP и внутреннее строение Интернета. SNMP не исключение — его развитие в основном управлялось RFC 1155 – RFC 1158, а также RFC 1213. RFC поддерживаются IESG (Internet Engineering Steering Group, управляющая инженерная группа Интернета). Вам также следует знать про существование IAB (Internet Architecture Board, комитет по архитектуре Интернета), который отвечает за установление стандартов Интернета и за управление процессом публикации RFC, а также за управление двумя подкомитетами IAB: IRTF и IETF.

Основателями SNMP считаются Маршал Роуз (Marshall Rose), вице-президент First Virtual Holdings, Inc., и Джеф Кейз (Jeff Case), президент SNMP Research.

Основой SNMP является простой набор спецификаций на сетевые взаимодействия. Эти спецификации покрывают основные задачи управления сетью, стремясь при этом быть максимально совместимыми с существующими сетями. SNMP работает за счет обмена сообщениями, содержащими сетевую информацию и известными как PDU (Protocol Data Unit, блок данных протокола). PDU можно представлять себе как объект, содержащий переменные, каждая из которых имеет имя и значение. SNMP в настоящий момент поддерживает пять типов PDU: один из них, так называемый «захват» (trap), используется для наблюдения за подключением и отключением оборудования; два других используются для получения терминальной информации; и два оставшихся — для установки терминальной информации.

Преимущества SNMP

Основные преимущества использования SNMP в качестве протокола управления сетью состоят в следующем:

- SNMP является хорошо проверенной и испытанной технологией, ее просто реализовать, не разрушая при этом существующую сеть.
- SNMP широко распространен; большинство производимых продуктов для межсетевой работы включают в себя SNMP, что упрощает его реализацию.
- Вам не требуется разрабатывать собственный интерфейс для управления сетью, если это не входит в планы вашей компании, поскольку такие программные продукты широко распространены.
- SNMP легко интегрируется с другими сетевыми технологиями. Он также является расширяемым, что упрощает его обновление при дальнейшем использовании.
- SNMP может легко объединяться в большие системы управления.
- SNMP предоставляет механизм, позволяющий управляющим консолям динамически получать информацию о новых компонентах и их оборудовании, следовательно, консоли, созданные год назад, могут управлять компонентами, разработанными сегодня.

Недостатки SNMP

SNMP, безусловно, не является совершенным инструментом для управления сетью, но он был умно разработан, поэтому почти всегда вы можете разрешить возникающие проблемы. Основные недостатки SNMP перечислены ниже:

- SNMP имеет серьезные проблемы с поддержкой политики безопасности, которые могут привести к несанкционированному доступу к информации и потенциально позволить неуполномоченному пользователю выключать оборудование.
- В SNMP отсутствуют усовершенствования (и связанная с ними дополнительная нагрузка), позволяющие получать подробную, высокоуровневую информацию, которая может понадобиться современным сетевым администраторам.

Терминология

В этой книге мы предполагаем, что вы уже знакомы с основными понятиями TCP/IP, однако управление сетью не всегда связывается с этой темой. Для поддержания у вас уверенности, что вам понятно, о чем речь, мы приводим краткий список терминов, относящихся к управлению сетью, которые мы будем использовать в этой главе.

- **Узел.** Любое сетевое устройство, в том числе рабочие станции и серверы. Узлы — это не только те устройства, которые могут управляться при помощи SNMP. SNMP часто используется для управления устройствами, работающими в глобальных сетях, такими как маршрутизаторы, концентраторы, переключатели и т. д.
- **Управляемые объекты.** Аппаратные и программные ресурсы узла, которые могут управляться и просматриваться с другого компьютера сети.
- **База данных управляющей информации (MIB, Management Information Base).** Файлы, находящиеся на узле и содержащие информацию об управляемых объектах этого устройства.
- **Управляющая консоль.** Любой компьютер, на котором запущен графический интерфейс для программного обеспечения, выполняющего функции диспетчера SNMP.

Агенты

В модели SNMP каждое сетевое управляемое устройство содержит компоненты программного обеспечения. Такой компонент называется *агентом* и содержит информацию об этом устройстве в хорошо структурированном виде. Агент отвечает за выполнение запросов к сетевому устройству и ответы на них. Когда агент получает запрос, он проверяет, исходит ли запрос от сообщества, к которому принадлежит агент. Если это так, агент обращается к базе данных управляющей информации (MIB) для этого запроса. Затем агент возвращает полученное из базы значение диспетчеру SNMP для данного сообщества или же, если агент получил set-запрос, изменяет значение

в базе. Также агент может отправить сообщение диспетчеру SNMP по собственной инициативе (такое сообщение называется захватом), предупреждая о попытках доступа неавторизованного диспетчера SNMP.

После того как агент начинает работу на устройстве, он ожидает SNMP-запрос от диспетчера. Когда запрос получен, агент выполняет одну из операций **get, get...next** или **set.** Единственная операция, происходящая без получения запроса, — захват. Эта операция предпринимается с целью сообщить диспетчеру, что устройство запущено, остановлено или находится в экстраординарном состоянии, например, при отсутствии свободного места на диске. По умолчанию компьютер использует порт 161 для обычных сообщений и порт 162 — для захватов. Отметим, для того чтобы использовать на одном компьютере, работающем под управлением Windows NT или Windows 95, несколько SNMP-агентов, требуется редактирование реестра.

Диспетчеры

Партнерами агентов являются так называемые *диспетчеры* или *управляющие консоли.* Диспетчер — это программный компонент, который позволяет отправлять сообщения, используя текстовый, графический или объектно-ориентированный интерфейс. Результаты запросов передаются пользовательскому интерфейсу, который позволяет администраторам просматривать информацию по запрашиваемому устройству. Обычно агент и диспетчер работают на различных сетевых устройствах и взаимодействуют через сеть при помощи общего протокола. Хотя Microsoft предоставляет простейшие управляющие SNMP-консоли, при необходимости выполнения более сложных задач вам может понадобиться мощь таких продуктов, как OpenView фирмы Hewlett-Packard или Sun Net Manager фирмы Sun, в качестве пользовательского интерфейса SNMP-диспетчера. Важное достоинство SNMP заключается в том, что вы можете подлаживать его под ваши нужды и финансовые возможности.

В некоторых случаях диспетчер отправляет агенту несколько последовательных запросов, не ожидая ответа. В других случаях он может отправлять следующий запрос только после получения ответа на предыдущий. Поскольку SNMP реализован на основе множества различных протоколов с различной степенью надежности и различными транспортными механизмами, обычным транспортным методом является их общий знаменатель — UDP. Поскольку UDP — протокол без установления соединения, каждое отдельное приложение-диспетчер должно иметь свою стратегию определения тайм-аутов и свою схему проверки.

MIB (База данных управляющей информации)

SNMP-агент состоит из набора частей, которые называются базами данных управляющей информации (MIB, Management Information Base). MIB является фактически файлом данных, содержащим значения объектов и спецификации управления объектом. MIB описываются на точно определенном языке, называемом «Абстрактная синтаксическая запись» (Abstract Syntax Notation, ASN). Вы можете считать, что это — один из компилируемых языков наподобие COBOL, FORTRAN или C. Управляющая консоль SNMP использует MIB для определения данных, обрабатываемых агентом SNMP, и предоставляет доступ к этим данным пользователю. Такая схема совместной работы агентов, MIB и диспетчеров позволяет агентам, разработанным сегодня, работать с диспетчерами, созданными несколько лет назад.

ASN позволяет определять типы данных, структуры и массивы структурной информации для управляемого устройства. MIB определяют для каждого объекта в агенте одно из следующего:

- Ассоциацию между записью данных для устройства и именем (идентификатором объекта, также называемым OID — Object Identifier).
- Определение типа данных для этого объекта.
- Текстовое описание объекта.
- Как объект индексируется (если объект является частью сложного типа данных).
- Какой доступ разрешен для этого объекта.

Несколько основанных на Windows NT MIB очень подробно описаны в приложении C *Windows NT Server Resource Kit.* Эти MIB по умолчанию поставляются с разработанными Microsoft продуктами. Их краткое описание следует ниже.

Internet MIB II

Internet MIB II была создана Microsoft для информационного сервера Интернета (Microsoft IIS), она содержит объекты, предоставляющие информацию о сетевых коммуникациях и производительности IIS. Она включает в себя Internet MIB I и является ее расширением, определяя 171 объект для анализа конфигурации и локализации сбоев сети. Из нее «выросли» несколько других MIB, в том числе FTP Server MIB, Gopher Server MIB и HTTP Server MIB. FTP Server MIB в основном предназначена для сбора статистики о работе сервера,

такой как общий объем переданной и полученной информации, количество анонимных пользователей, количество соединений и неуспешных попыток соединения. Поскольку они тоже предназначены для серверов, объекты Gopher MIB и HTTP MIB подобны объектам FTP MIB.

LAN Manager MIB II

Объекты этой MIB находятся в файле LMMIB2.MIB и описаны в документе Microsoft *LAN Manager 2.0 Management Information Base, LAN Manager MIB Working Group, Internet Draft: LanMgr-Mib-II*. Эта MIB поддерживает такие объекты, как предприятия, серверы, рабочие станции, домены и произвольные группы. В ней определены такие переменные, как синтаксис, доступ, статус и описание.

DHCP MIB II

Эта MIB содержит типы объектов, используемые для наблюдения за сетевым трафиком между удаленными узлами и сервером DHCP. Она содержит 14 параметров, включающих время запуска DHCP, общее количество выполненных и невыполненных запросов, таблицы контекста и адреса подсетей. DHCP MIB устанавливается автоматически при установке сервера DHCP и доступна при помощи удаленного DHCP Manager.

WINS MIB

Аналогично, WINS MIB содержит около 70 типов объектов, которые используются для наблюдения за сетевым трафиком между сервером WINS и удаленными узлами. Основное внимание уделено реально применимым объектам, таким как инициирующие и отвечающие службы WINS, последнее время обслуживания, обработка конфликтов в записях и трактовка записей в базе данных. Эта MIB также включает такие сложные темы, как плановая сборка мусора. WINS MIB, по всей видимости, является наиболее обширной из всех описанных MIB-примеров. Она автоматически устанавливается при установке сервера WINS и доступна при помощи удаленного WINS Manager.

Архитектура Microsoft SNMP

Теперь, после того как мы обсудили различные компоненты SNMP, давайте рассмотрим подробнее Microsoft SNMP. Хотя Windows не включает в себя управляющую консоль, она включает Win32 SNMP

API — программный интерфейс, соответствующий программному интерфейсу Windows Sockets. SNMP API может использоваться для разработки управляющих утилит третьими фирмами.

Кроме того, архитектура MIB является расширяемой, что позволяет сторонним разработчикам создавать динамически загружаемые библиотеки (Dynamic Link Libraries, DLL). Каждый объект в MIB идентифицируется при помощи иерархической схемы именования (рис. 14.1), разработанной IETF. Она позволяет однозначно присвоить каждому объекту универсальную метку, называемую идентификатором объекта (Object Identifier, OID). Такой OID уникален среди всех возможных OID; это позволяет всем разработчикам и производителям создавать новые компоненты и ресурсы с уникальными идентификаторами. IETF передает управление отдельными частями пространства имен отдельным организациям, таким как Microsoft.

Microsoft NT Server 4 работает с SNMP версии 1. SNMP реализован как 32-битная служба на компьютерах, которые используют протоколы TCP/IP и IPX на основе Windows Sockets. Установка TCP/IP на компьютер, работающий под управлением Windows NT, должна произ-

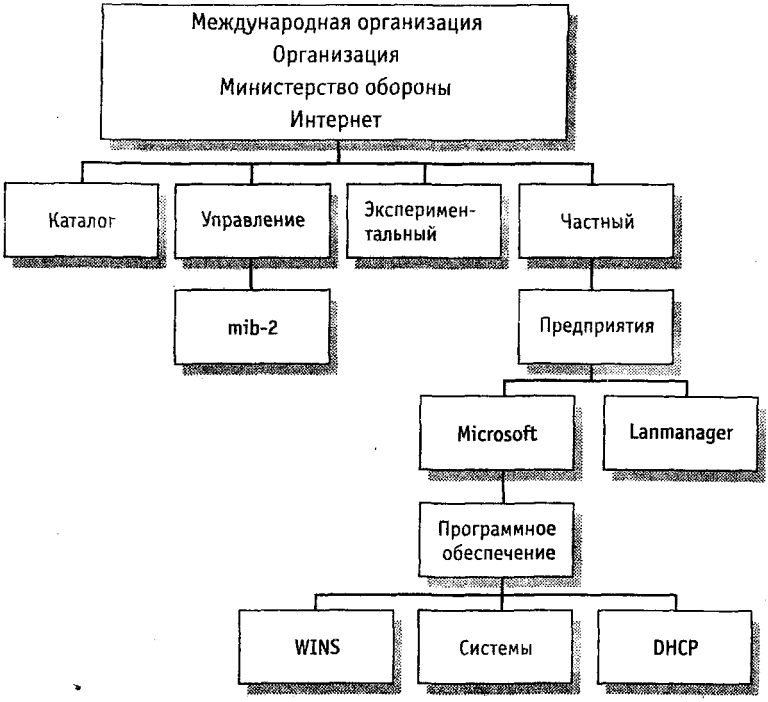


Рис. 14.1. Пример иерархии управляемых объектов

водиться до установки SNMP. Программы-агенты, которые реализуют дополнительные MIB для FTP, DHCP, WINS и служб Интернета, называются «агентами расширения». Агенты расширения работают с основной программой-агентом NT и реализованы как 32-битные DLL.

SNMP.EXE является службой SNMP Windows NT. Она представляет собой расширяемый агент SNMP, который позволяет разработчикам добавлять дополнительные DLL для работы с MIB сторонних производителей. Этот агент отвечает за получение SNMP-запросов от NT Workstation или NT Server и передачу этих запросов соответствующей DLL для обработки. Ответ на запрос возвращается агенту, который, в свою очередь, возвращает его аутентифицированной тоже управляющей станции, инициировавшей запрос. Расширяемый агент также имеет возможность отправки захватов от имени одной из DLL. Значения параметров в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents позволяют расширяемому агенту определить, какие DLL должны быть загружены.

Служба безопасности SNMP называется «службой аутентификации», поскольку управляющий запрос не будет обработан до того, как будет произведена аутентификация. SNMP использует имена сообщества как общие пароли, разделяемые между узлом и диспетчером для аутентификации запросов. Все SNMP-сообщения должны содержать имя сообщества. Если сообщение, полученное на каком-либо узле, содержит известное имя сообщества, то запрос выполняется. В противном случае запрос не выполняется и узел может послать сообщение-захват своей управляющей консоли о неуспешной попытке управления.

При установке SNMP по умолчанию используется имя сообщества «Public». Чтобы полностью разрешить работу службы SNMP, используйте окно диалога SNMP Service, доступное из меню Network Services, и удалите все имена сообществ, исключая Public. После этого служба SNMP будет обрабатывать все сообщения. Желательно это для вас или нет, но это является ожидаемым поведением, как указано в RFC 1157. Хотя эта возможность должна была быть компромиссом, она является наибольшей проблемой в обеспечении политики безопасности в SNMP. Многие администраторы используют имя сообщества по умолчанию — «Public», — не задумываясь, как широко они при этом открывают доступ в свои сети. Такое поведение не может быть рекомендовано ни при каких обстоятельствах.

Другой исполняемый файл, SNMPTRAP.EXE, получает SNMP-захваты от SNMP-агентов и пересылает их программному интерфейсу диспет-

чера SNMP на управляющей консоли. SNMPTRAP работает как процесс заднего плана и поэтому запускается только тогда, когда программный интерфейс диспетчера SNMP получает запрос диспетчера на обработку захватов.

Установка и настройка SNMP

Для того чтобы спланировать эффективную реализацию SNMP, администратор должен определить следующее:

- Работника, который будет выполнять роль локального администратора управляемого компьютера.
- Имена сообщества, разделяемые сетевыми узлами.
- IP-адрес, IPX-адрес или имя компьютера, на котором будет работать управляющая консоль SNMP.

Администратор должен определить имена сообществ и диспетчеров для этих сообществ. На рис. 14.2 приведен пример смешанной реализации сообществ, взятый из июльского издания Microsoft TechNet CD за 1997 год. В этом примере используются два сообщества: Engineering и используемое по умолчанию Public. Обратите внимание, что аген-

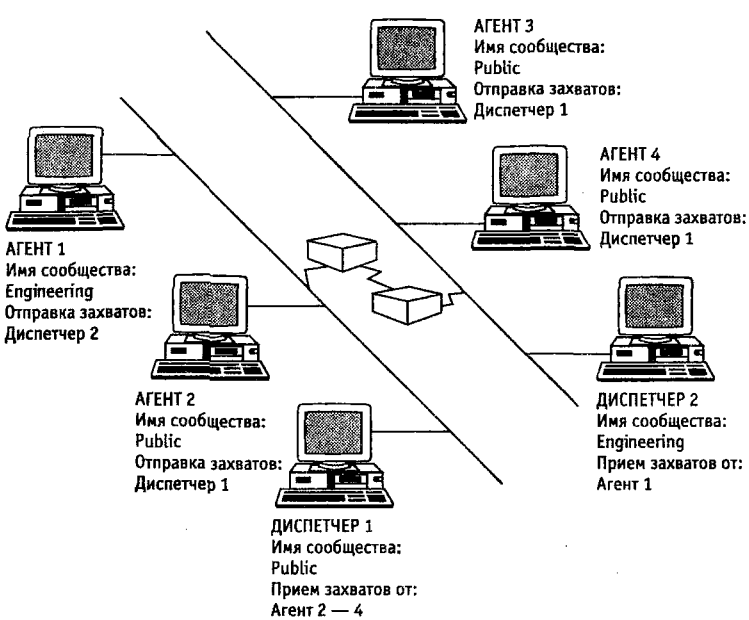


Рис. 14.2. Пример реализации смешанных SNMP-сообществ

ты и диспетчеры должны принадлежать к одному сообществу, чтобы иметь возможность взаимодействовать.

В этом примере Агент 1 может взаимодействовать только с Диспетчером 2, поскольку они принадлежат к одному сообществу: Engineering. Аналогично, Агент 2, Агент 3 и Агент 4 будут отправлять свои ответы и запросы Диспетчеру 1 в сообществе Public. Должно существовать как минимум одно имя сообщества.

Внимание

Имя сообщества по умолчанию в Windows NT — «Public».

После того как планирование будет закончено, можно переходить непосредственно к реализации SNMP. Для того чтобы вы могли установить службу SNMP (рис. 14.3), уже должна была быть проведена установка TCP/IP, даже если в качестве основного сетевого протокола установлен IPX. На клиенте, который будет получать сообщения-захваты, запустите IPCONFIG, чтобы определить его правильный IP-адрес. Затем вам следует установить агента, который будет отправлять сообщения-захваты. Для этого используйте кнопку Add в окне диалога Network Services.

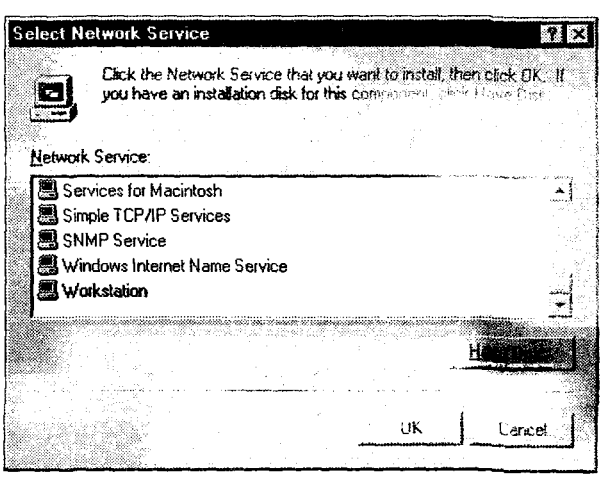


Рис. 14.3. Установка службы SNMP

После этого компьютер должен быть перезапущен. Затем вы можете настроить агенты, выбрав вкладку Agent в окне Microsoft SNMP Properties, открываемом со вкладки NT Network Services (рис. 14.4). Агенты Windows 95 должны настраиваться при помощи System Policy

Editor или редактирования реестра. Мы настоятельно рекомендуем вам ознакомиться с *Windows 95 Resource Guide*, быть любознательными и сохранять резервную копию реестра перед тем, как внести в него изменения.

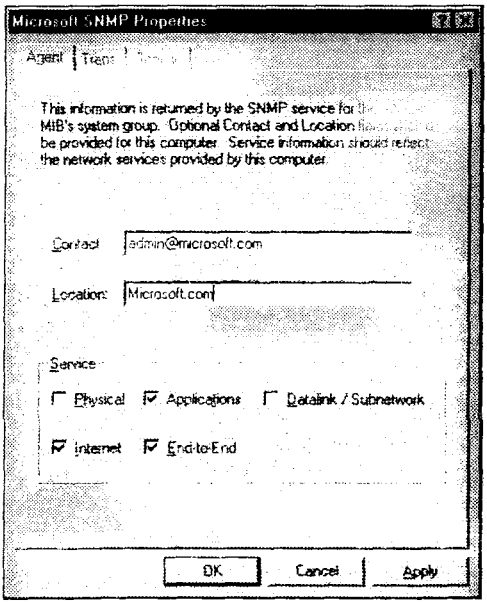


Рис. 14.5. Свойства SNMP и службы по умолчанию

Свойства SNMP, которые могут быть настроены на компьютерах, работающих под управлением Windows NT, — это Agent, Traps (рис. 14.5) и Security. Если вас устраивают настройки по умолчанию, вам требуется ввести только контактный адрес электронной почты администратора (например, admin@microsoft.com) и его месторасположение (microsoft.com). Вы можете выбрать следующие службы: Physical, Applications, Datalink/Subnetwork, Internet и End-to-End. Параметры по умолчанию изображены на рис. 14.4.

На компьютере, работающем под управлением Windows NT, вы можете использовать вкладку Traps в окне диалога SNMP Properties для того, чтобы указать, куда должны отправляться сообщения-захваты.

Внимание

Узел, на который будут отправляться сообщения-захваты, может быть указан при помощи имени узла, IP-адреса или IPX-адреса.

Для каждого имени сообщества захваты могут настраиваться отдельно. Сообщение-захват может отправляться не более чем пяти узлам в

каждом сообществе. В поле со списком Send Traps With Community Name введите IP-адрес, IPX-адрес или имя узла для компьютера, на который будут отправляться сообщения-захваты, и нажмите кнопку Add,

Имена сообществ определяются на вкладке Security (рис. 14.6).

Внимание

На вкладке Security должно быть определено хотя бы одно имя сообщества.

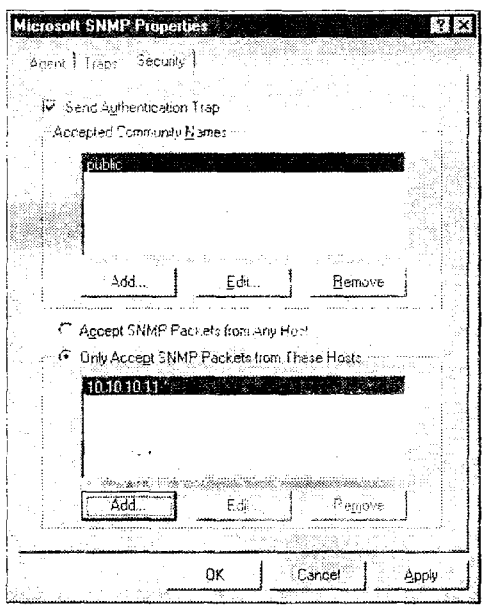


Рис. 14.6. Вкладка Security окна диалога Microsoft SNMP Properties

На этой вкладке вы также можете задать фильтр, указав, какие типы пакетов и с каких узлов будет принимать данный компьютер.

Теперь, после того как SNMP установлен и настроен для агента и диспетчера, давайте посмотрим, как все это работает в сетях Microsoft.

SNMP в действии

Реализация Microsoft поддерживает четыре основных типа команд. Команда **get** является запросом значения определенного объекта в MIB, находящейся на агенте. Команда **get-next** является запросом следующего значения объекта в MIB и используется для получения

последовательных значений в какой-либо ветви или подмножестве MIB. Команда **set** может использоваться для изменения значения объекта, если данный объект в MIB допускает запись. Для обеспечения безопасности многие объекты MIB позволяют доступ к своим значениям только на чтение.

Агент SNMP также генерирует сообщения-захваты (trap), которые отправляются указанному при настройке узлу: управляющей консоли SNMP. Вы можете указать, на какой узел отправлять сообщения-захваты, но когда отправлять такое сообщение, решает сам агент. Результаты операций отправляются программе-диспетчеру, которая ожидает SNMP-сообщения от агентов. Диспетчер отображает информацию на управляющей консоли SNMP или сохраняет данные в указанном файле или базе данных для последующего анализа. Мы выше обсуждали, что служба SNMP Windows NT является агентом SNMP, который, в свою очередь, является необходимой частью системы управления сетью. Однако отдельная программа-диспетчер SNMP должна выполнять управляющие операции. Схема процесса работы SNMP показана на рис. 14.7.

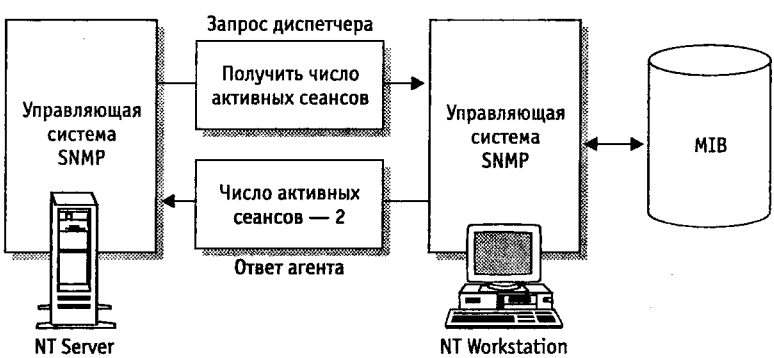


Рис. 14.7. Схема работы SNMP

Что может делать SNMP, кроме простейшего наблюдения за устройствами? После установки сетевой администратор может просматривать и устанавливать параметры для любого сервера WINS, а также наблюдать за серверами DHCP, используя расширяемые агенты, предоставляемые NT. Кроме того, могут просматриваться и изменяться параметры LAN Manager и баз MIB II. Performance Monitor после установки SNMP позволит наблюдать за производительностью TCP/IP, а именно производительностью ICMP, IP, сетевого интерфейса, TCP, UDP, DHCP, FTP, WINS и IIS. Вы сможете просматривать эти показатели, создав при помощи утилиты Perf2MIB, входящей в состав

Windows NT Server Resource Kit, новые файлы MIB для интересующих вас показателей. Простейшие функции SNMP-диспетчера могут быть найдены на компакт-диске *Windows NT Server Resource Kit*, или же вы можете использовать более высокоуровневые продукты сторонних производителей, например OpenView фирмы Hewlett-Packard.

После установки SNMP будет автоматически запускаться при загрузке компьютера. Однако, если SNMP будет остановлен, вы должны перезапустить его вручную. Обратите внимание, что остановка службы обрывает все сетевые соединения, которые могла использовать эта служба, поэтому пользуйтесь этой возможностью осторожно. Запуск и остановка службы SNMP могут быть произведены из командной строки (при помощи команд net start snmp и net stop snmp) или при помощи панели управления (в окне Services выделите службу SNMP и используйте кнопки Start и Stop). Эти действия необходимы при установке дополнительных DLL, расширяющих агент, а также при установке новых MIB.

Что вы должны сделать в случае возникновения проблем при установке SNMP? К счастью, обработка ошибок была включена в NT Server 4 и NT Workstation 4. Это улучшение хорошо заметно в графическом интерфейсе программы Event Viewer (рис. 14.8). Вы можете произвести фильтрацию списка событий, чтобы выделить только события, имеющие отношение к SNMP.

Реестр содержит информацию о расширяющих агент DLL и параметрах агента. Вы должны применять соответствующие пользовательские утилиты для редактирования реестра только после сохранения резервной копии реестра. На компьютерах, работающих под управлением Windows NT, соответствующие параметры находятся в разделе реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\SNMP\Parameters. В разделе HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\SNMP\Parameters\EnableAuthenticationTraps можно также задать, будет или нет служба SNMP отправлять сообщение-захват при получении запроса с неизвестным именем сообщества или фильтром узла (по умолчанию сообщение-захват отправляется). Также этот раздел позволяет указывать, какие расширяющие агент DLL должны быть загружены, корректные имена сообществ, узлы, на которые отправляются сообщения-захваты, и их расположение.

Вы должны убедиться, что при установке службы был указан правильный IPX-адрес узла, на который отправляются сообщения-захваты. В противном случае вы можете получить ошибку с кодом 3 при перезапуске компьютера. Этот код ошибки указывает, что IPX-адрес был введен неправильно. Имейте в виду, что IPX-адрес должен

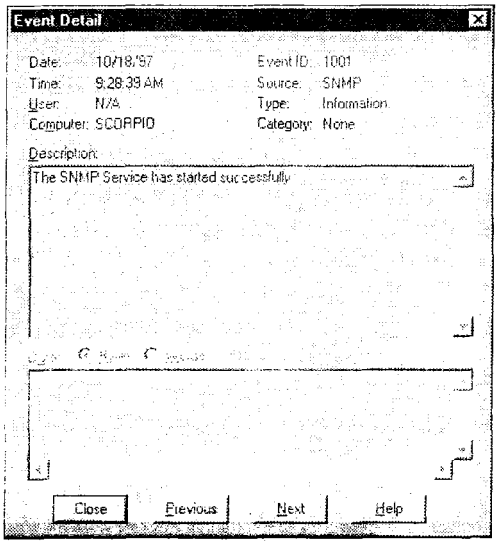


Рис. 14.8. Пример вывода программы Event Viewer для событий, связанных с SNMP

соответствовать требованиям SNMP-агента Microsoft, который не позволяет использовать запятые или дефисы (хотя некоторые популярные программы сторонних производителей позволяют вам это). Адрес узла, на который отсылаются сообщения-захваты, должен быть указан в формате «8.12» для сетевых номеров и MAC-адресов: xxxxxxxx.yyyyyyyyyyyy, где xxxxxxxx означает сетевой номер, а yyyyyyyyyyyy — MAC-адрес.

Следующее поколение

В этой главе мы рассказали вам об основах SNMP, а также о его агентах, диспетчерах и MIB. Вы познакомились с реализацией SNMP фирмой Microsoft, узнали, как установить и настроить SNMP, а также как устранить возникшие проблемы. Даже если вопросы по этой теме не будут включены в экзамен, мы думаем, что вам было бы интересно узнать о перспективах развития SNMP и о том, как это может повлиять на вашу работу.

Рабочая группа IETF по SNMPv2 пытается реализовать лучшую поддержку политики безопасности и другие необходимые SNMP улучшения, но она никогда не была в состоянии приспособиться к различным взглядам на SNMP. В связи с этим возникли два разных подхода (обычно называемые V2u и V2*). Поскольку IETF не пре-

успела в значительном улучшении SNMP при переходе к SNMPv2, версия 1 все еще остается основной в сегодняшней индустрии. Для того чтобы исправить это положение в SNMPv3, была сформирована группа, называемая Security and Administrative Framework Evolution for SNMP Advisory Team, или просто Advisory Team (Комитет по развитию поддержки политики безопасности и управляющих систем для SNMP). Основной целью этой группы является создание единого рекомендуемого подхода к развитию SNMP. Этот комитет также работает над определением MIB для специальных управляющих операций, для фильтрации уведомлений и для прокси-ретрансляции. Поскольку хорошо понятно, что быстрое завершение этого проекта должно сыграть большую роль в продолжении успеха SNMP, комитет надеется достигнуть целей обновления SNMP в соответствии с современными требованиями и ужесточающейся политикой безопасности, основываясь на следующих принципах:

- Использование настолько большой части разработок группы по созданию SNMPv2, насколько возможно.
- Приспособление разнообразных операционных окружений к различным задачам управления.
- Упрощение перехода к SNMPv3 от различных использовавшихся ранее протоколов.
- Упрощение процесса установки и администрирования.

Что это значит для вас — будущего профессионала Microsoft? Это означает, что была сделана попытка обеспечить жизнеспособность простого, удобного для работы стандарта для наблюдения за сетью и управления ей, будь то современная сеть или глобальная сеть будущего. Эта также значит, что важность простоты и функциональности в постоянно усложняющейся области наконец-то была осознана.

Вопросы для подготовки к экзамену

Question 1

What types of transactions can be performed by an SNMP agent?

- ❑ A. VARBIND
- ❑ B. GET
- ❑ C. GETALL
- ❑ D. Send trap

Вопрос 1

Какие типы взаимодействия может выполнять агент SNMP? (Укажите все правильные ответы.)

- ❑ A. VARBIND
- ❑ B. GET
- ❑ C. GETALL
- ❑ D. Отправка сообщения-захвата

Правильные ответы – B и D. Агент только отвечает на запросы, за исключением экстренных ситуаций, в которых он отправляет сообщение-захват на указанный узел. Одним из примеров такой ситуации является завершение работы узла. VARBIND – это структура данных, которая состоит из OID и структуры-значения. Следовательно, ответ A неверен. Такой команды, как GETALL, не существует. Следовательно, ответ C неверен.

Question 2

What types of devices can be monitored using SNMP? (Check all correct answers.)

- ❑ A. Hubs.
- ❑ B. Windows NT hosts.
- ❑ C. Terminal servers.
- ❑ D. Routers, bridges, and gateways.

Вопрос 2

За какими типами устройств можно наблюдать при помощи SNMP? (Укажите все правильные ответы.)

- ❑ A. Концентраторы.
- ❑ B. Узлы, работающие под управлением Windows NT.
- ❑ C. Терминальные сервера.
- ❑ D. Маршрутизаторы, мосты и шлюзы.

Все ответы правильны, если соответствующие устройства имеют возможность поддержки SNMP, включенную в них при разработке, и если существует соответствующая MIB.

Question 3

A request is sent to an SNMP-managed device, but no response is obtained. Assume the community name is correct, the OID is correct, and a request with other OIDs does elicit a response. What could be the problem?

- A. This is not a manageable device.
- B. The network is unstable.
- C. The request is a SET request.
- D. There is no alarm condition.

Вопрос 3

Управляемому при помощи SNMP устройству был отправлен запрос, но ответа получено не было. Предположим, что имя сообщества, указанное в запросе, верно, OID также правилен и запрос с другими значениями OID вызывает ответ. В чем может быть проблема?

- A. Устройство не является управляемым.
- B. Сеть нестабильна.
- C. Был отправлен SET-запрос.
- D. Нет экстренной ситуации.

Правильный ответ – C. SET-запрос — это запрос, вызывающий определенные действия со стороны агента, и ответ на него не обязателен. Ответ A неверен, поскольку в вопросе сказано, что устройство управляемое. Ответ B не подходит, поскольку запросы с другими OID вызывают ответы. В случае экстренных ситуаций отправляет сообщение-захват. Следовательно, ответ D неверен.

Question 4

What is an SNMP trap?

- A. PDU
- B. UDP
- C. Request
- D. Alarm

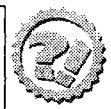
Вопрос 4

Что такое SNMP-захват?

- ○ A. PDU
- ○ B. UDP
- ○ C. Запрос
- ○ D. Предупреждение

Ответ D правилен. Сообщение-захват отправляется на указанный узел, чтобы предупредить диспетчер SNMP о необычных ситуациях, таких как запуск или останов системы, отсутствие места на диске или неверный пароль. По умолчанию агент SNMP не отправляет сообщений-захватов; он должен быть настроен на их отправку. PDU (Protocol Data Unit) — это транспортный метод, используемый SNMP. Следовательно, ответ A неверен. UDP — транспортный протокол без установки соединения и возможности подтверждения получения. Следовательно, ответ D неверен. Запрос может быть SNMP-запросом информации или запросом на выполнение определенных действий. Следовательно, ответ C неверен.

Question 5



Three attributes can be defined in the Only Accept SNMP Packets From These Hosts section of the SNMP Security tab. Which ones are they? (Check all correct answers.)

- ☐ A. MAC address
- ☐ B. IP address
- ☐ C. IPX address
- ☐ D. Host name

Вопрос 5

В области Only Accept SNMP Packets From These Hosts вкладки SNMP Security могут быть установлены три атрибута. Какие? (Укажите все правильные ответы.)

- ☐ A. MAC-адрес
- ☐ B. IP-адрес
- ☐ C. IPX-адрес
- ☐ D. Имя узла

Правильные ответы — B, C и D. MAC-адрес является атрибутом IPX и не устанавливается в области Only Accept SNMP Packets From These Hosts вкладки SNMP Security. Следовательно, ответ A — неверен.

Question 6

You are network administrator in the Big Enormous Comporation, and BEC policy dictates very strict data security. You want to monitor the Engineering PCs for unauthorized access, because very sensitive design data is kept on these computers. *You set up the SNMP agent on each client and designate two SNMP trap destinations* for the management console.You assign both of these SNMP servers to a single community known as Engineering and designate the host names of one of the two servers as the trap destination for the Engineering community. In the Security tab of the SNMP configuration at each client, you select the community name of Engineering and check the Accept SNMP Packets From Any Host box. How well does this solution fit the criteria?

- A. Meets the requirements and is an outstanding solution.
- B. Meets the requirements and is an adequate solution.
- C. Meets the requirements but is not a desirable solution.
- D. Does not meet the requirements, although it appears to work.

Вопрос 6

Вы являетесь сетевым администратором в Ненормально Большой Компании, и политика вашей фирмы требует реализации строгой политики безопасности. Вы хотите отслеживать попытки несанкционированного доступа к компьютерам инженерного отдела, поскольку на них хранятся крайне важные конструкторские разработки. Вы настроили агент SNMP на каждом компьютере и две управляющие консоли для приема SNMP-захватов. Оба эти сервера SNMP находятся в одном сообществе Engineering, и вы установили имя узла одного из этих серверов в качестве пункта назначения для сообщений-захватов сообщества Engineering. На вкладке Security окна настройки SNMP каждого клиента вы выбрали в качестве имени сообщества Engineering и установили переключатель Accept SNMP Packets From Any Host. Насколько хорошо это позволит решить ваши проблемы?

- A. Требования выполняются; это выдающееся решение.
- B. Требования выполняются; это решение адекватно поставленным задачам.
- C. Требования выполняются; решение посредственное.
- D. Требования не выполняются, хотя кажется, что все работает правильно.

Правилен ответ D, поскольку все будет работать, но требование жесткой политики безопасности не выполняется. Поскольку переключатель Accept SNMP Packets From Any Host установлен, то будут обрабатываться все SNMP-запросы, вне зависимости от идентификатора исходного узла, и ваша сеть будет открыта для вторжения. Если бы был установлен переключатель Accept SNMP Packets From These Hosts, то вы могли бы контролировать доступ и SNMP был бы настроен правильно.

Question 7

Once SNMP service is installed, an administrator can do which of the following? (Check all correct answers.)

- ❑ A. View and change parameters in the MIBs by using SNMP manager programs.
- ❑ B. Monitor and configure parameters for any WINS server.
- ❑ C. Monitor and configure parameters for any DHCP server.
- ❑ D. Use the *Resource Kit* utilities to perform management functions.

Вопрос 7

После установки SNMP администратор получает возможность... (Укажите все правильные ответы.)

- ❑ A. Просматривать и изменять параметры MIB, используя диспетчер SNMP.
- ❑ B. Просматривать и изменять параметры любого сервера WINS.
- ❑ C. Просматривать и изменять параметры любого сервера DHCP.
- ❑ D. Использовать утилиты из *Resource Kit* для выполнения управляющих функций.

Верны только ответы B и D. После установки SNMP администратор может просматривать и изменять параметры любого сервера WINS и использовать утилиты из *Resource Kit*. Ответ A верен частично; после установки службы SNMP администратор может просматривать и изменять параметры только баз данных управляющей информации LAN Manager и MIB II, но не всех. Ответ C неверен, потому что администратор может только наблюдать за сервером DHCP, но не изменять его параметры.

Question 8

The network administrator can view performance counters on a computer after installing SNMP. How is this accomplished?

- ○ A. By editing the Registry key KEY\LOCAL_MACHINE\System\CurrentControlSet\Services\Snmp\Parameter.
- ○ B. By editing the Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Snmp\Parameters.
- ○ C. By using the Perf2MIB utility to create new MIB files.
- ○ D. By using the management console user interface.

Вопрос 8

Сетевой администратор хочет наблюдать за производительностью компьютера *после установки* SNMP. *Как это может быть достигнуто?*

- A. Редактированием раздела реестра KEY\LOCAL_MACHINE\System\CurrentControlSet\Services\Snmp\Parameter.
- B. Редактированием раздела реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SNMP\Parameters.
- C. Использованием утилиты Perf2MIB для создания новых файлов MIB.
- D. Использованием интерфейса управляющей консоли.

Правильный ответ – C. Вы можете использовать утилиту Perf2MIB для создания новых файлов MIB, содержащих те показатели производительности, которые интересуют администратора. Ответ A неверен, поскольку использован неверный синтаксис; кроме того, реакции SNMP определяются MIB, а не значениями реестра. В ответе B используется правильный синтаксис для раздела реестра, но этот ответ также неверен, поскольку реакции SNMP определяются MIB, а не значениями реестра, хотя реестр может содержать необходимую информацию. Значения реестра в разделе HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SNMP\Parameters позволяют указать, какие DLL должны быть загружены агентом. Пользовательский интерфейс управляющей консоли может выводить показатели производительности только после того, как будут созданы соответствующие MIB, описывающие управляемые объекты, отражающие требуемые показатели производительности узла. Следовательно, ответ D неверен.

Question 9

How should the administrator troubleshoot SNMP errors?

- A. By choosing Start ➤ Programs ➤ Event Viewer.
- B. By changing the Security parameters to Accept SNMP Requests From These Hosts.
- C. By editing the Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Snmp\Parameter
- D. By using the Performance Monitor to monitor TCP/IP-related counters.

Вопрос 9

Как администратор должен производить поиск и устранение проблем SNMP?

- A. Выбрав в меню Start команду Programs ➤ Event Viewer.
- B. Установив на вкладке Security переключатель Accept SNMP Requests From These Hosts.
- C. Редактируя раздел реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Snmp\Parameter.
- D. Используя Performance Monitor для наблюдения за производительностью TCP/IP.

Правильный ответ — A. Ключ к поиску проблем в SNMP — Event Monitor, который был существенно улучшен в NT 4. Если переключатель Accept SNMP Requests From These Hosts установлен, то агент будет принимать запросы и отправлять ответы и сообщения-захваты только указанным узлам. Следовательно, ответ B неверен. Редактор реестра необходим для запуска нескольких агентов SNMP, но он не нужен для поиска ошибок. Следовательно, ответ C неверен. Performance Monitor может быть использован для поиска и устранения проблем только после того, как будут созданы соответствующие MIB. Следовательно, ответ D неверен.

Дополнительная информация

Microsoft TechNet, July, 97, Volume 5, Issue 7 содержит множество статей о SNMP. Простой поиск слова «SNMP» — все, что требуется для того, чтобы найти нужную информацию.

Существует множество групп новостей и Web-узлов, которые посвящены SNMP, в том числе:

- news:comp.protocols.snmp
- http://www.iol.unh.edu/consortiums/netmgt/rfc-snmprel.html
- http://ds.internic.net/
- http://netman.cit.buffalo.edu/Papers.html
- ftp://SunSITE.unc.edu/pub/micro/pc-stuff/ms-windows/winsnmp/winsnmp_app

Производительность, настройка и оптимизация

Термины, необходимые для понимания материала:

- *Скользящее окно*
- TTL
- Идентификатор контекста

Приемы и знания, которыми вы должны овладеть:

- Понимание последовательности подтверждения приема
- Понимание параметров реестра, имеющих отношение к производительности TCP/IP
- Знание утилит, позволяющих наблюдение за производительностью TCP/IP
- Знание следствий использования идентификаторов контекста

Множество различных факторов влияют на производительность и настройку TCP/IP. Первое и наиболее важное, что вам следует отметить, — это то, что TCP/IP, и особенно реализация Microsoft, большей частью является самонастраивающейся системой. Однако на экзамене вы должны знать, как наблюдать за TCP/IP и настраивать его и как управлять трафиком NetBIOS.

Основные факторы, влияющие на производительность

На производительность TCP/IP влияет множество факторов — начиная от скорости локальной или глобальной сети до топологии сети. Даже тип используемого метода передачи данных (асинхронный или синхронный) влияет на производительность.

Одним из основных факторов, определяющих производительность TCP/IP, является то, что по умолчанию получение каждого переданного фрагмента должно быть подтверждено перед началом передачи следующего фрагмента. Вы можете понять, как медленно работает этот процесс, используя асинхронную передачу (один символ за один раз) и Telnet для связи с удаленной системой по каналу связи с пропускной способностью 56К. Огорчает, чтобы не сказать больше.

Чтобы попытаться разрешить эту проблему, TCP/IP позволяет пользователю указать количество фрагментов, которые должны быть приняты до отправки подтверждения. Количество фрагментов, которые компьютер принимает без отправки подтверждения, называется «окном» или «скользящим окном». Не беспокойтесь; все сейчас станет понятно. Давайте посмотрим, как происходит процесс подтверждения приема.

Конфигурация по умолчанию, показанная на рис. 15.1, имеет размер окна, установленный в 1, что вызывает отправку принимающим компьютером подтверждения (ACK) после приема каждого пакета. Напомним, что принимающий компьютер подтверждает получение данных, запрашивая следующий пакет.

Наоборот, если размер окна велик, отправляющий компьютер ожидает ACK не после каждого пакета, а после отправки группы пакетов. На рис. 15.2 размер скользящего окна установлен в 4, что требует от получателя подтверждения после каждого четвертого пакета.

Конечно, TCP/IP ожидает подтверждения после каждого пакета для обеспечения надежности передачи. Когда получение каждого пакета подтверждено, то при случайной потере одного из пакетов получатель

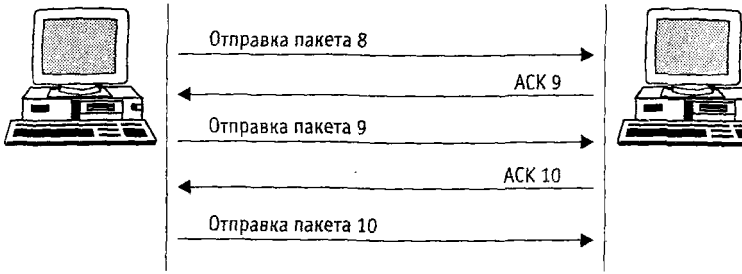


Рис. 15.1. По умолчанию компьютер, использующий TCP/IP, подтверждает получение каждого пакета

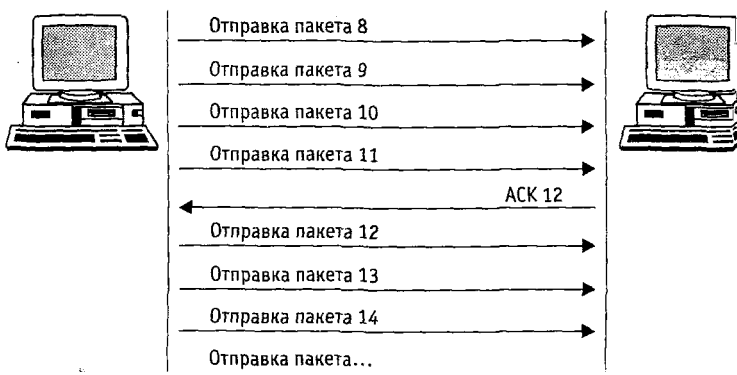


Рис. 15.2. Увеличение размера окна приводит к уменьшению количества ACK-пакетов

просто запрашивает его повторную отправку. Запомните, что TCP/IP-подтверждение на самом деле является запросом пакета с следующим номером; следовательно, если фрагмент 3 не достиг пункта назначения, то принимающий компьютер отправляет подтверждение, которое гласит: «Отправьте фрагмент 3 снова». Отправитель повторяет передачу фрагмента 3, ожидает подтверждения приема и переходит к фрагменту 4. Что происходит, если размер скользящего окна больше, чем 1, и происходит потеря пакета? Как вы могли догадаться, эта ситуация обрабатывается слегка по-другому. На рис. 15.3 изображена схема обработки потери пакета при размере окна 3.

В этом примере не был получен фрагмент 12, но был получен фрагмент 13. Как вы можете видеть из рисунка, принимающий компьютер подтверждает получение фрагмента 11, запрашивая фрагмент 12. Производится повторная отправка фрагмента 12, и принимающий

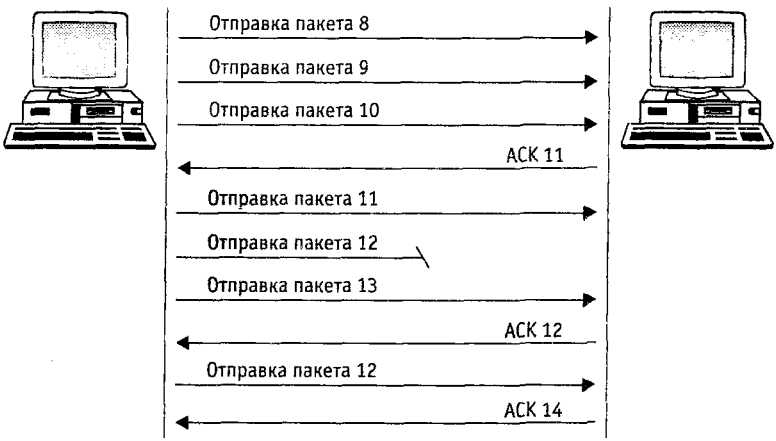


Рис. 15.3. Потерянный пакет обрабатывается иначе, если размер окна больше, чем 1

компьютер подтверждает прием фрагмента 13, запрашивая фрагмент 14 и продолжая передачу.

Размер отправляющего окна на каждом компьютере определяется при установлении TCP/IP-соединения. Он устанавливается равным размеру принимающего окна на другом конце соединения.

Методы настройки

Windows NT содержит несколько параметров реестра, которые могут использоваться для настройки поведения TCP/IP. Однако, как мы упоминали выше, TCP/IP является самонастраивающимся протоколом, и параметры, упомянутые ниже, должны добавляться вручную при помощи редактора реестра. Запомните, что любые изменения повлияют на TCP/IP в целом, а не только на один сеанс или тип протокола. Мы рекомендуем не производить никаких изменений, если это не является абсолютно необходимым.

Параметры реестра, используемые для настройки TCP/IP, содержатся в подразделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters. Они имеют тип «двойное слово» (DWORD) и добавляются при помощи редактора реестра (Regedit или regedt32). На рис. 15.4 показан процесс создания параметра при помощи Regedit; на рис. 15.5 показано выполнение той же задачи при помощи regedt32. Какой редактор вы будете использовать — исключительно дело вкуса.

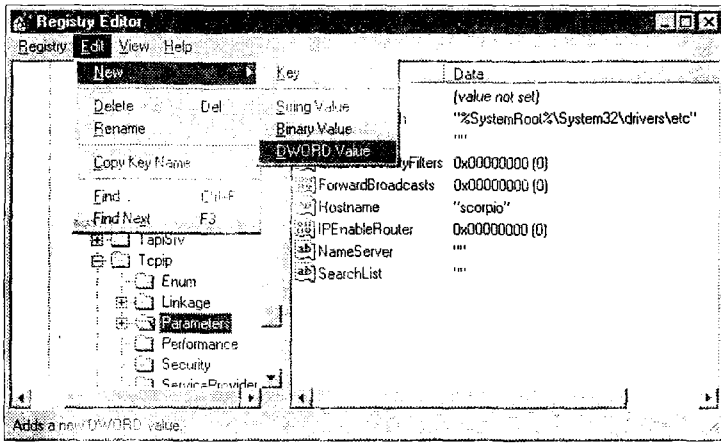


Рис. 15.4. Пример создания нового параметра типа DWORD при помощи Regedit

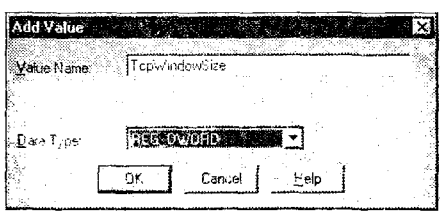


Рис. 15.5. При помощи утилиты regedt32вы можете создавать новые параметры, выбрав команду Add Value из меню Edit

После того как вы добавите параметры в реестр, вы легко можете изменить их значения. На рис. 15.6 показана процедура изменения значения параметра при помощи Regedit.

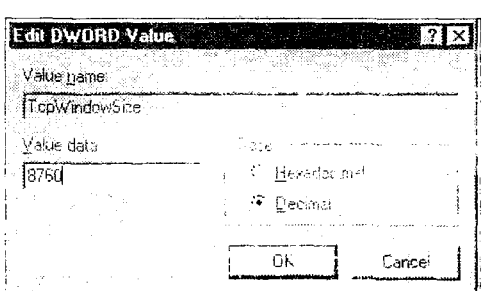


Рис. 15.6. Значения параметров реестра должны вводиться в десятичном формате

Ниже перечислены параметры, которые могут использоваться для настройки TCP/IP на компьютере, работающем под управлением Windows NT:

- **TcpWindowsSize.** Этот параметр задает размер принимающего скользящего окна для данного компьютера. Значение этого параметра задает размер не в полученных фрагментах, а в полученных байтах. Это связано с тем, что различные аппаратные средства (например, Ethernet и Token Ring) используют различный размер фрагмента. Это значение обычно не меньше, чем 8192 (8 Кбайт), если оно не изменялось вручную. Например, на системе, подключенной к Ethernet, оно по умолчанию равно 8760. Это размер 6 Ethernet-пакетов (размер одного пакета — 1460 байт).
- **ForwardBufferMemory.** Этот параметр используется только на системах с несколькими сетевыми интерфейсами, которые маршрутизируют TCP/IP-пакеты. Он определяет количество памяти, которое может использоваться для очереди маршрутизатора. Если размер буфера слишком мал, то компьютер будет терять пакеты. Значение по умолчанию — 72240, что позволяет сохранить 50 пакетов размером в 1480 байт (лишние 20 байт составляют разницу между TCP- и IP-заголовками, оставив при этом немного свободного места. Если компьютер постоянно маршрутизирует значительные объемы данных, возможно, увеличение размера этого буфера — хорошая идея. Если параметр IPEnableRouting установлен равным 0 (IP-маршрутизация запрещена), то параметр ForwardBufferMemory игнорируется.
- **NumForwardPackets.** Этот параметр работает в сочетании с параметром ForwardBufferMemory и определяет количество IP-пакетов, которые могут быть сохранены в очереди маршрутизатора. Значение по умолчанию — 50 пакетов.
- **DefaultTTL.** TTL (время жизни) пакета определяет, сколько секунд он может существовать. При превышении этого времени пакет уничтожается. Каждый маршрутизатор, через который проходит пакет, уменьшает его время жизни не менее чем на одну секунду, в зависимости от настроек маршрутизатора. Значение времени жизни пакета по умолчанию — 120 секунд. В сети с медленными каналами связи значение этого параметра может быть увеличено, чтобы обеспечить уверенность в том, что взаимодействие между удаленными компьютерами произойдет.

Советы по оптимизации сети

TCP/IP — очень динамичный протокол, и он обычно в состоянии сам себя настроить для достижения оптимальной производительно-

сти. Однако Performance Monitor, входящий в состав Windows NT, может помочь вам принять решение о необходимости оптимизации. Performance Monitor автоматически устанавливается при установке Windows NT; он позволяет вычислять статистику, связанную с серверными и сетевыми событиями. Также эта программа позволяет выводить в реальном времени графики и генерировать отчеты. Вы можете запустить Performance Monitor из подменю Administrative Tools (Common) меню Start.

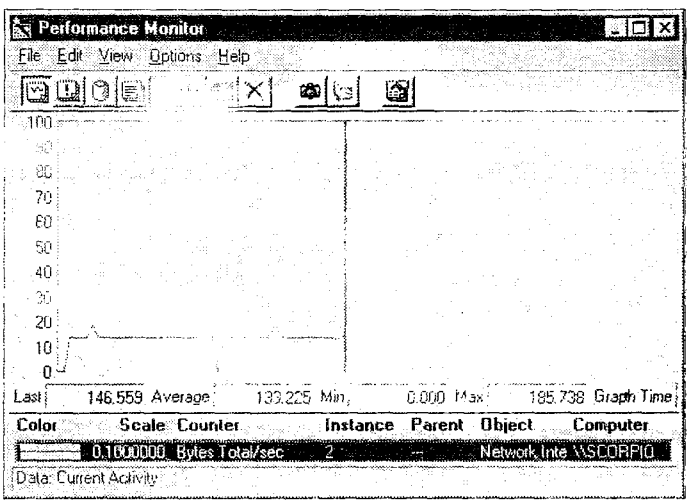


Рис. 15.7. Performance Monitor может использоваться для отслеживания сетевых событий

Performance Monitor (рис. 17.7) также позволяет отслеживать некоторые сетевые события, в том числе общее количество байтов, передаваемое каждую секунду, количество неудачных попыток установления TCP-соединения, количество полученных IP-датаграмм и ICMP-сообщений в секунду. Для того чтобы следить за определенным показателем, выберите команду Add To Chart в меню Edit. Появится окно, показанное на рис. 15.8, которое позволяет вам выбрать объект и параметр. Объекты объединяют параметры в логические группы. Например, выбрав объект IP, вы можете выбрать наблюдение за количеством полученных датаграмм (Datagram Received), количеством пропавших датаграмм (Datagram Discarded), количеством ретранслированных датаграмм в секунду (Datagrams Forwarded/sec) и многими другими параметрами. Для того чтобы получить дополнительную информацию об определенном параметре, нажмите кнопку Explain.

Имейте в виду, что, хотя Performance Monitor — великолепный инструмент для поиска неисправностей, он нагружает систему. Поэтому

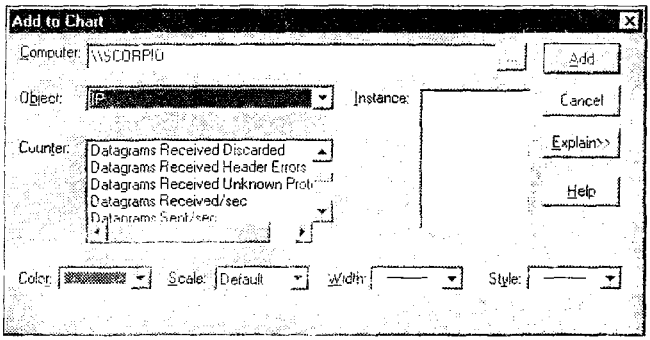


Рис. 15.8. При помощи Performance Monitor можно отслеживать значения разнообразных параметров

не следует запускать его на сервере — производите запуск на другом NT-компьютере сети.

Network Monitor (рис. 15.9) является даже более продвинутой утилитой, которая может использоваться для наблюдения за взаимодействиями в сети, общей загрузкой сети и для захвата данных. Эта утилита не устанавливается по умолчанию, но вы можете добавить ее в качестве службы на вкладке Services окна Network. Опять же, эта очень мощная программа нагружает систему, на которой работает. Вы должны избегать ее запуска на сервере.

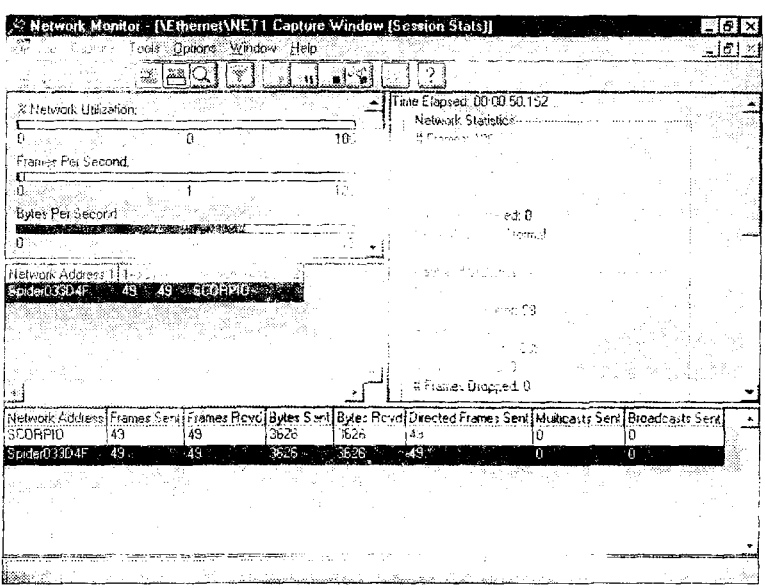


Рис. 15.9. Network Monitor предоставляет возможность наблюдения за сетью

После того как вы определите, какие изменения должны быть сделаны для улучшения работы TCP/IP, мы предлагаем вам придерживаться следующих принципов:

- Делайте изменения последовательно, по одному за раз. Если вы не замечаете изменения производительности, переходите к следующему изменению.
- Тщательно документируйте все сделанные изменения. Проблема может не проявляться дни или даже недели после того, как были сделаны изменения, но потом может оказаться, что все необходимо вернуть в исходное состояние.
- Когда возможно, тестируйте все изменения на компьютере, отказ которого не будет трагедией. Если вы планируете изменить настройки TCP/IP на сервере, вы всегда должны проверить их сначала на другом компьютере.

Управление трафиком NetBIOS

Учитывая природу NetBIOS, управление прохождением трафика NetBIOS по сети часто — сложная задача. Поскольку NetBIOS использует широковещательные сообщения и поиск имен, трафик NetBIOS может быть весьма значительным и «заморозить» и компьютеры, и всю сеть. NetBIOS поверх TCP/IP (NetBIOS Over TCP/IP, NBT) позволяет использовать дополнительный уровень аутентификации: контекст NetBIOS. Идентификатор контекста присоединяется к имени NetBIOS компьютера при сетевых взаимодействиях. Только компьютеры, имеющие один и тот же идентификатор контекста, могут взаимодействовать друг с другом. Хотя это и не снижает трафик в сети, но производится некоторая фильтрация и — до некоторой степени — улучшение безопасности сети.

Не рекомендуется использовать контекст NetBIOS в сети. Однако он может использоваться при тестировании. Контекст NetBIOS полезен в рабочих группах, в ситуациях, когда нет необходимости (или даже нежелательно взаимодействие между компьютерами двух рабочих групп, хотя они должны разделять общую сетевую среду). На рис. 15.10 показан пример ситуации, в которой может быть использован контекст NetBIOS.

Идентификатор контекста присваивается компьютеру на вкладке WINS окна свойств TCP/IP, как показано на рис. 15.11. Идентификатор контекста может содержать цифры или буквы, но полное имя NetBIOS (имя компьютера плюс идентификатор контекста) не может превышать 256 символов.

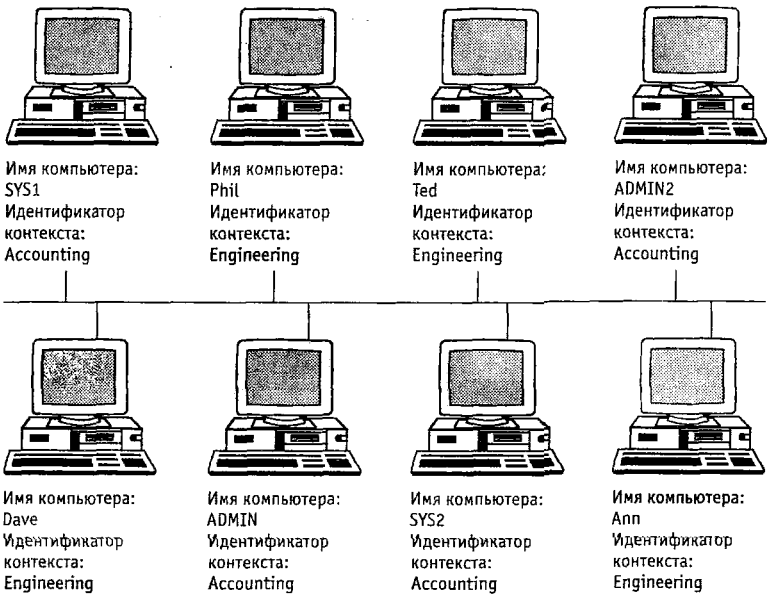


Рис. 15.10. Контекст NetBIOS может использоваться для ограничения взаимодействия между компьютерами

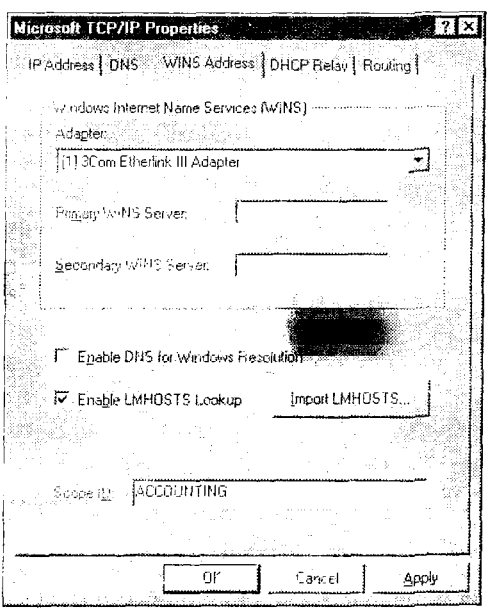


Рис. 15.11. Идентификатор контекста указывается на вкладке WINS окна Microsoft TCP/IP Properties

Вопросы для подготовки к экзамену

Question 1

After monitoring your network for a week, you have concluded that your Windows NT Server, which is acting as a router, is dropping packets. Which of the following Registry settings can be used to correct this problem? (Check all correct answers.)

- ❑ A. TcpWindowSize
- ❑ B. ForwardBufferMemory
- ❑ C. NumForwardPackets
- ❑ D. DefaultTTL

Вопрос 1

После наблюдения за сетью в течение недели вы обнаружили, что ваш Windows NT Server, работающий как маршрутизатор, теряет пакеты. Какой из следующих параметров реестра может быть использован для решения этой проблемы? (Укажите все правильные ответы.)

- ❑ A. TcpWindowSize
- ❑ B. ForwardBufferMemory
- ❑ C. NumForwardPackets
- ❑ D. DefaultTTL

Правильные ответы на этот вопрос — B и C. Каждый из этих параметров определяет, как маршрутизируемые пакеты сохраняются в памяти. ForwardBufferMemory определяет, как много данных может быть сохранено, а NumForwardPackets — сколько пакетов может быть помещено в очередь. TcpWindowSize определяет количество данных, которое должно быть получено из сети до отправки подтверждения. Следовательно, ответ A неверен. Параметр DefaultTTL определяет время жизни пакета. Следовательно, ответ D неверен.

Question 2

What type of communications does FTP use?

- ○ A. Synchronous
- ○ B. Asynchronous
- ○ C. Multisynchronous
- ○ D. Unisynchronous

Вопрос 2

Какой тип взаимодействия использует FTP?

- O A. Синхронный
- O B. Асинхронный
- O C. Мультисинхронный
- O D. Унисинхронный

Правильный ответ на этот вопрос — A, синхронный. Запомните, что при синхронном взаимодействии отправляются пакеты данных, а при асинхронном данные передаются по одному символу за один раз. Ответы C и D — подделка; таких типов взаимодействия не существует.

Question 3

Which of the following utilities is used to monitor the network? (Check all correct answers.)

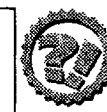
- ❑ A. Performance Monitor.
- ❑ B. Ethernet Monitor.
- ❑ C. WINS Monitor.
- ❑ D. Network Monitor.

Вопрос 3

Какие из следующих утилит могут использоваться для наблюдения за сетью? (Укажите все правильные ответы.)

- ❑ A. Performance Monitor.
- ❑ B. Ethernet Monitor.
- ❑ C. WINS Monitor.
- ❑ D. Network Monitor.

Ответы A и D — правильные. Как Performance Monitor, так и Network Monitor могут использоваться для отслеживания сетевых событий. Утилиты, указанные в ответах B и C, хотя и выглядят подходящими, не существуют.



Question 4

What kind of data types are the Registry values that pertain to TCP/IP tuning? (Check all correct answers.)

- ❑ A. DWORD
- ❑ B. STRING
- ❑ C. REG_DWORD
- ❑ D. REG_MULTI_SZ

Вопрос 4

Какой тип данных имеют параметры реестра, используемые для настройки TCP/IP? (Укажите все правильные ответы.)

- ❑ A. DWORD
- ❑ B. STRING
- ❑ C. REG_DWORD
- ❑ D. REG_MULTI_SZ

Правильные ответы на этот вопрос — A и C. Это сложный вопрос, ибо, хотя типом значений и является двойное слово, название типа зависит от того, какую утилиту вы используете. При использовании regedt32 тип называется REG_DWORD, а при использовании Regedit — DWORD. Ответы B и D не имеют отношения к параметрам, обсуждавшимся в этой главе.

Question 5

Which of the following protocols uses Scope ID to limit communications?

- ○ A. NWLink
- ○ B. NetBEUI
- ○ C. NBT
- ○ D. TCP

Вопрос 5

Какой из следующих протоколов использует идентификатор контекста при взаимодействиях?

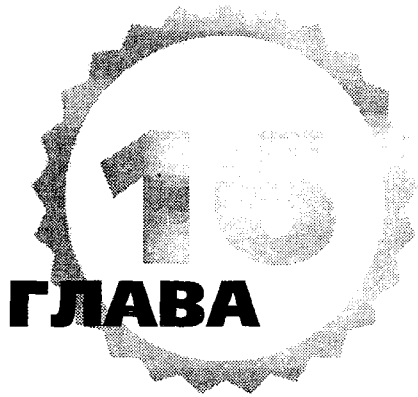
- ○ A. NWLink
- ○ B. NetBEUI
- ○ C. NBT
- ○ D. TCP

Правильный ответ на этот вопрос — C. NBT (NetBIOS поверх TCP/IP) поддерживает эту возможность.

Дополнительная информация

Microsoft TechNet, September, 97, PN99367. Документ «MS Windows NT 3.5, 3.51, 4.0 — TCP/IP Implementation Details» содержит исчерпывающую информацию по обсуждаемой теме. Вы также можете провести поиск в TechNet (на компакт-диске или в сети по адресу www.microsoft.com), используя ключевые слова «TcpWindowSize» и «NumForwardPackets».

The Windows NT Server Resource Kit содержит массу полезной информации по TCP/IP и родственным темам. Вы можете произвести поиск любой из обсуждавшихся тем.



Поиск и устранение неисправностей

Термины, необходимые для понимания материала:

- ARP
- HOSTNAME
- IPCONFIG
- NSLOOKUP
- NBTSTAT
- NETSTAT
- PING
- ROUTE
- TRACERT

Приемы и знания, которыми вы должны овладеть:

- Использование соответствующих случаю методов для поиска и устранения проблем с TCP/IP
- Использование различных ключей каждой диагностической команды для определения точного местонахождения проблемы
- Поиск и устранение неисправностей «снизу вверх»
- Поиск неисправностей при помощи утилит Performance Monitor и Network Monitor
- Поиск и устранение коммуникационных проблем
- Поиск и устранение проблем при определении имен

Мощь TCP/IP вызывает сложность, которая может «вызвать головную боль», когда что-то работает неправильно. В этой главе мы предлагаем вам обзор методологии поиска неисправностей и некоторых специальных диагностических TCP/IP-утилит. Вы не только найдете этот обзор полезным при подготовке к экзамену, но и обнаружите, что описываемые утилиты необходимы в реальной жизни. Затем мы обсудим различные задачи при поиске и устранении проблем в TCP/IP и разнообразные инструменты, которые помогут вам. Также мы кратко опишем использование Performance Monitor и Network Monitor для анализа сетевых проблем. И наконец, мы исследуем некоторые типичные проблемы TCP/IP-сетей и их решения.

Утилиты для поиска проблем в TCP/IP

В табл. 16.1 приведен обзор диагностических инструментов и утилит, которые поставляются вместе с Microsoft TCP/IP. Как вы можете видеть уже из длины этого списка, поиск неполадок может быть непростым занятием.

Таблица 16.1. Диагностические утилиты TCP/IP (в алфавитном порядке)

Утилита	Описание
ARP	Позволяет просматривать и изменять таблицы трансляции аппаратных адресов, используемые протоколом ARP. Может быть использована на локальном компьютере для поиска записей с неверными адресами
HOSTNAME	Выводит на экран имя локального узла
IPCONFIG	Выводит все значения параметров настройки сети. Особенно полезна на компьютерах, использующих DHCP
NBTSTAT	Выводит статистику протокола и список текущих TCP/IP-соединений, используемых NetBT. Очень полезная утилита
NETSTAT	Аналогична NBTSTAT. Выводит только TCP/IP-статистику и список TCP/IP-соединений
NSLOOKUP	Выводит информацию о серверах DNS. Доступно, только если была произведена установка TCP/IP
PING	Наиболее полезная утилита. Проверяет возможность простейшего сетевого взаимодействия с одним или несколькими удаленными компьютерами
ROUTE	Управляет таблицами маршрутизации
TRACERT	Определяет путь к указанному узлу, отправляя ICMP эхо-запросы и увеличивая значение параметра TTL (время жизни)

Помимо утилит, перечисленных в табл. 16.1, не забудьте о следующем:

- **Служба Microsoft SNMP.** Предоставляет статистическую информацию управляющим консолям SNMP. (См. главу 14, «Реализация службы SNMP».)
- **Event Viewer.** Отслеживает ошибки и события.
- **Performance Monitor.** Анализирует производительность сервера.
- **Network Monitor.** Анализирует сетевые протоколы на низком уровне.
- **Registry Editor.** Позволяет просматривать и изменять значения параметров реестра.

Советы по поиску неисправностей в TCP/IP

Как и при использовании любой методологии поиска неисправностей, постройте работу на научной основе. Запомните: процесс поиска неисправностей обычно приходится повторять — вы можете не достигнуть успеха с первого раза. В случае TCP/IP общим методом поиска неисправностей может быть такой:

1. Определите проблему, или, по крайней мере, симптомы, в которых она себя проявляет. Это бывает самым трудным шагом. Хотя проблема может на первый взгляд казаться вызванной каким-то одним элементом, процесс исключения и некоторая как бы детективная работа могут указать на что-либо совершенно другое.
2. Исключите то, что работает правильно, чтобы сузить «круг подозреваемых».
3. Исследуйте сначала физический уровень, а затем каждый уровень над ним; 90 процентов сбоев в сетях вызваны плохим креплением кабеля.
4. Выдвиньте гипотезу.
5. Проверьте вашу гипотезу.
6. Проанализируйте данные.
7. Предпримите действия, нужные для устранения проблемы.

Составьте список, в котором укажите, что работает и что — нет, затем изучите список, чтобы изолировать сбои и отказы. Не забудьте использовать Event Viewer для определения результатов любых изменений. Вообще говоря, лучше с самого начала проверить, правильно ли настроен TCP/IP на компьютере. Затем проверьте, что между компьютером и сетевым узлом существует соединение и путь, начав с проверки локального оборудования. Попробуйте множество раз использовать команду PING с различным количеством пакетов в слу-

3. Затем проверьте связь со шлюзом по умолчанию. Это позволит проверить, работает ли шлюз, а также доступен ли он локальному узлу: PING <IP-адрес шлюза по умолчанию>.
4. Отправьте эхо-запрос на IP-адрес удаленного узла для проверки работы маршрутизатора: PING <IP-адрес удаленного узла>.

Внимание

Шлюз по умолчанию должен находиться в той же логической подсети, что и IP-адрес локального узла. Если шлюз по умолчанию не находится в той же подсети, узел сможет взаимодействовать только с узлами, находящимися в одной с ним подсети.

На рис. 16.2 приведен результат выполнения команды PING без параметров, позволяющий вам представить, чего же следует ожидать.

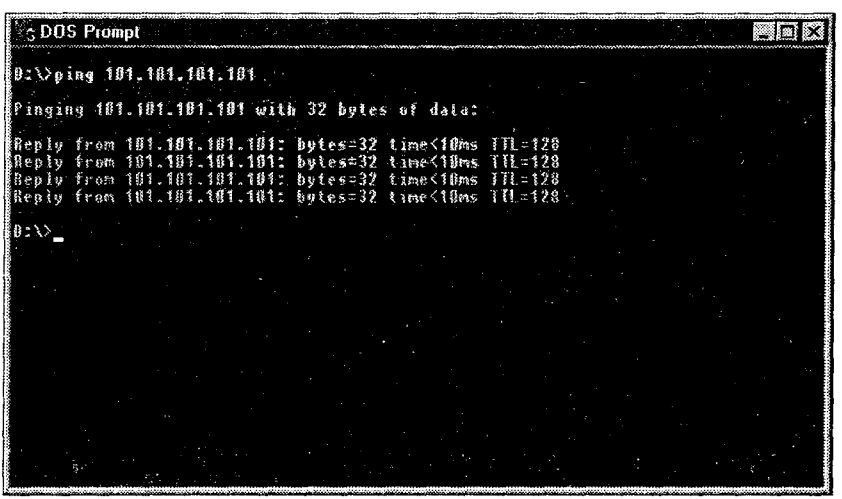


Рис. 16.2. Использование утилиты PING для проверки IP-связи

Заметьте, что ключи команды PING могут помочь подстроиться под практически любую ситуацию. Например, по умолчанию PING ожидает каждого ответа только 750 миллисекунд, после чего ответ считается неполученным. Ключ -w может использоваться для установки более продолжительного тайм-аута. Это может оказаться полезным в тех ситуациях, когда удаленная система связана с локальным каналом связи с большой задержкой, например спутниковым, в котором ответ может прийти через более продолжительное время. В табл. 16.3 приведен список ключей PING и их краткое описание.

Таблица 16.3. Ключи команды PING

Ключ	Описание
-t	Отправка запросов до прерывания работы
-a	Преобразование адресов в имена узлов
-n (число)	Отправка указанного числа запросов; по умолчанию отправляется 4 запроса
-l (длина)	Отправка эхо-запросов указанной длины. Значение по умолчанию — 64 байта; максимально допустимое значение — 8192.
-t время	Установка значения TTL для отправляемых пакетов
-v TOS	Установка указанного значения типа обслуживания (Type of Service)
-r (число)	Запись пути в соответствующее поле. Может быть указано от одного до девяти узлов
-s (число)	Установка штампа времени в указанное число хопов
-j (список узлов)	Маршрутизация пакетов через указанные узлы. Максимально допустимое IP число узлов — 9. Последовательные узлы могут быть разделены шлюзами (loose source routed)
-k (список узлов)	Маршрутизация пакетов через указанные узлы. Максимально допустимое IP число узлов — 9. Последовательные узлы *не могут* быть разделены шлюзами (strict source routed)
-w (тайм-аут)	Установка тайм-аута в миллисекундах
Узел	Отправка эхо-запроса на указанный узел

Диагностические утилиты и методы

Теперь, когда вы почувствовали, насколько мощны и эффективны основные утилиты для поиска неисправностей, давайте рассмотрим прочие диагностические утилиты, входящие в состав Microsoft-реализации TCP/IP. Если вы проверили, что все кабели подключены правильно и повели исходное тестирование при помощи PING и IPCONFIG для проверки связи и настройки, ваша проблема может заключаться в IP-адресе или имени узла. Для того чтобы определить проблемы с IP-адресацией, вы можете использовать утилиты ARP, ROUTE и TRACERT.

ARP

ARP — это еще одна очень полезная утилита, позволяющая вам просматривать и изменять таблицу ARP на локальном узле, а также просматривать кэш ARP и находить любые проблемы в определении адресов. Как вы знаете, в Windows NT реализации TCP/IP сетевые устройства при взаимодействии используют IP-адрес, имя узла в форме FQDN или имя NetBIOS. Вне зависимости от того, какое согла-

шение об именовании используется, имя должно однозначно определяться в MAC-адрес — аппаратный адрес. Протокол определения адресов (ARP, Address Resolution Protocol) позволяет найти аппаратный адрес нужного узла. Для повышения эффективности на каждом узле или маршрутизаторе на некоторое время кэшируются уже определенные соответствия между IP-адресом и аппаратным адресом; утилита ARP опрашивает этот кэш. Наличие такого кэша позволяет снизить количество повторных широковещательных запросов. Однако имейте в виду, что по умолчанию кэш обновляется с 10-минутным интервалом для обеспечения правильности определения адресов.

Ключи утилиты ARP достаточно полезны. Например, если вы хотите произвести поиск записи, относящейся к определенному узлу, используйте ключ -a. Синтаксис команды таков:

```
arp -a IP-адрес -N IP-адрес_интерфейса
```

Если IP-адрес указан в десятичной записи, выводятся только IP-адрес и аппаратный адрес данного узла. Ключ -N позволяет указать нужный сетевой интерфейс, задав его IP-адрес. Если адрес интерфейса не указан, будет использоваться первый найденный интерфейс.

Кроме того, вы можете использовать следующие формы этой команды:

- arp -d IP-адрес [IP-адрес_интерфейса] — Эта команда удаляет запись, соответствующую заданному IP-адресу.
- arp -s IP-адрес Ethernet-address [IP-адрес_интерфейса] — Эта команда создает запись в кэше ARP, устанавливая соответствие между заданными Ethernet- и IP-адресами. Аппаратный Ethernet-адрес задается в виде шести байтов в шестнадцатеричном формате, разделенных дефисами. IP-адрес задается в стандартном десятичном формате. Создаваемая запись становится статической и не удаляется из кэша со временем, однако она будет потеряна после перезагрузки компьютера.

NSLOOKUP

NSLOOKUP — очень мощная утилита, позволяющая выводить информацию, полученную от серверов DNS. Естественно, NSLOOKUP доступна, только если была проведена установка TCP/IP и доступен сервер DNS. Эта команда имеет следующий синтаксис:

```
nslookup [-параметр] [имя_узла | - [сервер] ]
```

NSLOOKUP имеет два режима: интерактивный и неинтерактивный, которые используются в зависимости от того, как много данных вам нуж-

но получить. Для того чтобы получить конкретную запись с сервера DNS, используйте неинтерактивный режим, указав IP-адрес или имя узла, которое должно быть определено, в качестве первого аргумента. В качестве второго аргумента укажите IP-адрес или имя сервера DNS. Если второй аргумент опущен, будет использоваться сервер DNS по умолчанию.

В интерактивном режиме вы можете производить последовательный поиск информации. В этом случае используйте в качестве первого аргумента дефис (-), а второй аргумент либо не указывайте (чтобы использовать сервер DNS по умолчанию), либо введите имя или IP-адрес, чтобы использовать определенный сервер. Для того чтобы завершить работу в интерактивном режиме, нажмите Ctrl+C. Запомните, что в интерактивном режиме неизвестные команды будут трактоваться как имена узлов. Для того чтобы NSLOOKUP восприняла встроенную команду как имя узла, введите перед ней символ \. С утилитой NSLOOKUP может быть использовано более 25 параметров, но общая длина командной строки не должна превышать 256 символов. Вам, скорее всего, не потребуется на экзамене знать назначение этих параметров, однако, если вы хотите узнать больше, обратитесь к встроенной справке Windows NT или к приложению А документа «Networking Guide», содержащегося в Microsoft *Windows NT Server Resource Kit.*

Проблемы с маршрутизацией

В Windows NT появился MPR — многопротокольный маршрутизатор (MultiProtocol Router). Он может использоваться для поддержки маршрутизации на компьютерах с одним или несколькими сетевыми интерфейсами. MPR использует протокол управления маршрутизацией (RIP, Routing Information Protocol) для TCP/IP и IPX. Мы описывали маршрутизацию и ее работу в Microsoft-сетях в главе 6, «Реализация IP-маршрутизации». Давайте рассмотрим две утилиты, позволяющие производить поиск проблем с маршрутизацией — ROUTE и TRACERT.

ROUTE

ROUTE — диагностическая утилита, которая позволяет манипулировать сетевыми таблицами маршрутизации. Она использует файл Networks для преобразования имен узлов назначения в адреса. Для того чтобы утилита ROUTE работала правильно, необходимо, чтобы сетевые номера были указаны в этом файле корректно; то есть все четыре октета были бы записаны в десятичном формате. Например, сетевой номер 10.10.1 должен быть указан в файле Networks как 10.10.1.0; дополнительные нули присоединяются, чтобы образовать нужное количество октетов.

Чтобы определить, вызвана ли проблема ошибками в IP-адресации, проверьте путь, выбираемый для отправки пакетов. Проблема может возникать из-за неправильной таблицы маршрутизации или отказа маршрутизатора. Если вы получаете ответ на команду PING от локального узла, но не получаете ответа от маршрутизатора, это свидетельствует о проблемах с маршрутизатором. Если вы не получаете ответ на PING от узлов за маршрутизатором, проблема может состоять в таблицах маршрутизации. Команда ROUTE print позволяет выводить таблицы маршрутизации на экран. Другие ключи команды ROUTE — add, delete и change — позволяют соответственно добавлять, удалять и изменять записи в таблице маршрутизации.

TRACERT

Чтобы проверить маршрутизаторы в пути, используйте утилиту TRACERT. Если узел назначения не может быть достигнут, то вы увидите, какой маршрутизатор не работает; если сеть работает медленно, TRACERT покажет вам, сколько времени затрачивается на передачу пакетов от одного маршрутизатора другому. В следующем примере шлюз по умолчанию определил, что к узлу 10.10.0.1 не имеется пути. Это означает, что либо маршрутизатор настроен неверно, либо сеть 10.10.0.0 не существует (или задан неверный IP-адрес).

```
C:>\tracert 10.10.0.1
Tracing route to 10.10.0.1 over a maximum of 30 hops
192.54.48.1 reports: Destination net unreachable.
Trace complete.
```

Поиск проблем при помощи наблюдения

Windows NT Server и Windows NT Workstation включают в себя утилиту Performance Monitor, которая может использоваться для наблюдения за многими параметрами TCP/IP. После установки службы SNMP вы можете наблюдать за работой сетевого интерфейса, IP, ICMP, UDP, TCP и NetBT. Одним из преимуществ Performance Monitor является то, что вы можете наблюдать сразу за несколькими показателями в одном окне. Вы можете установить уровни для всех показателей, при достижении которых будет выводиться предупреждение.

В состав Windows NT Server также входит Network Monitor — утилита, упрощающая поиск сложных сетевых проблем. Компьютеры, на которых запущена эта утилита, могут подключаться к узлам, на которых работает агентское программное обеспечение, при помощи локальной сети или коммутируемого подключения. Это может оказаться полезным для наблюдения за удаленной системой.

Network Monitor позволяет захватывать входящий и исходящий трафики локального компьютера. Чтобы выделить необходимую для последующего анализа информацию, можно определять фильтры. Фильтры могут основываться на аппаратном адресе отправителя либо получателя пакета, на адресе, используемом протоколом, а также на совпадении с образцом. Фильтры для вывода позволяют изолировать потенциальные проблемы и уменьшить объем информации, которая должна быть проанализирована. Выводимый на экран отчет состоит из окна, содержащего краткую информацию, окна с подробным описанием информации и шестнадцатеричного вывода. информация

Обычные проблемы с TCP/IP и их решения

На протяжении этой книги мы исследовали различные аспекты TCP/IP, такие как связь, определение имен, маршрутизация, определение адресов и отказоустойчивая настройка. Мы также рассмотрели множество утилит, позволяющих определить проблемы при их возникновении. Прежде чем мы применим все эти знания на практике, давайте рассмотрим несколько примеров обычных TCP/IP-проблем и их решений.

Если вы не получаете ответа на команду PING и не можете другим образом соединиться с удаленным узлом при использовании локальной сети в качестве клиента удаленного доступа, вы, возможно, не установили флажок Use Default Gateway On Remote Network при настройках TCP/IP в адресной книге службы удаленного доступа. Эта возможность добавляет в таблицу маршрутизации новую запись. Эта запись позволяет отправлять пакеты, для которых IP-адрес узла назначения невозможно определить при помощи других записей в таблице маршрутизации, — на шлюз с другой стороны канала, используемого службой удаленного доступа. Эта возможность должна быть разрешена для использования утилит Интернета, таких как Web-броузер или FTP.

Используйте команду ROUTE add для создания пути к подсети, которую вы пытаетесь использовать, и связывания этого пути с локальным шлюзом. Например, если компьютер, с которым вы соединяетесь, имеет IP-адрес 11.1.0.3, используйте для создания пути в таблице следующую команду:

```
route add 11.0.0.0 MASK 255.0.0.0 199.199.41.1
```

Это позволит отправлять все пакеты, предназначенные для сети 11.x.x.x, на шлюз (199.199.41.1) в локальной сети.

Используйте команду NBTSTAT -n для определения причины проблем, которые возникают при установлении связи с сервером, имеющим

определенное имя. Эта команда позволит вам узнать, какое имя сервер зарегистрировал в сети. Команда NBTSTAT также полезна, когда необходимо вывести на экран значения для удаленных компьютеров из кэша имен — записей из файла LMHOSTS, помеченных тегом #PRE, либо записей для недавно определенных имен.

Если при соединении с удаленным компьютером IP-адреса работают, но имена узлов — нет, убедитесь, что файл HOSTS и DNS настроены правильно. Для этого проверьте настройки определения имен, выбрав в окне Network вкладку DNS. Убедитесь, что IP-адреса серверов DNS указаны верно и в нужном порядке. Используйте NSLOOKUP, чтобы убедиться, что сервер DNS работает правильно. Отправьте эхо-запрос на удаленный компьютер при помощи команды PING, использовав как IP-адрес, так и имя узла, чтобы убедиться, что имя узла определяется правильно. Если вы используете для определения имен файл HOSTS, проверьте его дважды — нет ли в нем каких-нибудь опечаток.

Если ваше TCP/IP-соединение с удаленным компьютером выглядит зависшим, используйте команду NETSTAT -a для вывода статуса всех активных TCP- и UDP-портов на локальной машине. Если кажется, что с соединением все в порядке, то, скорее всего, размер очереди для отправки и приема установлен в 0 байт. Если данные заблокированы в очереди или состояние соединения отличается от обычного, то, вероятно, существует проблема со связью; в противном случае проблема, скорее всего, связана с сетью или с приложениями.

Получение технической поддержки от Microsoft

Следующий список доступных материалов может оказаться полезным, если у вас больше не осталось никаких идей.

- **Microsoft Frequently Asked Questions (FAQ).** Ответы на основные технические вопросы.
- **Microsoft Software Library.** Содержит бесплатные добавления, исправления ошибок, драйверы периферийных устройств, обновления и вспомогательные программы.
- **Microsoft Knowledge Base.** База данных, поддерживаемая инженерами Microsoft и предназначенная для поиска ответов на технические вопросы. Она является исчерпывающей коллекцией из более чем 70 000 подробных статей с технической информацией о продуктах Microsoft, списков ошибок и их исправлений и ответов на часто задаваемые технические вопросы.

- **Интернет-службы (WWW- и FTP- узлы).** Web-узел Microsoft расположен по адресу www.microsoft.com; FTP-узел расположен по адресу ftp.microsoft.com.
- **Microsoft Network (MSN) и прочие доступные в Сети службы.** Для того, чтобы получить доступ к службам поддержки Microsoft в MSN, выберите Go To Other Location в меню Edit и введите MSsupport.
- **Microsoft TechNet.** Основной ресурс для быстрого поиска подробных ответов на технические вопросы о продуктах Microsoft. Подписка на TechNet стоит $299 в год (лицензия на одного пользователя) или $699 в год (лицензия на один сервер, неограниченное количество пользователей). Для того чтобы подписаться на TechNet, позвоните по телефону 1-800-344-2121.
- **Microsoft Developer Network Library (MSDN).** Для того чтобы подписаться на MSDN, позвоните по телефону 1-800-759-5474. Даже если вы не являетесь разработчиком, это великолепный Web-узел. В настоящий момент он доступен любому Microsoft Certified Professional через Web-узел Microsoft.
- **Microsoft Download Service (MSDL).** MSDL содержит примеры программ, драйверов устройств, исправлений, обновлений и вспомогательных программ. Прямой модемный доступ к MSDL возможен по номеру 1-206-936-6375. Эта служба доступна 24 часа в сутки, 365 дней в году. Информация о соединении: 1200, 2400, 9600 или 14400 бод; без проверки четности, 8 бит данных, 1 стоп-бит.
- **Microsoft FastTips.** Microsoft FastTips — автоматическая служба, позволяющая быстро получить ответ на общие технические вопросы при помощи автоматического бесплатного телефонного номера, по телефаксу или по почте. Для того чтобы получить доступ к FastTips или получить карту и каталог, позвоните по номеру, соответствующему вашим интересам. А именно — Приложения для десктоп-систем: 1-800-936-4100; Продукты для разработчика: 1-800-936-4300; Продукты для персональных систем: 1-800-936-4200; Бизнес-системы: 1-800-936-4400.
- **Электронная служба запросов при необходимости.** Эта служба доступна Premier, Priority Comprehencive 35 и 75 и Priority Developer 35 покупателям. Вы можете непосредственно отправить запрос инженерам Microsoft, которые получат его и помогут решить вашу проблему. Эта возможность также позволяет получить доступ к информации, необходимой для независимой поддержки и устранения неисправностей в ваших Microsoft-продуктах. Обратитесь за более подробной информацией к вашему Microsoft Solution Provider.

- **Стандартная поддержка.** На первые 30 дней после регистрации продукта вы получаете доступ к неограниченной бесплатной поддержке инженеров Microsoft по темам установки, использования и устранения сообщений об ошибках при помощи телефонного звонка в интервале между 6:00 и 18:00 по Тихоокеанскому времени, с понедельника по пятницу, кроме праздничных дней. Когда вы совершаете звонок, вы должны иметь под рукой компьютер и документацию на соответствующий программный продукт. Будьте готовы сообщить:
  - Номер версии используемого вами продукта Microsoft.
  - Тип используемого аппаратного обеспечения, в том числе сетевого аппаратного обеспечения, если оно имеется.
  - Точный текст сообщения об ошибке, появляющегося на вашем экране.
  - Описание того, что случилось, и того, чем вы занимались в этот момент.
  - Описание того, как вы пытались решить проблему.
- **Срочная поддержка.** Служба технической поддержки Microsoft гарантирует срочную техническую поддержку инженеров Microsoft 24 часа в сутки, 7 дней в неделю, за исключением праздников, в США. В США звоните по номеру 1-900-555-2020; стоимость услуги $55 за вопрос. Плата появится в вашем телефонном счете.
- **Телетайп.** Microsoft телетайп-службы (TT/TDD) доступны для глухих или плохо слышащих. В США вы можете, используя телетайп-модем, звонить по номеру 1-206-635-4948. В Канаде используйте номер 1-905-568-9641.

Вопросы для подготовки к экзамену

Question 1

You have just received a new Windows NT Workstation. You're able to connect to other IP machines on your local subnetwork using the UNC name of the targeted resource, but you seem to be having trouble mapping a drive to another Windows NT host that resides on a remote network. However, no one else is having problems connecting to the remote Windows NT host. What is the first thing you should check?

- ○ A. Cabling.
- ○ B. IP address of the remote host.
- ○ C. IP address of the local host.
- ○ D. IP address of the default gateway.

Вопрос 1

Вы только что установили новую Windows NT Workstation. Вы можете соединяться с другими IP-узлами в вашей сети, используя UNC-имя требуемого ресурса, но вы не в состоянии использовать разделяемый диск другого NT-узла, находящегося в удаленной подсети. Что вы проверите с самого начала?

- A. Кабели.
- B. IP-адрес удаленного узла.
- C. IP-адрес локального узла.
- D. IP-адрес шлюза по умолчанию.

Правильный ответ — D. Запомните, что шлюз по умолчанию должен находиться в той же логической подсети, что и локальный узел, и его IP-адрес должен быть правильно указан при настройке локального узла. Если проблема была бы связана с плохим подключением кабелей, вы не смогли бы взаимодействовать с узлами локальной сети. Следовательно, ответ A неверен. Аналогичная ситуация возникла бы, если бы адрес локального узла был бы установлен неверно. Следовательно, ответ C неверен. Если бы IP-адрес удаленного узла был установлен неверно, никто не смог бы использовать разделяемый диск на нем. Следовательно, ответ B неверен.

Question 2

You've added an entry to your LMHOSTS file and are now experiencing long connect times. What could be causing the delay?

- A. The delay is normal and will clear up the next time you reboot.
- B. There's a problem with the DNS.
- C. There's a problem with the LMHOSTS file.
- D. This indicates a cabling problem.

Вопрос 2

Вы добавили запись в файл LMHOSTS, и теперь установление соединения происходит очень медленно. Что может быть причиной этого?

- A. Так и должно быть; задержка исчезнет после перезагрузки.
- B. Проблема с сервером DNS.
- C. Проблема с файлом LMHOSTS.
- D. Проблема с кабелем.

Правильный ответ — C. Задержка при установлении соединения может быть вызвана тем, что соответствующая запись находится в кон-

це большого файла LMHOSTS. Пометьте эту запись как предзагружаемую при помощи тега #PRE в конце строки. Затем используйте команду NBTSTAT -R для немедленного обновления кэша имен. Или же вы можете поместить соответствующую запись ближе к началу файла LMHOSTS. Часто используемые записи должны находиться в начале файла, а редко используемые — в конце. Ответ A просто неверен. Ответ B неверен, поскольку проблемы с DNS вызвали бы не замедление соединения, а его отсутствие. Ответ D включен, чтобы запутать вас. Задержка при ответе может быть вызвана плохим подключением кабеля, но это не самая вероятная причина для возникновения описанной ситуации.

Question 3

Mary has just taken over the desktop support for a different department of her company. She is setting up a new laptop on the local subnet for the CEO. During setup, she gets the following error message: «Your default gateway does not belong to one of the configured interfaces». What should Mary do?

- A. Check the cabling.
- B. Check the PCMCIA card and reinsert it.
- C. Run IPCONFIG.
- D. Check the spelling of the default gateway entry in the LMHOSTS file.

Вопрос 3

Мария устанавливает переносной компьютер для своего начальника. При установке она получает следующее сообщение об ошибке: «Ваш шлюз по умолчанию не принадлежит ни одному из настроенных интерфейсов». Что Мария должна сделать?

- A. Проверить кабель.
- B. Проверить PCMCIA-карту и переподключить ее.
- C. Запустить IPCONFIG.
- D. Проверить запись для шлюза по умолчанию в файле LMHOSTS.

Правильный ответ — C. Для того чтобы определить, находится ли настроенный шлюз по умолчанию в той же логической подсети, используйте команду IPCONFIG (WINIPCFG при работе с Windows 95). Сравните сетевую часть адреса шлюза с сетевым идентификатором сетевого PCMCIA-адаптера. Сетевые части IP-адресов должны совпадать, чтобы шлюз находился в той же подсети. Например, если IP-адрес шлюза по умолчанию 192.89.x.y, то IP-адрес сетевого адаптера также должен иметь такой вид. Если бы проблема заключалась в плохом подключении кабеля, то, вероятно, было бы выдано сообще-

ние об отсутствии сети. Следовательно, ответы A и B неверны. Файл LMHOSTS не используется при установке. Следовательно, ответ D неверен.

Question 4

You have established a Telnet session with a remote computer named «Sales», but the banner displays the name «Accnt». You check the IP address and it appears to be right. What should you check next? (Check all correct answers.)

- ❑ A. Make sure the DNS name and HOSTS tables are current and correct.
- ❑ B. Make sure two computers on the network don't have the same IP address.
- ❑ C. arp -g
- ❑ D. This is not possible.

Вопрос 4

Вы установили Telnet-сеанс с удаленным компьютером, имя которого «Sales», но при входе в систему вы обнаружили, что она представляет себя как «Accnt». Вы проверили IP-адрес, и он правилен. Что вы должны сделать дальше? (Укажите все правильные ответы.)

- ❑ A. Убедиться, что имена DNS и файлы HOSTS правильны.
- ❑ B. Убедиться, что в сети нет двух компьютеров с одним IP-адресом.
- ❑ C. arp -g
- ❑ D. Такая ситуация невозможна.

Правильные ответы на этот вопрос – A, B и C. По умолчанию ARP считает верным первый ответ, который получает. Ответ узла-самозванца может достигнуть локального компьютера раньше, чем ответ нужного узла. Если вы проверили работу DNS, и файл HOSTS, используйте команду arp -g на локальном компьютере для вывода содержимого его кэша ARP. Если вы знаете Ethernet-адрес удаленного компьютера, проверьте, что он соответствует записи в кэше. Если это не так, сотрите запись, используя команду arp -d, форсируйте создание новой записи в кэше, отправив при помощи команды PING запрос на удаленный узел, и снова проверьте кэш ARP. Если в вашей сети действительно существует самозванец, велики шансы, что рано или поздно вы обнаружите несоответствие. Используйте Network Monitor для поиска хозяина системы, вызывающей проблемы.

Question 5

Mary is having some problems with her TCP/IP network. She tries PINGing her local machine, the local gateway (router), and a remote router with success on every occasion. However, when she tries to use the NET USE command to set up a drive mapping to the Engineering server's NetBIOS name, the command fails. She tries the NET VIEW command with the NetBIOS name, and it also fails. Finally, she tries a PING to the NetBIOS name, and it succeeds. She calls the Engineering department and finds out that the computer is not hung and that she typed the NetBIOS name correctly. What else can Mary do to troubleshoot this problem? (Check all correct answers.)

- ❑ A. Check to make sure the server's service has started.
- ❑ B. Verify that a DNS is working properly and the HOSTS file is correct.
- ❑ C. Check to see whether the entry in question has been misspelled or entered incorrectly.
- ❑ D. Check to see whether there are two different machines with the same NetBIOS name with neither knowing if the other has responded, causing both machines to refuse to connection.

Вопрос 5

Мария столкнулась с проблемами в своей TCP/IP-сети. Она пыталась отправить PING-запросы на свой локальный компьютер, на локальный шлюз (маршрутизатор) и на удаленный маршрутизатор. Все эти попытки заканчивались успешно. Однако когда она попыталась использовать команду NET USE для подключения разделяемого диска на сервере с именем NetBIOS Engineering, это не удалось. Команда NET VIEW для данного имени NetBIOS также не сработала. Наконец, она попыталась использовать команду PING, указав имя NetBIOS, и ответ от удаленного узла был получен. Она позвонила в инженерный отдел и выяснила, что компьютер работает и она вводит имя NetBIOS правильно. Что еще может сделать Мария для поиска неисправности? (Укажите все правильные ответы.)

- ❑ A. Проверить, запущена ли служба сервера.
- ❑ B. Проверить, что DNS работает правильно и файл HOSTS не содержит ошибок.
- ❑ C. Проверить правильность записи в файле LMHOSTS.
- ❑ D. Проверить, нет ли в сети двух машин с одинаковыми именами NetBIOS, каждая из которых не знает, ответила ли другая, что приводит к отказу соединения с обоими компьютерами.

Правильные ответы на этот вопрос — A, B и C. Ответ A верен, поскольку сервер будет отвечать на эхо-запросы, даже если служба сервера не запущена. Однако для установления соединения требуется служба сервера. Ответ B верен потому, что такие команды, как NET USE, могут прекратить работу по тайм-ауту до того, как произойдет определение имени при помощи файла HOSTS, но PING дождется определения имени. Ответ C верен, поскольку имя NetBIOS должно

быть правильно указано как в командной строке, так и в файле LMHOSTS. Ответ D просто неверен.

Question 6

George is working the Help Desk at 11:00 p.m. when he gets a call from a frantic engineer. She needs to access a server on the 128.131.0.0 network but can't. She's on the 10.10.0.0 network and can access resources on other networks. George instructs her on PINGing the local loopback address (127.0.0.1) and both sides of her default gateway, with successful results. PINGing a station on the remote network 128.131.0.0 fails. What should George check next?

- A. The default gateway.
- B. The HOSTS file.
- C. Static routing.
- D. Her subnet mask.

Вопрос 6

Георгий работает в службе технической поддержки. В 11:00 ему позвонила взбешенная инженер. Ей требуется доступ к северу в сети 128.131.0.0, но установить соединение невозможно. Она находится в сети 10.10.0.0 и может использовать ресурсы в других сетях. Георгий предложил ей выполнить команду PING для адреса ее локального адаптера (127.0.0.1) и для обоих интерфейсов шлюза по умолчанию; во всех случаях ответ был получен. Однако команда PING 128.131.0.0 не приводит к ответу от удаленного узла. Что Георгий должен теперь проверить?

- A. Шлюз по умолчанию.
- B. Файл HOSTS.
- C. Статическую маршрутизацию.
- D. Маску подсети на компьютере инженера.

Правильный ответ — C. Получив ответы на команды PING для локального адаптера и интерфейсов шлюза, Георгий убедился, что компьютер и маршрутизатор работают. Следовательно, маска подсети и шлюз по умолчанию настроены правильно. Следовательно, ответы A и D неверны. Вероятная причина отказа — неправильная статическая маршрутизация. Команда ROUTE print — то, что должен выбрать Георгий для определения проблемы.

Question 7

John and Mary both start to work at the Big Enormous Company at the same day. Each is supplied with a laptop that is configured with NWLink and TCP/IP. Because they are both in the Engineering department, they decide they might need to share files in the future. However, when they try to do this, they discover the can communicate only with NWLink and not TCP/IP. When Mary types in «IPCONFIG», she notices that the subnet mask is 0.0.0.0. What could be the problem?

- A. They use the same NetBIOS name.
- B. They use the same default gateway.
- C. The use the same IP address.
- D. John configured his default gateway incorrectly.

Вопрос 7

Иван и Мария начали работать в один день в Ненормально Большой Компании. Каждый из них имеет переносной компьютер, на котором настроены NWLink и TCP/IP. Поскольку они оба работают в инженерном отделе, они решили, что в будущем им может понадобиться разделять файлы. Однако, когда они попытались сделать это, они обнаружили, что их компьютеры могут взаимодействовать только при помощи NWLink, но не при помощи TCP/IP. Когда Мария ввела команду IPCONFIG, она обнаружила, что маска подсети на ее компьютере — 0.0.0.0. Что может быть причиной проблемы?

- A. Их компьютеры используют одно имя NetBIOS.
- B. Их компьютеры используют один шлюз по умолчанию.
- C. Их компьютеры используют один IP-адрес.
- D. Иван неверно настроил шлюз по умолчанию.

Правильный ответ на этот вопрос — C. TCP/IP использует ARP для определения аппаратных адресов, соответствующих IP-адресам. Следовательно, если два компьютера имеют один IP-адрес, TCP/IP не будет работать. Одинаковые имена NetBIOS приведут к выводу на экран пользователя сообщения об ошибке. Следовательно, ответ A неверен. Поскольку Иван и Мария работают в одном отделе, велики шансы, что они находятся в одной подсети. Следовательно, вряд ли верен ответ D. По тем же причинам неверен ответ B: если они находятся в одной подсети, они и должны использовать один шлюз по умолчанию.

Дополнительная информация

Microsoft TechNet, September, 97, PN99367, содержит множество статей о поиске проблем. Проведите поиск по ключевым словам «NT», «TCP/IP» и «trouble».

Кроме того, вы можете использовать справку Windows NT. Проведите поиск фразы «TCP/IP Procedures Help». Также обратите внимание на список технических ресурсов Microsoft, приведенных в разделе «Получение технической поддержки от Microsoft» выше в этой главе.

Пример экзамена

В следующих разделах мы поможем вам разработать стратегию успешной сдачи теста. Вы должны научиться выбирать правильный ответ, расшифровывать двусмысленности, работать в структуре тестов Microsoft, решать, что заучивать при подготовке к тесту. Наконец, мы предоставим 58 вопросов, которые относятся к темам экзамена TCP/IP. Желаем успеха!

Вопросы, вопросы, вопросы

Вы, конечно, понимаете: экзамен, который вам предстоит сдавать, состоит из множества вопросов. Экзамен по TCP/IP содержит 58 вопросов, на которые вам отводится 90 минут. Запомните, все вопросы делятся на четыре типа:

- Вопросы, в которых требуется выбрать единственный правильный ответ.
- Вопросы, в которых требуется выбрать несколько ответов.
- Вопросы, состоящие из нескольких частей, в которых требуется выбрать единственный ответ.
- Вопросы, в которых требуется указать область на иллюстрации.

Обязательно прочитайте вопрос дважды, прежде чем отвечать на него. И еще: не забудьте посмотреть, нет ли в вопросе кнопки Exhibit, которая позволяет открыть схемы и графики, обычно используемые для того, чтобы пояснить вопрос, сообщить дополнительные данные или показать структуру обсуждаемых объектов. Не обратив внимания на эти иллюстрации, на такой вопрос ответить трудно.

Не каждый вопрос подразумевает единственный правильный ответ — во многих вопросах вы должны указать несколько ответов. Более того, встречаются вопросы, в которых вы должны пометить все предлагаемые ответы. Внимательное прочтение вопроса поможет вам понять, сколько ответов вы должны выбрать. Также обращайте внимание на инструкции в скобках, подсказывающие, как вы должны выбирать ответы (например, «укажите все правильные ответы» или «выберите наилучший ответ»).

Выбор правильных ответов

Естественно, чтобы сдать экзамен, необходимо правильно отвечать на вопросы. Однако сертификационные экзамены Microsoft не являются стандартизированными экзаменами наподобие SAT или GRE — они более хитрые и запутанные. Иногда вопросы сформулированы столь загадочно, что разобраться, что имеется в виду, совершенно невозможно. В таких случаях вам может понадобиться техника исключения. Обычно как минимум про один из предложенных вариантов ответов сразу ясно, что он неверен. Такой вариант ответа

- либо не имеет отношения к описываемой ситуации;
- либо описывает несуществующие объекты;
- либо не согласуется с текстом вопроса.

После того как вы исключите очевидно неверные ответы, напрягите вашу память, чтобы распознать и другие. Ищите варианты, которые выглядят подходяще, но ссылаются на команды, действия или возможности, недоступные в описываемой ситуации.

Если после исключения неверных ответов вы все еще вынуждены угадывать правильный ответ из нескольких вариантов, перечитайте вопрос. Постарайтесь нарисовать мысленную картину и представить, как в нее укладываются оставшиеся ответы.

Если вы не можете исключить еще какие-либо варианты, но так и не знаете, какой же ответ верен, у вас остается единственный путь — попробуйте угадать! Вопрос без ответа не принесет вам баллов, а угадывание все же дает шанс правильно ответить на вопрос. Однако не торопитесь. Угадывайте ответы на вопросы только тогда, когда время экзамена истекает и угадать ответ — ваш последний шанс.

Искоренение двусмысленностей

Вопросы экзаменов Microsoft имеют репутацию трудно понимаемых, запутанных и двусмысленных. Наш опыт показывает, что так оно и есть. Экзамены Microsoft трудно сдавать. Они разработаны так, чтобы их сдали примерно 30 процентов от общего числа экзаменуемых — иными словами, чтобы 70 процентов экзаменуемых провалились.

Единственный способ выиграть эту игру на чужом поле — быть готовым к ней. Вы обнаружите, что многие вопросы экзамена проверяют знание вами вещей, непосредственно не связанных с темой вопроса. Это означает, что не только вопросы, но и предлагаемые ответы (даже неверные) проверяют ваши знания. Если вы не знакомы со всеми тонкостями работы TCP/IP, вы не сможете исключить даже очевидно неверные варианты ответов, поскольку они могут относиться к областям TCP/IP, отличным от обсуждаемых в вопросе.

Формулировки вопросов часто содержат подсказки, но чтобы найти их, вы должны владеть дедуктивным методом лучше Шерлока Холмса. Зачастую подсказки включены в текст и выглядят ничего не значащей информацией. Вы должны понять, что каждый вопрос сам по себе является маленьким экзаменом, и от того, насколько хорошо вы будете справляться с такими экзаменами, зависит общий результат. Ищите подсказки в названиях групп, настроек или даже в указанных способах локального или удаленного доступа. Такие мелочи могут указать на правильный ответ; если же вы не будете обращать на них внимания, вам останется только выбирать ответ наугад.

Еще одна трудность экзаменов Microsoft — используемая терминология. Microsoft имеет скверную привычку давать утилитам и возмож-

ностям программ иногда интуитивно понятные, а иногда совершенно бессмысленные названия. Особенно это относится к печати и удаленному доступу: изучите термины, описанные в главе 13.

Структура работы

Вопросы экзамена располагаются в случайном порядке. Обращение к одной теме может дублироваться в нескольких вопросах, и таких тем немало. Зачастую получается так, что правильный ответ на один из вопросов также является неправильным ответом на другой. Прочитайте все предлагаемые варианты ответов, даже если вы сразу видите правильный. Неправильные ответы могут подхлестнуть вашу память при размышлениях над другим вопросом.

Вы можете изменять ответ на вопрос столько раз, сколько хотите. Если вы не уверены в ответе, установите специальный флажок — это позволит вам потом легко найти данный вопрос. Помечайте также вопросы, которые, как вы думаете, могут помочь вам при поиске ответа на другие вопросы. Мы при сдаче экзамена обычно помечаем от 25 до 50 процентов вопросов. Программное обеспечение, используемое на экзамене, разработано так, чтобы помочь вам отметить ответ на каждый вопрос — используйте его возможности. Помечайте все вопросы, которые вы хотели бы рассмотреть еще раз; программа поможет вам вернуться к ним.

Что нужно выучить наизусть?

Объем материала, который вам придется заучить, зависит от того, насколько хорошо вы запоминаете то, что читаете. Если у вас хорошая зрительная память и вы мысленно представляете выпадающие меню и окна диалога, вам не потребуется заучивать столько же, сколько тому, у кого зрительная память хуже.

Важно, чтобы вы выучили наизусть:

- На каких уровнях моделей TCP/IP и OSI находятся основные протоколы.
- Ключи реестра, относящиеся к настройке TCP/IP.
- Как расшифровать маску подсети (128+64+32+16+8+4+2+1).
- Процесс определения имен — как при помощи WINS, так и при помощи DNS.

Если вы проработали эту книгу, сидя за компьютером с Windows NT, для вас не составит проблемы запомнить эти важные данные.

Подготовка к экзамену

Лучший способ подготовиться к экзамену — после того, как вы изучили весь материал, — попытаться сдать как минимум один репетиционный экзамен. Эта глава содержит вариант такого экзамена; вопросы приведены после следующего раздела. Вы должны попытаться ответить на них в течение 90 минут. Будьте честными и не заглядывайте в предыдущие главы. После того как время истечет, проверьте себя — правильные ответы приведены в главе 18, «Ответы».

Если вы хотите попытаться сдать дополнительные репетиционные экзамены, вы можете найти их в Интернете по адресу www.microsoft.com/Train_Cert/.

Сдача экзамена

Расслабьтесь. После того как вы сели перед компьютером для сдачи экзамена, уже ничто не может улучшить ваши знания или подготовку к экзамену. Сделайте глубокий вдох, соберитесь и приступайте к первому вопросу.

Не суетитесь у вас вполне достаточно времени, чтобы ответить на вопросы и просмотреть второй раз пропущенные. Если вы прочитали вопрос дважды и все еще не знаете ответ, пометьте этот вопрос и двигайтесь дальше. Простые и сложные вопросы распределены по экзамену в случайном порядке. Не навредите себе, потратив на сложный вопрос так много времени, что вы не успеете ответить на простые вопросы, расположенные ближе к концу экзамена. Пройдите через весь экзамен и, прежде чем вернуться к помеченным вопросам, проверьте, сколько времени вы затратили и на сколько вопросов ответили. После того как вы найдете ответ на вопрос, снимайте с него пометку. Продолжайте пересматривать помеченные вопросы до тех пор, пока время экзамена не подойдет к концу или пока вы не ответите на все вопросы.

Вот и все советы, которые мы хотели вам дать. Приступайте к репетиционному экзамену.

Пример экзамена

Question 1

A DHCP-enabled client is moved from Subnet A to Subnet B. After the move, the users complain that they are no longer able to use TCP/IP. What is the possible cause for the problem?

- A. DHCP cannot support multiple subnets.
- B. The WINS server cannot see the client.
- C. The default gateway was configured manually before the computer was moved.
- D. The client did not terminate its lease before the computer was moved.

Вопрос 1

DHCP-клиент был перемещен из подсети A в подсеть B, после чего пользователи сообщили, что они больше не могут использовать TCP/IP на этой машине. Чем может быть вызвана эта проблема?

- A. DHCP не может поддерживать несколько подсетей.
- B. Сервер WINS не видит клиента.
- C. Адрес шлюза по умолчанию был установлен вручную до переноса компьютера в другую подсеть.
- D. Клиент не прервал DHCP-аренду до его переноса в другую подсеть.

Question 2

A request is sent to an SNMP-managed device but no responce is obtained. Assume the community name is correct, the OID is correct, and a request with other OIDs does elicit a responce. What could be the problem?

- A. The network is unstable.
- B. The request is a **set** request.
- C. There is no alarm condition.
- D. This is not a manageable device.

Вопрос 2

SNMP-устройству был отправлен запрос, но ответ не был получен. Предположим, что имя сообщества и OID были указаны правильно и запросы с другими OID приводят к получению ответа. Как это можно объяснить?

- A. Сеть работает нестабильно.
- B. Отправленный запрос был set-запросом.
- C. Ситуация не требует отправки предупреждения.
- D. Устройство не поддерживает SNMP.

Question 3

Which of the following describe a router? (Check all correct answers.)

- ❑ A. A gateway.
- ❑ B. An information service.
- ❑ C. A specialized standalone device.
- ❑ D. Software used to exchange email.

Вопрос 3

Что можно назвать маршрутизатором? (Укажите все правильные ответы.)

- ❑ A. Шлюз.
- ❑ B. Информационную службу.
- ❑ C. Отдельное специализированное устройство.
- ❑ D. Программное обеспечение, используемое для обмена электронной почтой.

Question 4

After monitoring your network for a week, you have concluded that your Windows NT Server, which is acting as a router, is dropping packets. Which of the following Registry settings can be used to correct this problem? (Check all correct answers:)

- ❑ A. TcpBufferSize
- ❑ B. TcpWindowSize
- ❑ C. ForwardBufferMemory
- ❑ D. NumForwardPackets

Вопрос 4

После наблюдений за вашей сетью в течение недели вы установили, что ваш Windows NT Server, работающий в качестве маршрутизатора, теряет пакеты. Какие из следующих ключей реестра могут быть использованы для решения этой проблемы?

- ❑ A. TcpBufferSize
- ❑ B. TcpWindowSize
- ❑ C. ForwardBufferMemory
- ❑ D. NumForwardPackets

Question 5

By default, how many hosts will a Class B address support?

- A. 65,534
- B. 254
- C. 2,097,152
- D. 16,384

Вопрос 5

Сколько узлов поддерживает по умолчанию сеть класса B?

- A. 65,534
- B. 254
- C. 2,097,152
- D. 16,384

Question 6

By default, the first ___ octet(s) of a Class C address are used to identify the network ID.

- A. 1
- B. 2
- C. 3
- D. 4

Вопрос 6

Количество октетов, используемых по умолчанию для идентификатора сети адреса класса C равно

- A. 1
- B. 2
- C. 3
- D. 4

Question 7

Choose from the following options the answer that best describes the purpose of a subnet mask.

- A. The subnet mask is used to help TCP/IP distinguish the network ID from the host ID. This aids in determining the IP address of other hosts.
- B. The subnet mask aids in determining the location of other TCP/IP hosts.
- C. The subnet mask is used to mask a portion of an IP address for TCP/IP.
- D. The subnet mask is used to help TCP/IP distinguish the network ID from the host ID. This aids in determining the location of other TCP/IP hosts.

Вопрос 7

Какой из следующих ответов наилучшим образом описывает назначение маски подсети?

- A. Маска подсети позволяет TCP/IP отделить адрес сети от адреса узла. Это помогает определять IP-адреса других узлов.
- B. Маска подсети позволяет определить местонахождение других TCP/IP-узлов.
- C. Маска подсети используется TCP/IP для маскирования части IP-адреса.
- D. Маска подсети позволяет TCP/IP отделить адрес сети от адреса узла. Это помогает определить местонахождение других TCP/IP-узлов.

Question 8

Choose the option that best defines TCP/IP.

- A. A suite of protocols designed by Microsoft to allow everyday people to access resources on the Internet.
- B. A suite of protocols that allows communicaton between different types of applications running on various platforms an in various network environments.
- C. A protocol designed by Microsoft to allow information to be routed between heterogeneous network environments.
- D. A protocol designed by the IAB to allow many different hardware and software vendors to access the Internet.

Вопрос 8

Что такое TCP/IP? (Выберите наилучший ответ.)

- A. Набор протоколов, разработанный Microsoft для того, чтобы позволить обычным пользователям получать доступ к ресурсам в Интернете.
- B. Набор протоколов, позволяющий взаимодействовать различным приложениям, работающим на различных аппаратных платформах и в различных типах сетей.
- C. Протокол, разработанный Microsoft для маршрутизации информации между разнородными сетями.
- D. Протокол, разработанный IAB для того, чтобы различные производители программного и аппаратного обеспечения могли получить доступ к Интернету.

Question 9

Each of the following statements lists layers of the OSI Reference Model and the respective layers of the TCP/IP Reference Model. Which of the following statements correctly maps corresponding layers? (Check all correct answers.)

- ❑ A. OSI Presentation and TCP/IP Application.
- ❑ B. OSI Session and TCP/IP Transport.
- ❑ C. OSI Network and TCP/IP Internet.
- ❑ D. OSI Physical and TCP/IP Network Interface.

Вопрос 9

Каждый из приведенных ответов описывает соответствие между уровнем эталонной модели OSI и уровнем модели TCP/IP. Какие соответствия указаны правильно? (Укажите все правильные ответы.)

- ❑ A. OSI: уровень представления; TCP/IP: уровень приложения.
- ❑ B. OSI: уровень сеанса; TCP/IP: уровень транспорта.
- ❑ C. OSI: уровень сети; TCP/IP: межсетевой уровень.
- ❑ D. OSI: физический уровень; TCP/IP: уровень сетевого интерфейса.

Question 10

After checking its cache, what step does a computer take when resolving an address on the local network?

- ○ A. Sends a request to the router.
- ○ B. Sends a request to the ARP server.
- ○ C. Checks its HOSTS file for the information.
- ○ D. Sends a broadcast packet.

Вопрос 10

Что предпринимает компьютер после проверки кэша при определении адреса в локальной сети?

- ○ A. Отправляет запрос на маршрутизатор.
- ○ B. Отправляет запрос на сервер ARP.
- ○ C. Обращается к файлу HOSTS.
- ○ D. Отправляет широковещательный запрос.

Question 11

As an administrator, you have recently implemented SNMP on your Windows NT system. However, you don't think it's working correctly. Which of the following applications can you use to troubleshoot SNMP errors?

- A. Registry Editor.
- B. Event Viewer.
- C. Performance Monitor.
- D. Task Manager.

Вопрос 11

Как администратор сети вы недавно установили SNMP на вашей Windows NT системе. Однако вам кажется, что SNMP работает неправильно. Какое из следующих приложений лучше всего использовать для поиска проблем, связанных с SNMP?

- A. Редактор реестра (Registry Editor).
- B. Монитор событий (Event Viewer).
- C. Монитор производительности (Performance Monitor).
- D. Диспетчер задач (Task Manager).

Question 12

What is the binary value of the decimal number 213?

- A. 11010101
- B. 11100001
- C. 11111000
- D. 11111001

Вопрос 12

Какое двоичное значение соответствует десятичному числу 213?

- A. 11010101
- B. 11100001
- C. 11111000
- D. 11111001

Question 13

UDP resides at which layer of the TCP/IP protocol stack? (Choose the best answer.)

- A. Network Interface.
- B. Internet.
- C. Transport.
- D. Application.

Вопрос 13

На каком уровне модели TCP/IP находится протокол UDP? (Выберите наилучший ответ)

- A. На уровне сетевого интерфейса.
- B. На межсетевом уровне.
- C. На уровне транспорта.
- D. На уровне приложения.

Question 14

A new computer has been added to the network. Although you configured it yourself, the computer is having problems communicating. When you use IPCONFIG, you notice that the subnet mask is 0.0.0.0. What could be the problem?

- A. There's another computer with the same DNS configuration.
- B. There's another computer with the same WINS configuration.
- C. There's another computer with the same NetBIOS name.
- D. There's another computer with the same IP address.

Вопрос 14

В вашу сеть был включен новый компьютер. Хотя вы настраивали его самостоятельно, при работе с сетью возникают проблемы. Утилита IPCONFIG утверждает, что маска подсети — 0.0.0.0. В чем причина проблемы?

- A. В сети имеется другой компьютер с такой же настройкой DNS.
- B. В сети имеется другой компьютер с такой же настройкой WINS.
- C. В сети имеется другой компьютер с таким же именем NetBIOS.
- D. В сети имеется другой компьютер с таким же IP-адресом.

Question 15

You have added a new #PRE entry to the LMHOSTS file to your computer and you want to verify that the changes you made are being used. Which of the following sets of commands will you use to test whether or not the file you edited is located in the correct directory and is being used for resolution?

- A. NBTSTAT -r, followed by NBTSTAT -c
- B. NBTSTAT -R, followed by NBTSTAT -c
- C. NETSTAT -r, followed by NBTSTAT -d
- D. NETSTAT -R, followed by NBTSTAT -d

Вопрос 15

Вы добавили в файл LMHOSTS новую запись #PRE и хотите проверить внесенные изменения. Какие команды вы используете, чтобы проверить, что файл, который вы редактировали, находится в правильном каталоге и используется при определении имен?

- A. NBTSTAT -r, затем NBTSTAT -c
- B. NBTSTAT -R, затем NBTSTAT -c
- C. NETSTAT -r, затем NBTSTAT -d
- D. NETSTAT -R, затем NBTSTAT -d

Question 16

Juanita has just taken over the desktop support for her company. She is setting up a new laptop on the local subnet for the boss. During setup, she gets the following error message: «Your default gateway does not belong to one of the configured interfaces...» What should Juanita do?

- A. Check the PCMCIA card and reinsert it.
- B. Check the spelling of the default gateway entry in the LMHOSTS file.
- C. Check the cabling.
- D. Run IPCONFIG.

Вопрос 16

Нина устанавливает в локальной подсети новый переносной компьютер для своего начальника. При установке она получает следующее сообщение об ошибке: «Your default gateway does not belong to one of the configured interfaces...» («Шлюз по умолчанию не соответствует ни одному из настроенных сетевых интерфейсов...»). Что должна сделать Нина?

- A. Проверить PCMCIA-карту и вставить ее заново.
- B. Проверить запись, соответствующую шлюзу по умолчанию, в файле LMHOSTS.
- C. Проверить подключение кабелей.
- D. Запустить утилиту IPCONFIG.

Question 17

Mary is having some problems with her TCP/IP network. She tries PINGing her local machine, the local gateway (router), and a remote router with success on every occasion. However, when she tries to use the NET USE command to set up a drive mapping to the Engineering server's NetBIOS name, the command fails. She tries the NET VIEW command with the NetBIOS name and it also fails. Finally, she tries a PING to the NetBIOS name and it succeeds. She calls the Engineering department and finds out that the computer is not hung and that she typed the NetBIOS name correctly. What else can Mary do to troubleshoot this problem? (Check all correct answers.)

- ❑ A. Check to make sure the Server service has started.
- ❑ B. Verify that a DNS is working properly and the HOSTS file is correct.
- ❑ C. Check to see whether the entry in question has been misspelled or entered incorrectly.
- ❑ D. Check to see whether there are two different machines with the same NetBIOS name and neither knows if other has responded, so both machines refuse to connection.

Вопрос 17

Мария испытывает проблемы со своей TCP/IP сетью. Она использовала утилиту PING для отправки эхо-запросов на локальную машину, локальный шлюз (маршрутизатор) и удаленный маршрутизатор — и в каждом случае получила ответ. Однако, когда она попыталась применить команду NET USE для подключения сетевого диска с сервера отдела разработки, используя его имя NetBIOS, ничего не получилось. Команда NET VIEW для данного имени NetBIOS также не сработала. Наконец, она попыталась отправить эхо-запрос на этот сервер, передав команде PING в качестве аргумента имя NetBIOS сервера, и получила ответ. Она позвонила в отдел разработки и убедилась, что сервер работает и что она вводит его имя NetBIOS правильно. Что еще может сделать Мария для поиска проблемы? (Укажите все правильные ответы.)

- ❑ A. Проверить, запущена ли служба сервера.
- ❑ B. Проверить, что DNS работает правильно, и проверить файл HOSTS.
- ❑ C. Проверить, правильно ли она вводила имя NetBIOS.
- ❑ D. Проверить, нет ли в сети машины с тем же именем NetBIOS и не получается ли так, что ни одна из них не знает, ответила ли другая на запрос, и в результате обе машины отказываются устанавливать соединение.

Question 18

By using the Advanced IP Addressing properties sheet, how many addresses can be added to an interface?

- ○ A. 7
- ○ B. 8
- ○ C. 5
- ○ D. 6

Вопрос 18

Сколько адресов может быть добавлено в окне диалога Advanced IP Addressing?

- ○ A. 7
- ○ B. 8
- ○ C. 5
- ○ D. 6

Question 19

You have just installed the SNMP service on a Windows NT computer. Which of the following functions can you now perform? (Check all correct answers.)

- ☐ A. Use the *Resource Kit* utilities to perform management functions.
- ☐ B. Monitor and configure parameters for any DHCP server.
- ☐ C. View and change parameters in the MIBs by using SNMP manager programs.
- ☐ D. Monitor and configure parameters for any WINS server.

Вопрос 19

Вы только что установили службу SNMP на компьютере, работающем под управлением Windows NT. Какие возможности вы теперь получаете? (Укажите все правильные ответы.)

- ☐ A. Использовать утилиты из набора *Resource Kit* для выполнения управляющих функций.
- ☐ B. Просматривать и изменять настройки серверов DHCP.
- ☐ C. Просматривать и изменять параметры баз данных MIB, используя программы-диспетчеры SNMP.
- ☐ D. Просматривать и изменять настройки серверов WINS.

Question 20

Shannon is getting ready to subnet his IP network and must determine the number of network IDs required before he can calculate an appropriate subnet mask for his network. Which of the following options would help him properly calculate the number of necessary network Ids? (Check all correct answers.)

- ☐ A. Calculate a unique network ID for each network printer on a segment.
- ☐ B. Calculate a unique network ID for each segment of the network bordered by a router.
- ☐ C. Calculate only one unique network ID for network segments bordered by two or more routers.
- ☐ D. Calculate a unique network ID for each interface of a router.

Вопрос 20

Александр собирается разбить свою сеть на подсети и должен определить необходимое количество адресов сетей, чтобы он мог вычислить маску подсети. Что он должен посчитать при вычислении количества необходимых адресов сетей? (Укажите все правильные ответы.)

- ❑ A. Каждый сетевой принтер в каждом сегменте.
- ❑ B. Каждый сегмент, отделенный от остальной сети одним маршрутизатором.
- ❑ C. Один раз каждый сегмент, отделенный от остальной сети несколькими маршрутизаторами.
- ❑ D. Каждый интерфейс маршрутизатора.

Question 21

The Billington Steambath Company currently has nine divisions, and each one requires its own subnet. The company has been assigned the network ID 130.121.0.0. *Billington anticpated the need to support up to 3,000 hosts in each division.* Which subnet would you recommend that it use?

- ○ A. 255.255.240.0
- ○ B. 255.255.255.0
- ○ C. 255.255.224.0
- ○ D. 255.255.248.0

Вопрос 21

Великорусская банная компания состоит из девяти подразделений, каждому из которых требуется своя собственная подсеть. Компания получила идентификатор сети 130.121.0.0. Требуется поддержка до 3000 узлов в подразделении. Какую маску подсети вы бы посоветовали использовать?

- ○ A. 255.255.240.0
- ○ B. 255.255.255.0
- ○ C. 255.255.224.0
- ○ D. 255.255.248.0

Question 22

Which of the following correctly states the order of the first four steps of the NetBIOS name resolution process?

- ○ A. NetBIOS name cache, b-node broadcast, LMHOSTS, WINS.
- ○ B. WINS, NetBIOS name cache, b-node broadcast, LMHOSTS.
- ○ C. NetBIOS name cache, WINS, b-node broadcast, LMHOSTS.
- ○ D. B-node broadcast, WINS, NetBIOS name cache, LMHOSTS.

Вопрос 22

Какой из ответов перечисляет первые четыре шага процесса определения имен NetBIOS в правильном порядке?

- A. Кэш имен NetBIOS, широковещательный B-запрос, файл LMHOSTS, WINS.
- B. WINS, кэш имен NetBIOS, широковещательный B-запрос, файл LMHOSTS.
- C. Кэш имен NetBIOS, WINS, широковещательный B-запрос, файл LMHOSTS.
- D. Широковещательный B-запрос, WINS, кэш имен NetBIOS, файл LMHOSTS.

Question 23

The following statements describe individual parts of the threeway handshake used to establish a session. Which of these statements is incorrect?

- A. «I have information for you, can we establish communication?»
- B. «Great, I received your responce, here is the rest of the information.»
- C. «Yes, I am available for communication. Continue with your transmission.»
- D. «No, I am busy right now and don't have time for you. Try back in few minutes.»

Вопрос 23

Следующие утверждения описывают отдельные стадии трехступенчатого открытия соединения. Какое из утверждений неверно?

- A. «У меня есть информация для тебя. Можем мы установить соединение?»
- B. «Отлично, я получил твой ответ. Вот остаток информации.»
- C. «Да, я готов к открытию соединения. Продолжай передачу.»
- D. «Нет, я сейчас занят и у меня нет времени на тебя. Попытайся еще раз через несколько минут.»

Question 24

The ROUTE utility can be used to perform what functions to a routing table? (Check all correct answers.)

- ☐ A. Test a route.
- ☐ B. Add new routes.
- ☐ C. Remove gateway entries.
- ☐ D. Display existing routes.

Вопрос 24

Какие операции позволяет выполнять утилита ROUTE над таблицей маршрутизации? (Выберите все правильные ответы.)

- ❑ A. Протестировать путь.
- ❑ B. Добавить новые пути.
- ❑ C. Удалить записи о шлюзе.
- ❑ D. Вывести список существующих путей.

Question 25

Three attributes can be defined in the Only Accept SNMP Packets From These Hosts section of the SNMP Security tab. The are: (Check all correct answers.)

- ❑ A. IPX address
- ❑ B. IP address
- ❑ C. MAC adress
- ❑ D. Host name

Вопрос 25

В области Only Accept SNMP Packets From These Hosts вкладки SNMP Security могут быть установлены три атрибута. Какие? (Укажите все правильные ответы.)

- ❑ A. IPX-адрес
- ❑ B. IP-адрес
- ❑ C. MAC-адрес
- ❑ D. Имя узла

Question 26

Using the default host name resolution order for Microsoft Windows NT, complete the following statement: «After checking the local _____, the _____ is consulted. If it cannot resolve the host name, TCP/IP will next consult the _____.»

- ○ A. host name; the LMHOSTS file; NetBIOS name cache.
- ○ B. HOSTS file; local DNS server; NetBIOS name cache.
- ○ C. DNS server; NetBIOS name cache; local host name.
- ○ D. NetBIOS name cache; WINS server; local HOSTS file.

Вопрос 26

Считая, что определение имени узла происходит в порядке, заданном по умолчанию, вставьте слова в следующее предложение: «После того как TCP/IP произведет проверку локального _____, производится обращение к _____. Если нужный IP-адрес еще не найден, TCP/IP обратится к _____.»

- ○ A. имени узла, файлу LMHOSTS, кэш имен NetBIOS.
- ○ B. файла HOSTS, локальному серверу DNS, кэш имен NetBIOS.

- C. сервера DNS, кэшу имен NetBIOS, локальному имени узла.
- D. кэша имен NetBIOS, серверу WINS, локальному файлу HOSTS.

Question 27

What is the default time an entry will stay in the ARP cache?

- A. 10 minutes
- B. 20 minutes
- C. 5 minutes
- D. 1 minute

Вопрос 27

Какое время сохраняется запись в кэше ARP по умолчанию?

- A. 10 минут
- B. 20 минут
- C. 5 минут
- D. 1 минуту

Question 28

What type of address resolution takes place with proxy ARP?

- A. Remote address resolution.
- B. Local address resolution.
- C. Kinetic address resolution.
- D. Router address resolution.

Вопрос 28

Какой тип сопоставления адреса производится при помощи прокси-ARP?

- A. Удаленое сопоставление адреса.
- B. Локальное сопоставление адреса.
- C. Кинетическое сопоставление адреса.
- D. Маршрутизируемое сопоставление адреса.

Question 29

What types of transactions can be performed by an SNMP agent? (Check all correct answers.)

- ❑ A. Send trap
- ❑ B. Get
- ❑ C. GetAll
- ❑ D. VarBind

Вопрос 29

Какие типы передачи могут производиться агентом SNMP? (Отметьте все правильные ответы.)

- ❑ A. Отправка сообщения-захвата.
- ❑ B. Get.
- ❑ C. GetAll.
- ❑ D. VarBind.

Question 30

Which items detailed in a routed packet are not the same when the packet reaches its destination as compared to their original values at the source host? (Check all correct answers.)

- ❑ A. Source HWA.
- ❑ B. Source IP address.
- ❑ C. Destination HWA.
- ❑ D. Destination IP address.

Вопрос 30

Какие данные в полученном маршрутизированном пакете отличаются от того, что содержал пакет при отправке? (Отметьте все правильные ответы.)

- ❑ A. Аппаратный адрес отправителя.
- ❑ B. IP-адрес отправителя.
- ❑ C. Аппаратный адрес получателя.
- ❑ D. IP-адрес получателя.

Question 31

Which method of host name resolution uses a single static text file to resolve Internet names? (Choose the best answer.)

- ○ A. LMHOSTS.
- ○ B. HOSTS.
- ○ C. Domain Name Space.
- ○ D. Domain Name System.

Вопрос 31

Какой из методов определения имен использует один текстовый файл для определения имен Интернет-узлов.

- ○ A. LMHOSTS.
- ○ B. HOSTS.
- ○ C. Пространство имен доменов.
- ○ D. Система имен доменов.

Question 32

Which of the following are benefits of subnetting a given network ID? (Check all correct answers.)

- ❑ A. Subnetting allows the interconnection of networks that use different network technologies.
- ❑ B. Subnetting allows you to overcome the physical limitations of a network's capacity.
- ❑ C. Subnetting allows for an effective increase in network bandwidth by cutting down on the amount of broadcasts a network must process.
- ❑ D. Subnetting allows for the arbitrary allocation of IP addresses, regardless of host location.

Вопрос 32

В чем состоят преимущества разбиения сети на подсети? (Укажите все правильные ответы.)

- ❑ A. Разделение на подсети позволяет связывать сети, использующие разные сетевые технологии.
- ❑ B. Разделение на подсети позволяет преодолеть физические ограничения на размер сети.
- ❑ C. Разделение на подсети увеличивает пропускную способность сети, снижая количество широковещательных сообщений, обрабатываемых компьютерами в сети.
- ❑ D. Разделение на подсети позволяет произвольно выбирать IP-адрес узла, вне зависимости от его местонахождения.

Question 33

Which of the following are benefits of using DHCP? (Check all correct answers.)

- ❑ A. Less chance of human error.
- ❑ B. Centralized IP name resolution.
- ❑ C. Dynamic NetBIOS name registration.
- ❑ D. Dynamic IP configuration.

Вопрос 33

В чем состоят преимущества использования DHCP? (Укажите все правильные ответы.)

- ❑ A. *Уменьшение шансов на человеческую ошибку.*
- ❑ B. Централизованное определение IP-имен.
- ❑ C. Динамическая регистрация имен NetBIOS.
- ❑ D. Динамическая настройка IP.

Question 34

Which of the following are benefits of using WINS? (Check all correct answers.)

- ❑ A. Dynamic NetBIOS name registration.
- ❑ B. Dynamic IP configuration.
- ❑ C. Reduction in broadcast traffic.
- ❑ D. Increase in network throughput capacity.

Вопрос 34

В чем состоят преимущества использования WINS? (Укажите все правильные ответы.)

- ❑ A. Динамическая регистрация имен NetBIOS.
- ❑ B. Динамическая настройка IP.
- ❑ C. Уменьшение широковещательного трафика.
- ❑ D. Увеличение общей мощности сети.

Question 35

Which of the following are items found in a static routing table? (Check all correct answers.)

- ❑ A. Interface IP.
- ❑ B. Hop metric.
- ❑ C. Network address.
- ❑ D. Netmask.

Вопрос 35

Какие поля содержатся в статической таблице маршрутизации? (Укажите все правильные ответы.)

- ❑ A. IP адрес сетевого интерфейса.
- ❑ B. Метрика.
- ❑ C. Адрес сети.
- ❑ D. Маска подсети.

Question 36

Your Windows NT computer is attached to a network with numerous Unix machines. Which of the following utilities could you use to execute a command on one of those systems? (Check all correct answers.)

- ❑ A. RPD
- ❑ B. REXEC
- ❑ C. RCP
- ❑ D. RSH

Вопрос 36

Ваш компьютер, работающий под управлением Windows NT, подключен к сети, содержащей множество Unix-машин. Какие из следующих утилит вы можете использовать для выполнения команд на одной из Unix-систем?

- ❑ A. RPD
- ❑ B. REXEC
- ❑ C. RCP
- ❑ D. RSH

Question 37

Which of the following commands will not result in the HOSTS file being accessed?

- ○ A. TRACERT
- ○ B. TFTP
- ○ C. NET VIEW
- ○ D. PING

Вопрос 37

Какая из следующих команд не приведет к обращению к файлу HOSTS?

- ○ A. TRACERT
- ○ B. TFTP
- ○ C. NET VIEW
- ○ D. PING

Question 38

Which of the following files contain DNS resource records for name resolution? (Check all correct answers.)

- ❑ A. 12.122.205.IN-ADDR.ARPA.DNS
- ❑ B. Boot file
- ❑ C. CACHE.DNS
- ❑ D. LANW.COM.DNS

Вопрос 38

Какие из следующих файлов содержат записи ресурсов DNS, используемые для определения имен?

- ❑ A. 12.122.205.IN-ADDR.ARPA.DNS
- ❑ B. Boot file
- ❑ C. CACHE.DNS
- ❑ D. LANW.COM.DNS

Question 39

In implementing your new TCP/IP network, you would like to use host names to identify computers on your network. Your boss, on the other hand, thinks that it's too much work to assign and keep track of the names. Which of the following arguments could you use to convince your boss to implement a host name system? (Check all correct answers.)

- ❑ A. Host names are easier to remember than IP addresses.
- ❑ B. Host names allow you to assign several IP addresses to the same machine.
- ❑ C. Alphanumeric host names can convey more meaning than plain numeric IP addresses.
- ❑ D. The use of a host name to identify a machine allows the IP address and location of the machine to be transparent to the end user.

Вопрос 39

Вы проектируете новую TCP/IP-сеть и хотели бы использовать имена узлов для идентификации компьютеров. Однако ваш начальник считает, что процесс присвоения и отслеживания имен слишком сложен и требует выполнения большого объема работ. Какие аргументы вы можете использовать, убеждая начальника в необходимости реализации системы имен узлов? (Укажите все правильные ответы.)

- ❑ A. Имена узлов проще запоминать, чем IP-адреса.
- ❑ B. Имена узлов позволяют присвоить несколько IP-адресов одному компьютеру.
- ❑ C. Имена узлов, состоящие из алфавитно-цифровых символов, могут нести больший смысл, нежели чисто цифровые IP-адреса.
- ❑ D. Использование имен узлов для идентификации компьютеров делает IP-адрес и местонахождение компьютера несущественными для конечного пользователя.

Question 40

Which of the following protocols uses Scope ID to limit communications?

- ○ A. NBT
- ○ B. TCP
- ○ C. NetBEUI
- ○ D. NWLink

Вопрос 40

Какой из следующих протоколов использует идентификатор контекста для ограничения взаимодействий?

- ○ A. NBT
- ○ B. TCP
- ○ C. NetBEUI
- ○ D. NWLink

Question 41

Which of the following statements about configuring a host name on a Windows NT machine are true? (Check all correct answers.)

- ❑ A. You must change the default host name (that is, the original NetBIOS name) to some name other than the name that is currently being used as the NetBIOS name.
- ❑ B. By default, the NetBIOS name of the machine will be used as the host name.
- ❑ C. Any invalid characters in the NetBIOS name will be converted to dashes (-) in the host name.
- ❑ D. You can configure the host name and the DNS domain name in the DNS properties sheet of the TCP/IP properties.

Вопрос 41

Какие из следующих утверждений о настройке системы верны для компьютера, работающего под управлением Windows NT? (Укажите все правильные ответы.)

- ❑ A. Вы должны заменить устанавливаемое по умолчанию имя узла (совпадающее с именем NetBIOS компьютера) на имя, не используемое в качестве имени NetBIOS.
- ❑ B. По умолчанию имя NetBIOS компьютера используется в качестве имени узла.
- ❑ C. Все недопустимые символы в имени NetBIOS преобразуются в дефисы (-) в имени узла.
- ❑ D. Вы можете установить имя узла и имя домена на вкладке DNS окна свойств TCP/IP.

Question 42

Which of the following statements are potential problems that can occur when using the LMHOSTS file? (Check all correct answers.)

- ❑ A. The LMHOSTS file is not in the root directory of the system drive.
- ❑ B. The LMHOSTS file has been saved with incorrect name or extension.
- ❑ C. The entry in file has been misspelled or entered incorrectly.
- ❑ D. There are two different entries for the same NetBIOS name, and the one that occurs first in the list is incorrect.

Вопрос 42

Какие из следующих утверждений описывают потенциальные проблемы, которые могут возникнуть при использовании файла LMHOSTS? (Укажите все правильные ответы.)

- ❑ A. Файл LMHOSTS не находится в корневом каталоге системного диска.
- ❑ B. Файл LMHOSTS имеет неверное имя или расширение.
- ❑ C. Запись в файле содержит опечатку или неверна.
- ❑ D. В файле содержатся две записи для одного имени NetBIOS, и та из них, которая встречается первой, ошибочна.

Question 43

Which of the following utilities can be used to administer the DHCP database?

- ○ A. IPCONFIG.
- ○ B. JETPACK.
- ○ C. DHCP Manager.
- ○ D. Network applet.

Вопрос 43

Какая из следующих утилит может использоваться для администрирования базы данных DHCP?

- ○ A. IPCONFIG.
- ○ B. JETPACK.
- ○ C. Диспетчер DHCP (DHCP Manager).
- ○ D. Приложение Сеть (Network) панели управления.

Question 44

Which of the following utilities is used to monitor printing on a remote Unix system?

- ○ A. LPD
- ○ B. LPS
- ○ C. LPQ
- ○ D. LPR

Вопрос 44

Какая из следующих утилит может использоваться для наблюдения за процессом печати на удаленной Unix-системе?

- ○ A. LPD
- ○ B. LPS
- ○ C. LPQ
- ○ D. LPR

Question 45

Which of the following utilities is used to monitor the network? (Check all correct answers.)

- ❑ A. WINS Monitor
- ❑ B. Ethernet Monitor
- ❑ C. Performance Monitor
- ❑ D. Network Monitor

Вопрос 45

Какие из следующих утилит могут использоваться для наблюдения за состоянием сети? (Укажите все правильные ответы.)

- ❑ A. WINS Monitor
- ❑ B. Ethernet Monitor
- ❑ C. Performance Monitor
- ❑ D. Network Monitor

Question 46

Which of the following utilities provide file transfer capabilities in a TCP/IP environment? (Check all correct answers.)

- ❑ A. FTP
- ❑ B. RSH
- ❑ C. Telnet
- ❑ D. RCP

Вопрос 46

Какие из следующих утилит позволяют производить пересылку файлов в рамках TCP/IP? (Укажите все правильные ответы.)

- ❑ A. FTP
- ❑ B. RSH
- ❑ C. Telnet
- ❑ D. RCP

Question 47

Which types of names can WINS resolve for DNS?

- ○ A. Host
- ○ B. FQDN
- ○ C. Domain
- ○ D. Root

Вопрос 47

Какой тип имен может определять WINS по запросу DNS?

- ○ A. Имена узлов.
- ○ B. Полные доменные имена узлов (FQDN).
- ○ C. Имена доменов.
- ○ D. Корневые имена.

Question 48

Why is the dynamic routing protocol RIP limited to 15 hops?

- ○ A. To prevent infinite counting of looped paths.
- ○ B. To force large networks to be divided into smaller subnets.
- ○ C. No network system ever needs more than 15 hops.
- ○ D. The routing table uses hex codes to store hop values.

Вопрос 48

Почему длина маршрута при использовании протокола маршрутизации RIP ограничена 15 хопами?

- ○ A. Чтобы предотвратить появление бесконечных циклов.
- ○ B. Чтобы большие сети разбивались на подсети.
- ○ C. Ни в одной сети не могут понадобиться более длинные маршруты.
- ○ D. Таблица маршрутизации использует шестнадцатеричные коды для хранения длины маршрута.

Question 49

You're attempting to resolve a communication problem with a computer named «bob15» on a remote subnet. You can successfully PING other computers on the same subnet as bob15; however, when you try to PING bob15, you get no responce. Which of the following could be the problem? (Check all correct answers.)

- ☐ A. Bob15 has a NetBIOS scope ID that is different from the other computers, including yours.
- ☐ B. Bob15 has an incorrect default gateway.
- ☐ C. Your default gateway is configured incorrectly.
- ☐ D. Bob15 is offline.

Вопрос 49

Вы пытаетесь разрешить проблему с компьютером «bob15» в удаленной подсети. Вы получаете ответы от других компьютеров той же подсети, в которой находится компьютер «bob15», при использовании утилиты PING, но не от самого «bob15». В чем может заключаться проблема? (Укажите все правильные ответы.)

- ☐ A. Идентификатор контекста NetBIOS отличается от установленного на других компьютерах — в том числе от установленного на вашем.
- ☐ B. На компьютере bob15 неверно указан шлюз по умолчанию.
- ☐ C. На вашем компьютере неверно указан шлюз по умолчанию.
- ☐ D. Компьютер bob15 отключен от сети или выключен.

Question 50

You're getting ready to install and configure TCP/IP on your Windows NT Server. Which of the following items is not a requirement to complete the installation?

- ❑ A. You must have a good understanding of the required settings and configurations.
- ❑ B. You must be a member of the local administrators group for the machine you are configuring.
- ❑ C. You must have some type of access to the original installation files.
- ❑ D. You must be a domain administrator for the domain in which the machine is installed.

Вопрос 50

Вы собираетесь установить и настроить поддержку TCP/IP на Windows NT Server. Что для этого не требуется?

- ❑ A. Вы должны хорошо понимать параметры и настройки TCP/IP.
- ❑ B. Вы должны быть членом локальный группы Администраторы (Administrators).
- ❑ C. Вы должны иметь доступ к установочным файлам Windows NT.
- ❑ D. Вы должны быть администратором домена, в котором находится компьютер.

Question 51

You're thinking about creating an application that will require a constant end-to-end connection with another machine that is running a corresponding service. You do not want to include code in your program that ensures the data is arriving at its destination in an orderly and timely fashion. With these requirements in mind, which of the following protocols is most appropriate for use with your application?

- ○ A. TCP
- ○ B. UDP
- ○ C. ARP
- ○ D. ICMP

Вопрос 51

Вы разрабатываете приложение, которое потребует постоянного взаимодействия с другим компьютером, на котором будет запущена соответствующая служба. Вы не хотите включать в программу код, проверяющий, что данные были получены адресатом в правильном порядке в нужное время. Какой из перечисленных ниже протоколов подойдет для использования в вашем приложении?

- ○ A. TCP
- ○ B. UDP
- ○ C. ARP
- ○ D. ICMP

Question 52

You have been asked to configure several Windows NT workstations for your company's network that uses DNS and WINS for name resolution.

Required Result:

The computers must be able to communicate with each other via a computer name, Internet-style name, or IP address.

Optional Desired Results:

Keep the broadcast traffic to a minimum.

Give the clients a level of fault tolerance for name resolution if the primary WINS server is unavailable.

Proposed Solution:

Place an LMHOSTS file on each computer that has mappings for the computer names and IP addresses.

Which results does the proposed solution produce?

- A. The proposed solution produces the required result and produces both of the optional desired results.
- B. The proposed solution produces the required result and produces only one of the optional results.
- C. The proposed solution produces the required result but does not produce any of the optional desired results.
- D. The proposed solution does not produce the required result.

Вопрос 52

Вам требуется настроить несколько рабочих станций в сети вашей компании, использующей для определения имен WINS и DNS.

Требуемый результат:

Компьютеры должны иметь возможность взаимодействовать друг с другом, указывая адресат при помощи имени компьютера, его Интернет-имени или IP-адреса.

Необязательные желательные результаты:

Свести широковещательный трафик к минимуму.

Обеспечить отказоустойчивость на случай отказа основного сервера WINS.

Предлагаемое решение:

Поместить на каждый компьютер файл LMHOSTS, который будет содержать сответствия между именами компьютеров и их IP-адресами.

К каким результатам приведет предлагаемое решение?

- A. Будут достигнуты как требуемый, так и оба желательных результата.
- B. Будут достигнуты требуемый и только один из желательных результатов.
- C. Будет достигнут только требуемый результат.
- D. Предлагаемое решение не приведет к достижению требуемого результата.

Question 53

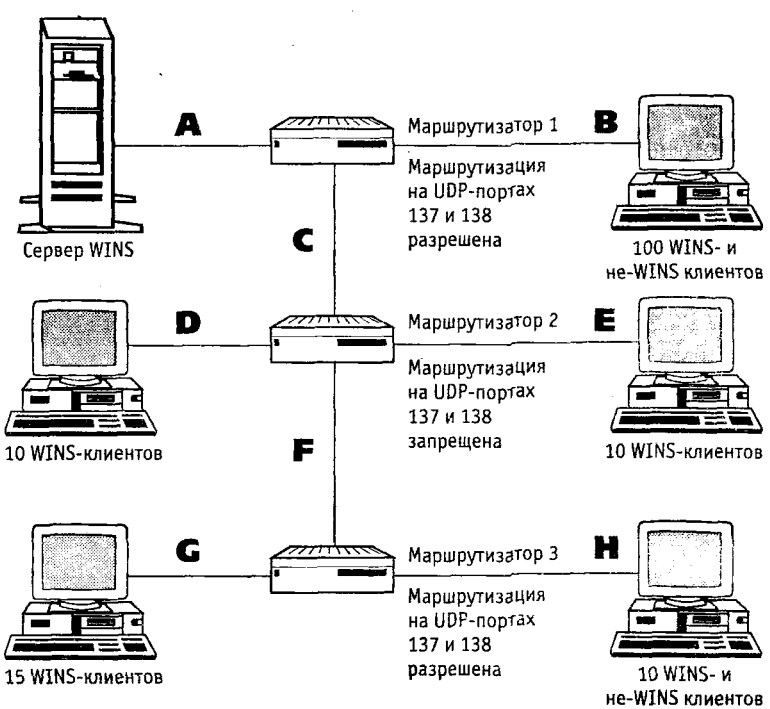
You have been asked to provide dynamic name resolution for your entire network. Your network is configured as shown in the following graphic. What is the minimum number of WINS Proxy Agents you require and where would you put them?

- A. None.
- B. Two, one for segment H and one for segment B.
- C. Seven, one for each segment, except segment A.
- D. One, for segment H.

Вопрос 53

Вам нужно обеспечить динамическое определение имен во всей сети. Топология сети показана на приведенном ниже рисунке. Каково наименьшее количество прокси-агентов WINS, которые вы должны установить и где вы должны их установить?

- A. Ноль.
- B. Два: один в сегменте H, один в сегменте B.
- C. Семь: по одному в каждом сегменте, кроме A.
- D. Один: в сегменте H.



Question 54

You have just received a new Windows NT Workstation and you seem to be having trouble mapping a drive to a Windows NT host that resides on a remote network. Your network does not currently have a WINS server providing NetBIOS name resolution. Which of the following files should you modify to enable Windows NT to correctly resolve the name of the Windows host to which you are trying to connect?

- A. HOSTS
- B. LMHOST
- C. LMHOSTS
- D. HOST

Вопрос 54

Вы только что получили новую Windows NT Workstation и не можете подключить сетевой диск, находящийся на Windows NT-узле в удаленной подсети. В вашей сети не установлена служба WINS для определения имен. Какой из следующих файлов вы должны изменить, чтобы Windows NT могла корректно *определить имя Windows-узла, с которым вы пытаетесь соединиться?*

- A. HOSTS
- B. LMHOST
- C. LMHOSTS
- D. HOST

Question 55

You have just received a new Windows NT Workstation. You are able to connect to other IP machines on your local subnetwork using the UNC name of the targeted resource, but you seem to be having trouble mapping a drive to a Windows NT host that resides on a remote network. However, no one else is having problems connecting to the remote Windows NT host. What is the first thing you should check?

- A. Your default gateway setting.
- B. The other machine's default gateway setting.
- C. The other machine's IP address.
- D. Your IP address.

Вопрос 55

Вы только что получили новую Windows NT Workstation. Вы можете соединяться с другими IP-узлами в вашей локальной подсети, используя UNC-имя ресурса, но вы не можете подключить сетевой диск, находящийся на TE-узле в удаленной подсети. Однако такие проблемы проявляются только у вас. Что вы первое проверите?

- A. Настройку шлюза по умолчанию на вашем компьютере.
- B. Настройку шлюза по умолчанию на удаленном узле.

- C. IP-адрес удаленного узла.
- D. Ваш IP-адрес.

Question 56

You manage a network of 1,500 Microsoft clients, all configured to use DHCP. You have been asked to implement WINS on your network for NetBIOS name resolution. What is the easiest way to configure these client computers to use WINS?

- A. Configure the DHCP server with option 44 WINS/NBNS only.
- B. Configure each client with the address of the WINS server manually.
- C. Configure the DHCP server with options 44 WINS/NBNS and 46 WINS/NBT.
- D. Configure the DHCP server with option 46 WINS/NBT only.

Вопрос 56

Вы управляете сетью, содержащей 1500 Microsoft-клиентов, которые настроены на использование DHCP. Вам требуется установить в вашей сети WINS для определения имен NetBIOS. Как проще всего настроить клиенты на использование WINS?

- A. Установить на сервере DHCP параметр 44 WINS/NBNS.
- B. Настроить на каждом клиенте адрес сервера WINS вручную.
- C. Установить на сервере DHCP параметры 44 WINS/NBNS и 46 WINS/NBT.
- D. Устнановить на сервере DHCP параметр 46 WINS/NBT.

Question 57

Your company has configured seven different Internet-style domains for your network. You are responsible for the Southwestern domain. Which of the following could you implement to distribute the name resolution load on your domain? (Check all correct answers.)

- A. Caching-only server.
- B. Primary name server.
- C. DNS Round-Robin.
- D. Secondary zone.

Вопрос 57

Сеть вашей компании содержит семь Интернет-доменов. Вы отвечаете за юго-западный домен. Что вы можете сделать, чтобы распределить нагрузку, вызываемую в вашем домене определением имен? (Укажите все правильные ответы.)

- A. Установить кэширующий сервер.
- B. Установить основной сервер имен.
- C. Использовать возможность Round-Robin сервера DNS.
- D. Установить дополнительную зону.

Question 58

You have established a Telnet session with a remote computer named «Sales», but the banner displays the name «Accnt». You check the IP address, and it appears to be right. What should you check next? (Check all correct answers.)

- ❑ A. The DNS name and HOSTS tables to make sure they are current and correct.
- ❑ B. The two computers on the network to make sure they don't have the same IP address.
- ❑ C. arp -g
- ❑ D. This is not possible.

Вопрос 58

Вы установили Telnet-сеанс с удаленным компьютером «Sales», но при входе в систему был выдан заголовок, сообщающий, что имя системы — «Accnt». Вы проверили IP-адрес: он правилен. Что вы должны сделать дальше? (Укажите все правильные ответы.)

- ❑ A. Проверить имя DNS и таблицы HOSTS и убедиться, что они верны и отражают текущее состояние.
- ❑ B. Проверить, нет ли в сети двух компьютеров с одним IP-адресом.
- ❑ C. arp -g
- ❑ D. Это невозможно.

Ответы на вопросы экзамена

1. C
2. B
3. A, C
4. C, D
5. A
6. C
7. D
8. B
9. A, C, D
10. D
11. B
12. A
13. C
14. D
15. B
16. D
17. A, B, C
18. C
19. A, D
20. B, C, D
21. A
22. C
23. D
24. B, C, D
25. A, B, D
26. B
27. A
28. A
29. A, B
30. A, C
31. B
32. A, B, C
33. A, D
34. A, C
35. A, B, C, D
36. B, D
37. C
38. A, C, D
39. A, C, D
40. A
41. B, C, D
42. B, C, D
43. B
44. C
45. C, D
46. A, D
47. A
48. A
49. B, D
50. D
51. A
52. D
53. D
54. C
55. A
56. C
57. A, D
58. A, B, C

Вопрос 1

Правильный ответ — C. Если какие-либо настройки были произведены вручную, настройка, передаваемая при помощи DHCP, не будет учитываться. Вне зависимости от того, прервал ли клиент аренду, при загрузке компьютера в новой подсети процесс аренды будет начат заново. Следовательно, ответ D неверен. DHCP поддерживает несколько подсетей, если маршрутизатор настроен на ретрансляцию DHCP-запросов. Следовательно, ответ A неверен. Сервер WINS не имеет никакого отношения к настройке TCP/IP. Следовательно, ответ B неверен.

Вопрос 2

Правильный ответ — B, поскольку set-запрос не требует ответа. Ответ A не подходит, поскольку на запросы с другими OID приходит ответ. При необходимости отправки предупреждения посылается сообщение-захват. Следовательно, ответ C неверен. Ответ D также неверен, поскольку он противоречит условию вопроса.

Вопрос 3

Маршрутизатор может быть шлюзом или отдельным устройством. **Следовательно, ответы A и C верны.** Маршрутизатор не является информационной службой. Следовательно, ответ B неверен. И, хотя программу для обмена электронной почтой иногда можно назвать маршрутизатором, обычно используется термин «шлюз». Следовательно, ответ D неверен.

Вопрос 4

Правильные ответы на этот вопрос — C и D. Каждый из этих параметров определяет, как ведут себя маршрутизируемые пакеты в памяти. Параметр ForwardBufferMemory определяет, какое количество данных может быть сохранено, в то время как параметр NumForwardPackets задает максимальную длину очереди пакетов. TcpWindowSize определяет размер окна TCP/IP. Следовательно, ответ B неверен. TcpBufferSize — несуществующий параметр. Следовательно, ответ A неверен.

Вопрос 5

Правильный ответ на этот вопрос — A. Количество доступных идентификаторов узлов определяется по формуле $2^n - 2$, где через n обозначено число битов, используемых для идентификатора узла. По умолча-

нию в сети класса B для идентификатора узла используется 16 бит. Таким образом, в этом случае $2^n - 2 = 65534$. Количество узлов, поддерживаемых по умолчанию сетью класса C, — 254; количество идентификаторов сетей, доступных в пространстве адресов класса C, — по умолчанию 1097152; количество идентификаторов сетей, доступных в пространстве адресов класса B, — по умолчанию 16384. Следовательно, ответы B, C и D неверны.

Вопрос 6

Правильный ответ на этот вопрос — C. По умолчанию для идентификатора сети в адресе класса C используются первые три октета. В адресах класса A используется по умолчанию один октет, и в адресах класса B — два. Хотя вы можете изменить длину идентификатора сети, используя маски подсети, спрашивалось о значении по умолчанию. Следовательно, ответы A, B и D неверны.

Вопрос 7

Лучший ответ на этот вопрос — D. Маска подсети используется TCP/IP для того, чтобы определить при загрузке идентификатор локальной сети. Затем эта информация используется, чтобы определить, находится узел-адресат в локальной или в удаленной сети. Ответ B *частично верен, но это не лучший ответ, поскольку он не содержит* достаточный объем информации. Ответ C неверен по той же самой причине. Ответ A неверен, поскольку маска подсети не помогает TCP/IP определить IP-адрес удаленного узла. Для того чтобы можно было применить маску подсети, IP-адрес должен быть известен.

Вопрос 8

Правильный ответ на этот вопрос — B. TCP/IP позволяет связываться по сети системам, работающим практически на любой программной платформе: Unix, Windows, Macintosh и др. TCP/IP не был разработан Microsoft, хотя Microsoft создала реализацию этого протокола. Следовательно, ответы A и C неверны. И хотя IAB и его подкомитет, IETF, были вовлечены в процесс стандартизации TCP/IP, они не являются разработчиками TCP/IP. Следовательно, ответ D неверен.

Вопрос 9

Правильные ответы на этот вопрос — A, C и D. Уровень приложения модели TCP/IP соответствует уровням сеанса, представления и приложения эталонной модели OSI; уровень сети модели OSI соот-

ветствует межсетевому уровню TCP/IP; уровень сетевого интерфейса TCP/IP выполняет функции физического и канального уровней модели OSI. Как вы можете видеть, функции уровня сеанса модели OSI выполняются уровнем приложения модели TCP/IP. Следовательно, ответ B неверен.

Вопрос 10

Правильный ответ на этот вопрос — D. Если компьютер не находит аппаратный адрес узла-получателя в кэше, то он отправляет в сеть широковещательный запрос. Ответ A неверен, поскольку описывается определение локального адреса — запросы на маршрутизатор отправляются только для определения удаленных адресов. Ответ B неверен, поскольку сервер ARP — несуществующее устройство. Файл HOSTS не содержит информации, касающейся аппаратных адресов. Следовательно, ответ C неверен.

Вопрос 11

Правильный ответ на этот вопрос — B. Монитор событий (Event Viewer) более чем любое другое приложение, подходит для поиска проблем при отправке или получении SNMP-пакетов.

Вопрос 12

Правильный ответ — A. Для того чтобы правильно ответить на этот вопрос, вы должны уметь переводить числа из десятичной системы счисления в двоичную. Вы можете просто запомнить последовательность 128 + 64 + 32 + 16 + 8 + 4 + 1 и выбирать из нее наибольшее число, не превышающее данное десятичное. В этом вопросе первое число, которое вы должны выбрать, — 128. Затем выберите наибольшее число, при сложении которого со 128 сумма все еще не превысит исходное число. Продолжайте эту операцию, пока вы не получите требуемое число. В этом вопросе вы должны получить 213 = 128 + 64 + 0 + 16 + 0 + 4 + 0 + 1. Теперь выкиньте знаки «+» и замените каждое ненулевое число на 1. Вы получите требуемое двоичное значение: 11010101.

Вопрос 13

Правильный ответ — C. Протокол UDP находится на уровне транспорта модели TCP/IP.

Вопрос 14

Правильный ответ на этот вопрос — D. TCP/IP использует ARP для определения MAC-адресов, соответствующих данным IP-адресам.

Следовательно, если два компьютера имеют один IP-адрес, TCP/IP не будет работать. Настройка DNS и WINS не влияет на IP-адрес компьютера. Следовательно, ответы A и B неверны. При наличии повторяющихся имен NetBIOS на экран пользователя будет выведно сообщение об этом. Следовательно, ответ C неверен.

Вопрос 15

Правильный ответ на этот вопрос — B. Это связано с тем, что NBTSTAT (утилита NetBIOS), запущенная с ключом -R, позволяет очистить кэш имен NetBIOS и перезагрузить записи из файла LMHOSTS. После этого вы можете использовать ключ - c утилиты NBTSTAT, чтобы просмотреть содержимое кэша имен NetBIOS. Наличие в кэше предзагружаемых (#PRE) записей показывает, что файл LMHOSTS находится в правильном каталоге и используется для определения имен NetBIOS.

NBTSTAT -r выведет статистику регистрации и определения имен NetBIOS, а также методы, использованные для определения имен (WINS или широковещательный запрос). Следовательно, ответ A неверен. Команда NETSTAT не выводит связанной с NetBIOS информации. Следовательно, ответы C и D неверны. Кроме того, утилита NBTSTAT не имеет документированного ключа -d. Следовательно, ответы, упоминающие этот ключ, неверны.

Вопрос 16

Правильный ответ — D. Для того чтобы определить, находится ли установленный шлюз по умолчанию в той же логической подсети, воспользуйтесь утилитой IPCONFIG (или WINIPCFG, если вы используете Windows 95). Сравните идентификатор сети шлюза с идентификатором PCMCIA сетевого адаптера. Если шлюз находится в той же подсети, они должны совпадать. Если бы проблемы были с подключением сетевого адаптера, Setup, вероятно, не смог бы обнаружить сеть вообще. Следовательно, ответы A и C неверны. Файл LMHOSTS не используется программой Setup. Следовательно, ответ B неверен.

Вопрос 17

Правильные ответы на этот вопрос — A, B и C. Ответ A верен, поскольку сервер может отвечать на запросы команды PING, даже если служба сервера не запущена. Однако служба сервера необходима для установления соединения. Ответ B верен, поскольку команды, такие как NET USE, могут заканчивать работу по тайм-ауту до того, как произойдет определение имени при помощи файла HOSTS, но команда PING будет работать. Ответ C верен, так как имя NetBIOS должно быть указано правильно как в командной строке, так и в файле HOSTS. Ответ D, очевидно, неверен.

Вопрос 18

Правильный ответ на этот вопрос — C. Windows NT позволяет вам настроить до пяти адресов при помощи интерфейса Advanced IP Addressing. Вы можете добавить более пяти адресов, но для этого необходимо редактировать реестр. Следовательно, ответы A, B и D неверны.

Вопрос 19

Верны только ответы A и D. Ответ B частично неверен: администратор может просматривать, но не изменять параметры сервера DHCP. Ответ C частично верен: после того как служба SNMP установлена, администратор может просматривать и изменять параметры в LAN Manager MIB и MIB-II MIB, но не во всех базах данных MIB.

Вопрос 20

Правильные ответы на этот вопрос — B, C и D. При определении необходимого для сети числа идентификаторов подсетей вы должны учесть каждый сегмент вашей сети, отделенный от оставшейся части сети как минимум одним маршрутизатором. Однако для замкнутой сети (без внешнего доступа), содержащей два маршрутизатора с двумя сетевыми интерфейсами каждый, потребуются три идентификатора подсети (ответ C должен быть использован в сочетании с ответом B). Ответ A неверен, поскольку, хотя каждому сетевому принтеру или узлу нужен собственный идентификатор узла, они все могут использовать один идентификатор подсети.

Вопрос 21

Правильный ответ на этот вопрос — A. Значение «.240» в третьем октете маски подсети позволяет использовать в рассматриваемой сети 14 подсетей. Такая маска подсети удовлетворяет текущим требованиям и допускает дальнейший рост сети. Кроме того, такая маска подсети позволяет использовать до 4094 идентификаторов узлов в каждой подсети, что удовлетворяет заданным требованиям. Ответы B и D неверны, так как хотя они и предоставляют достаточное число подсетей, но не позволяют установить в каждой из подсетей требуемое число узлов. Ответ C неверен, поскольку он не обеспечивает достаточное количество подсетей.

Вопрос 22

Правильный ответ на этот вопрос — C. По умолчанию компьютер, работающий под управлением Windows NT и настроенный на ис-

пользование как минимум основного сервера WINS, использует H-запрос, который является смешанной формой: это проверка кэша имен NetBIOS и затем отправка запроса на сервер WINS. Если сервер WINS не может определить имя, отправляется широковещательный запрос в локальную сеть в надежде обнаружить машину с нужным именем. Если ответ на широковещательный запрос не получен, то происходит (если выполнены соответствующие настройки) проверка файла LMHOSTS.

Вопрос 23

Правильный ответ на этот вопрос — D. Трехступенчатое открытие соединения не допускает ответа «Нет» от адресата. Если узел недоступен, он просто не отвечает. Если узел доступен, но сильно загружен другими соединениями, он использует механизм управления потоком данных, для того чтобы попросить отправителя замедлить передачу данных. Ответы A, B и C правильно описывают трехступенчатое открытие соединения.

Вопрос 24

Утилита ROUTE может использоваться для создания (при помощи параметра add) новых путей, удаления записей о шлюзах (при помощи параметра -f), а также для вывода (print) существующих путей. **Следовательно, ответы B, C и D верны.** Утилита ROUTE не может протестировать путь — для этого используется TRACERT. Следовательно, ответ A неверен.

Вопрос 25

Правильные ответы — A, B и D. MAC-адрес не может использоваться для указания узла. Следовательно, ответ C неверен.

Вопрос 26

Правильный ответ на этот вопрос — B. Windows NT может быть настроена так, что один или несколько шагов в процессе определения имени будут опущены. То, есть, на первый взгляд кажутся правильными несколько ответов. Однако только в ответе B шаги процесса определения имени приведены в правильном порядке. Запомните, что по умолчанию определение имени происходит в следующем порядке: имя локального узла > файл HOSTS > DNS > кэш имен NetBIOS > WINS > широковещательный запрос > LMHOSTS. Ответ A неверен, поскольку сразу после проверки имени локального узла TCP/IP проверяет файл HOSTS. Ответ C неверен, так как по умолчанию про-

верка имени локального узла происходит до применения других методов определения имени. Ответ D неверен, потому что по умолчанию файл HOSTS проверяется до любых попыток определения имен NetBIOS.

Вопрос 27

Правильный ответ на этот вопрос — A. По умолчанию запись сохраняется в кэше ARP в течение 10 минут.

Вопрос 28

Правильный ответ на этот вопрос — A. ARP-прокси — термин для удаленного сопоставления адреса, поскольку шлюз по умолчанию или маршрутизатор работает как прокси-агент для локального компьютера. Локальное сопоставление адреса не использует прокси. Следовательно, ответ B неверен. Кинетическое и маршрутизируемое сопоставление адреса — хорошо звучащие, но несуществующие термины. Следовательно, ответы C и D также неверны.

Вопрос 29

Правильные ответы — A и B. Агент выполняет get-запросы, за исключением случая, когда необходимо отправить предупреждения при отправке сообщения-захвата. Одним из примеров такого состояния может служить остановка работы узла. Команда GetAll не существует. Следовательно, ответ C неверен. VarBind — это структура данных. Следовательно, ответ D также неверен.

Вопрос 30

Аппаратные адреса отправителя и получателя изменяются каждый раз при прохождении пакета через шлюз. **Следовательно, правильные ответы — A и C.** IP-адреса отправителя и получателя не изменяются при прохождении маршрутизируемых пакетов через сеть. Следовательно, ответы B и D неверны.

Вопрос 31

Правильный ответ на этот вопрос — B. Хотя файл LMHOSTS является статическим текстовым файлом, используемым для определения имен, он позволяет определять имена NetBIOS, а не имена узлов. Следовательно, ответ A неверен. Ответы C и D ссылаются на распределенную систему определения имен, а не на текстовые файлы и, следовательно, неверны.

Вопрос 32

Правильные ответы на этот вопрос — A, B и C. Поскольку маршрутизаторы часто используются для передачи информации из Ethernet-сетей в сети на базе Token Ring и наоборот, разделение сети на подсети позволит взаимодействовать между собой узлам, использующим различные сетевые технологии. Разделение на подсети также позволяет преодолеть ограничения на размер сети, специфичные для сетевых технологий, таких как Ethernet. Если количество узлов превышает максимально допустимое для Ethernet-сегмента, разбиение на подсети позволит распределить эти узлы между различными физическими сегментами. Наконец, поскольку разделение на подсети физически изолирует сегменты друг от друга, широковещательный трафик снижается, что увеличивает пропускную способность сети. Ответ D неверен, поскольку при разделении сети на подсети IP-адреса должны назначаться не как попало, а по вполне определенной схеме.

Вопрос 33

Правильные ответы на этот вопрос — A и D. Одним из основных преимуществ DHCP является возможность динамической конфигурации узлов. Поскольку при использовании DHCP все настройки собраны в одном месте — на сервере DHCP, — то вероятность человеческой ошибки снижается. За централизованное определение IP-имен отвечает DNS, а не DHCP. Следовательно, ответ «b» неверен. Аналогично, неверен ответ C, поскольку, хотя адрес сервера WINS и может назначаться при помощи DHCP, собственно DHCP не имеет никакого отношения к определению имен NetBIOS.

Вопрос 34

Правильные ответы на этот вопрос — A и C. WINS доускает динамическую регистрацию имен, а также их освобождение и определение. WINS снижает широковещательный трафик, поскольку клиенты WINS используют для определения имен сервер WINS вместо широковещательных запросов. Динамическую настройку IP позволяет произвести не WINS, а DHCP. Следовательно, ответ B неверен. Хотя уменьшение широковещательного трафика в некотором смысле увеличивает мощность сети, ответ D неверен, так как реальное увеличение мощности сети требует обновления аппаратного обеспечения и не связано с WINS или определением имен.

Вопрос 35

Статическая таблица маршрутизации содержит пять полей: адрес сети, маска подсети, адрес шлюза, IP адрес сетевого интерфейса и метрику. **Следовательно, все ответы верны.**

Вопрос 36

Правильные ответы на этот вопрос — B и D. Как RSH, так и REXEC могут использоваться для запуска команды на удаленной системе. Однако REXEC требует ввода пароля. RCP просто копирует файлы, следовательно, ответ C неверен. Ответ A неверен, так как команды RPD не существует.

Вопрос 37

Правильный ответ на этот вопрос — C, так как команда NET VIEW является одной из многих команд NetBIOS, которые могут использоваться в Windows NT. Эта команда выводит список доступных ресурсов NetBIOS, таких как серверы и разделяемые диски. TFTP, TRACERT, PING, Telnet, FTP и даже Web-броузеры — это приложения, обращающиеся к файлу HOSTS для определения имен узлов (если система настроена на использование этого файла).

Вопрос 38

Правильные ответы на этот вопрос — A, C и D. Загрузочный файл содержит информацию, используемую только при запуске DNS. Все остальные указанные в ответе файлы используются для определения имен. Файл CACHE.DNS используется для того, чтобы указать вашему серверу имен корневые серверы имен InterNIC. Файл 12.122.205.IN-ADDR.ARPA.DNS используется для выполнения запросов на обратное определение имен в сети класса C 205.122.12.0. Файл LANW.COM.DNS содержит записи ресурсов для домена lanw.com.

Вопрос 39

Ответы A, C и D верны. Ответ B содержит неправильное утверждение, следовательно, он неверен.

Вопрос 40

Правильный ответ — A. NBT (NetBIOS поверх TCP/IP) является единственным протоколом, поддерживающим указанную функцию. Не запутайтесь, TCP не поддерживает идентификатор контекста.

Вопрос 41

Правильные ответы на этот вопрос — B, C и D. По умолчанию Windows NT использует имя NetBIOS в качестве имени узла для TCP/IP. При этом недопустимые символы преобразуются в дефисы. Если вы хотите изменить установленное по умолчанию имя узла, вы мо-

жете сделать это в панели управления, выбрав Network ➤ Protocols ➤ TCP/IP Properties ➤ DNS. Ответ A неверен, поскольку вы можете и не изменять установленное по умолчанию имя узла.

Вопрос 42

Правильные ответы на этот вопрос — B, C и D. Ответ A неверен, поскольку файл LMHOSTS должен находиться не в корневом каталоге, а в каталоге *systemroot*\system32\drivers\etc.

Вопрос 43

Правильный ответ на этот вопрос — B. Утилита JETPACK используется для сжатия базы данных DHCP. IPCONFIG используется для просмотра информации о настройке и для обновления или прекращения DHCP-аренды, но не позволяет администрировать базу данных. DHCP Manager может применяться для изменения базы данных, но администрирование обычно означает архивацию, сохранение и сжатие, а не управление. Приложение Сеть (Network) панели управления может использоваться для установки DHCP, но на этом его полезность заканчивается.

Вопрос 44

Ответ на этот вопрос — C. Запомните, что LPQ используется для проверки состояния очереди печати на удаленной системе. LPD — это демон, позволяющий печать с удаленной системы. Следовательно, ответ A неверен. LPR отправляет задание на печать на удаленную систему, следовательно, ответ D неверен. Утилита LPS не существует, так что ответ B неверен тоже.

Вопрос 45

Ответы C и D правильны. Для наблюдения за событиями в сети могут использоваться как монитор производительности (Performance Monitor), так и монитор сети (Network Monitor). Ответы A и B описывают несуществующие утилиты.

Вопрос 46

Правильные ответы на этот вопрос — A и D. Telnet — это программа эмуляции терминала и не позволяет выполнять передачу файлов. Следовательно, ответ C неверен. RSH позволяет выполнить команду на удаленной системе, но не позволяет передавать файлы. Следовательно, ответ B неверен.

Вопрос 47

Правильный ответ — A. Все, что вам следует знать, — это то, что хотя DNS производит определение FQDN, но серверу WINS отсылается только имя узла без имени домена. Имена доменов и корневые имена не обрабатываются сервером WINS.

Вопрос 48

Ограничение в 15 хопов введено с целью предотвращения появления бесконечных циклов. **Следовательно, ответ A правилен.** Ограничение на длину маршрута в 15 хопов позволяет использовать протокол RIP не только в маленьких, но и относительно больших сетях; многие крупные сети, такие как Интернет, используют маршруты большей длины; шестнадцатеричные коды не используются в таблице маршрутизации. Следовательно, ответы B, C и D неверны.

Вопрос 49

Правильные ответы — B и D. Ваш шлюз по умолчанию настроен правильно, поскольку другие компьютеры (не bob15) отвечают. Следовательно, ответы A и C неверны.

Вопрос 50

Правильный ответ на этот вопрос — D. Вам не требуется быть администратором домена для установки или настройки TCP/IP на обычной NT Workstation или Server. Однако в ответах A, B и C перечислены необходимые требования.

Вопрос 51

Правильный ответ на этот вопрос — A. «Надежное» взаимодействие с установлением соединения обеспечивает протокол TCP. Ответ B неверен, поскольку UDP является «ненадежным» протоколом, просто «пытающимся» доставить информацию. Ответы C и D также неверны. ARP используется для определения аппаратного адреса по соответствующему ему IP-адресу, а ICMP — для управления потоком данных. Эти два протокола не позволяют производить передачу пользовательских данных.

Вопрос 52

Ответ на этот вопрос — D. Предлагаемое решение не обеспечит достижение требуемого результата. Файл LMHOSTS не используется для определения Интернет-имен, таких как www.microsoft.com. Вам

потребуется сервер DNS или файл HOSTS. Запомните: если предлагаемое решение в подобных вопросах не обеспечивает выполнение требуемого результата, не беспокойтесь о желательных.

Вопрос 53

Правильный ответ на этот вопрос — D. Только сегмент H нуждается в прокси-агенте WINS. Если вы думаете, что A — правильный ответ, обратите внимание на Маршрутизатор 2 на иллюстрации к вопросу. Этот маршрутизатор будет отфильтровывать запросы не-WINS клиентов из сегмента H раньше, чем они достигнут сервера WINS в сегменте A. Сегмент B не нуждается в прокси, поскольку Маршрутизатор 1 не отфильтровывает запросы. Поскольку только сегменты B и H содержат не-WINS клиенты, другие сегменты не должны рассматривать в качестве кандидатов на установку в них WINS-прокси.

Вопрос 54

Правильный ответ на этот вопрос — C.

Вопрос 55

Правильный ответ на этот вопрос — A. Запомните, что шлюз по умолчанию должен находиться в одной с локальным узлом подсети и должен быть правильно указан при настройке системы. Если на системе неверно указан шлюз по умолчанию, ни один узел не сможет общаться с ней. Следовательно, ответ B неверен. Те же соображения по отношению к IP-адресу показывают, что ответ C тоже неверен. Если IP-адрес вашего компьютера неверен, ни один узел не сможет с ним взаимодействовать. Следовательно, ответ D неверен.

Вопрос 56

Лучший ответ на этот вопрос — C. В сети 1500 компьютеров — вряд ли вы хотите бегать от одного к другому и настраивать их вручную, если вы уже используете DHCP. Вы не можете добавить на сервере DHCP параметр 44 без параметра 46.

Вопрос 57

Правильные ответы на этот вопрос — A и D. DNS Round-Robin не позволяет вам распределить нагрузку, связанную с определением имен. Это метод распределения по сетевым серверам нагрузки, со-

здаваемой клиентами, при помощи подстановки альтернативных IP-адресов для одного имени узла. Основной сервер имен не поможет вам, поскольку он обрабатывает запросы на определение имен не из того домена, в котором находится. Вы можете создать дополнительную зону или установить кэширующий сервер имен.

Вопрос 58

Правильные ответы на этот вопрос — A, B и C. По умолчанию ARP верит первому полученному ответу, поэтому, если ответ самозванца придет раньше, чем ответ нужного узла, возникнут проблемы. Если вы убедились, что имя узла указано верно и проверили файл HOSTS, используйте команду `arp -g` для вывода записей ARP-кэша. Если вы знаете Ethernet-адрес удаленного компьютера, убедитесь, что он соответствует адресу, указанному в кэше. Если адреса отличаются, используйте команду `arp -d` для удаления записи из кэша и форсируйте появление в кэше новой записи, использовав команду PING. Опять проверьте кэш, сравнив адрес с тем, что было в первый раз. Если в сети есть самозванец, вы рано или поздно обнаружите несоответствие. Далее используйте Netwrok Monitor для поиска системы, вызывающей проблемы.

Глоссарий

#DOM tag (тег #DOM) — в файле LMHOSTS тег #DOM используется для обозначения записи, соответствующей контроллеру домена.

#PRE tag (тег #PRE) — в файле LMHOSTS тег #PRE используется для указания того, что запись должна быть загружена в кэш имен NetBIOS.

administrator (администратор) — работник, отвечающий за поддержку, управление и безопасность сети. Также (с прописной буквы — Administrator) — пользователь Windows NT, имеющий полный контроль над всей системой.

agents (агенты) — в TCP/IP программное обеспечение на SNMP-управляемом устройстве, выполняющее **get-** и **set-** запросы и отправляющее сообщения-захваты.

alphanumeric host names (буквенно-цифровые имена узлов) — имена узлов, состоящие из букв и цифр.

ANDing (операция логического «И») — процесс, используемый TCP/IP для определения расположения узла: в локальной или удаленной подсети.

API, Application Programming Interface (программный интерфейс) — формат сообщений и запросов, позволяющий программистам использовать функции определенного приложения.

Application Layer (прикладной уровень, уровень приложения) — седьмой уровень модели OSI. Этот уровень предоставляет приложениям возможность работы с сетью. Пользовательские приложения и системные службы обычно получают доступ к сети, взаимодействуя с процессом, работающим на уровне приложения.

architecture (архитектура) — термин, используемый для обозначения строения сети и того, как сетевые компоненты связаны друг с другом.

ARP, Address Resolution Protocol (протокол сопоставления адреса) — протокол межсетевого уровня, отвечающий за определение аппаратного адреса (также называемого MAC-адресом), соответствующего данному IP-адресу.

ARP cache (кэш ARP) — область хранения информации о соответствиях между аппаратными и IP-адресами узлов сети.

ARPANet, Advanced Research Project Agency Network (сеть Агентства по перспективным научным разработкам) — сеть, разработанная ARPA и в течение многих лет служившая основой Интернета.

ASCII, American Standard Code for Information Interchange (Американский стандартный код для обмена информацией) — способ ко-

дировки, позволяющий записывать буквы, числа и символы в числовой форме.

ASN, Abstract Syntax Notation (абстрактная синтаксическая запись) — точно определенный язык для описания MIB. Вы можете думать об ASN как о компилируемом языке наподобие COBOL, FORTRAN или C.

assessment exam (репетиционный экзамен) — как и сертификационный экзамен, этот экзамен предоставляет вам возможность ответить на набор вопросов. На этом экзамене также используется то же, что и на сертификационном экзамене, программное обеспечение.

ATEC, Authorized Technical Education Center (Авторизованный центр технического обучения) — место, где вы можете пройти курсы в соответствии с Официальным учебным планом Microsoft под руководством преподавателей, получивших статус Microsoft Certified Trainers.

ATM, Asynchronous Transfer Mode (асинхронный режим передачи) — высокоскоростная технология передачи данных, поддерживающая передачу данных, а также звука и изображения в реальном времени.

BDC, Backup Domain Controller (резервный контроллер домена) — резервный сервер, обеспечивающий целостность и доступность базы данных SAM. BDC не могут производить изменения в базе данных, но они могут использовать базу данных для аутентификации пользователей.

binary (бинарный, двоичный) — способ представления данных в компьютере. Все данные кодируются при помощи битов; каждый бит может находиться только в одном из двух состояний (1 или 0).

BIND, Berkeley Internet Name Domain (домен имен Интернета Berkeley) — спецификация DNS, разработанная в университете Беркли в Калифорнии.

b-node broadcast (широковещательный B-запрос) — широковещательный запрос, инициируемый локальным узлом в локальной сети в том случае, если имя NetBIOS не может быть определено при помощи сервера WINS.

boot disk (загрузочный диск) — жесткий или гибкий диск, на котором находятся загрузочные файлы. Загрузочные файлы необходимы для запуска операционной системы.

boot file (загрузочный файл) — файл, содержащий необходимую для определения имен вне официальных доменов информацию.

BOOTP, Bootstrap Protocol (загрузочный протокол) — протокол, обеспечивающий запуск и автоматическую настройку TCP/IP на бездисковых клиентах. На BOOTP основан протокол DHCP.

bottlenecks (узкие места, буквально — «бутылочные горлышки») — эффект, вызываемый попыткой передачи слишком большого количества информации через сеть с неадекватной пропускной способностью и заключающийся в значительном снижении быстродействия системы.

browsing (просмотр) — возможность обнаружения и использования сетевых ресурсов NetBIOS без необходимости заранее знать об их наличии.

cache (кэш) — специальная область высокоскоростной памяти, используемой для хранения данных, доступ к которым недавно был произведен или будет произведен в ближайшее время.

cache-only name server (кэширующий сервер имен) — сервер имен, кэширующий результаты запросов на определение имен.

CIDR, Classless Inter-Domain Routing (безклассовая междудоменная маршрутизация) — метод, используемый для увеличения количества подсетей, соответствующих данной длине адреса. CIDR определяет идентификатор сети и идентификатор узла в IP-адресе в соответствии с используемым числом битов.

classes (классы) — метод сетевой адресации, позволяющий легко отделить идентификатор сети от идентификатора узла, поскольку граница между ними располагается на границе между октетами.

CNAMEs, canonical name records (записи CNAME) — записи, позволяющие задать псевдонимы для имен узлов. Эти записи позволяют вам ассоциировать более одного имени узла с IP-адресом.

community names (имена сообществ) — имена, используемые SNMP для определения доступа к программным агентам.

computername (*имя компьютера*) — *имя компьютера в локальной* сети, уникальное для конкретной рабочей станции или сервера.

Control Panel (Панель управления) — приложение Windows, позволяющее изменять настройки системы, такие как используемые шрифты, цвета, настройки SCSI-оборудования, настройки принтеров и др.

CPU, Central Processing Unit (процессор) — *мозг вашего компьютера.*

cut score (проходной балл) — наименьшее достаточное количество баллов для сдачи сертификационного экзамена Microsoft.

daemon (демон) — unix-программа, предоставляющая службы, такие как FTP или TFTP, клиентам[1].

Data Link Layer (канальный уровень) — второй уровень модели OSI. Этот уровень состоит из двух подуровней: Logical Link Control (LLC) —

[1] Строго говоря, в Unix демоном называется процесс, не имеющий связанного с ним управляющего терминала. — *Примеч. перев.*

подуровня управления логической связью и Media Access Control (MAC) — подуровня управления доступом к устройствам. Эти два подуровня отвечают за перемещение пакетов в сеть и получение их из сети.

database (база данных) — информация, упорядоченная и сохраняемая так, чтобы обеспечить к ней простой и быстрый доступ.

datagram (датаграмма) — еще один термин для пакета данных; обычно применяется при обсуждении служб, не устанавливающих соединение, таких как UDP.

default (по умолчанию) — настройки, используемые в том случае, если они не будут явно изменены пользователем.

DHCP, Dynamic Host Configuration Protocol (протокол динамической конфигурации узла) — служба, позволяющая динамически выделять узлам IP-адреса из указанного диапазона.

DHCP Relay (DHCP-ретрансляция) — ретрансляция маршрутизатором широковещательных DHCP (BOOTP) пакетов из одной подсети в другую.

DNS, Domain Name System (доменная система имен) — распределенная база данных соответствий между именами узлов и доменов с одной и IP-адресами с другой стороны, позволяющая предоставить службы определения имен клиентским приложениям TCP/IP.

domain (домен) — группа компьютеров и периферийных устройств, использующих общую базу данных безопасности.

Domain Master Browser (мастер-сервер просмотра домена) — в сетях Windows NT — сервер просмотра, компилирующий список просмотра и распространяющий его по подсетям.

domain name (имя домена) — имя группы рабочих станций и серверов в одной сети.

Domain Name Space (доменное пространство имен) — структура и данные, образующие распределенную базу данных доменной системы имен, используемой в Интернете.

DOS, Disk Operating System (дисковая операционная система) — наиболее популярная на всех PC операционная система. Она предоставляет управляемое из командной строки окружение для компьютеров, основанных на платформе x86.

dotted-decimal notation (точечно-десятичная запись) — способ представления IP-адреса. IP-адрес записывается в виде четырех десятичных чисел, называемых *октетами*, разделенных точками.

DWORD entries (тип DWORD) — один из типов данных реестра.

dynamic routing (динамическая маршрутизация) — способ маршрутизации, который автоматически подстраивается под изменения в трафике или топологии сети.

echo packets (эхо-пакеты) — пакеты, используемые ICMP, при ответе на PING-запросы.

encryption (шифрование) — метод кодирования данных, при котором получатель должен иметь специальный код для декодирования.

Ethernet — наиболее часто используемый тип локальной сети; был разработан фирмой Xerox.

Exam Preparation Guides (руководства по подготовке к экзамену) — руководства, содержащие информацию по темам сертификационных экзаменов Microsoft и призванные помочь в подготовке к экзамену.

fault tolerance (отказоустойчивость) — способность системы продолжать работу даже при возникновении системных ошибок.

firewall (брандмауэр) — барьер (программный и/или аппаратный) между двумя сетями, позволяющий устанавливать только авторизованные межсетевые соединения.

FQDN, fully qualified domain name (полное доменное имя) — полное имя узла в Интернете.

FTP, File Transfer Protocol (протокол передачи файлов) — протокол, который позволяет передавать файлы между локальной системой и удаленным FTP-сервером в TCP-IP сети, например в Интернете.

gateway (шлюз) — специальный компьютер или маршрутизатор, имеющий более полный список окружающих подсетей, чем обычный узел.

gateway address (адрес шлюза) — столбец данных в таблице маршрутизации, указывающий IP-адреса точки входа для каждой подсети.

Gopher service (служба Gopher) — служба Интернета, предоставляющая чисто текстовую информацию. Эта служба лучше всего подходит для передачи больших документов, не содержащих форматирования или иллюстраций.

GUI, graphical user interface (графический интерфейс пользователя) — интерфейс, использующий графику, окна и трекбол или мышь в качестве средств взаимодействия с пользователем.

hard drive (жесткий диск) — постоянная область хранения данных.

hardware (аппаратное обеспечение) — физические компоненты компьютерной системы.

hexadecimal value (шестнадцатеричное значение) — число в шестнадцатеричной системе счисления. Используется для краткой записи больших двоичных чисел.

host (узел) — компьютерная система или другое устройство, подключенное к сети.

host ID (идентификатор узла) — IP-адрес, идентифицирующий определенный узел в сети.

host name (имя узла) — имя или псевдоним, присвоенные TCP/IP-узлу, которые проще запомнить, чем числовой адрес.

host name resolution (определение имени узла) — механизм, используемый для преобразования имен узлов или имен доменов в IP-адреса.

HOSTS file (файл HOSTS) — файл, содержащий список имен узлов и соответствующих им IP-адресов.

HTML, Hypertext Markup Language (гипертекстовый язык разметки) — основанный на SGML язык разметки документов, применяемый для создания Web-страниц.

HTTP, Hypertext Transfer Protocol (гипертекстовый протокол передачи файлов) — протокол, используемый для передачи HTML-документов через Интернет или интрасети, а также для реакции на события (такие, как щелчки пользователя на гипертекстовых ссылках).

HWA, hardware address (аппаратный адрес) — низкоуровневый адрес, связанный с аппаратным устройством в сети. HWA связан с номером на сетевой карте.

IAB, Internet Architecture Board (Совет по архитектуре Интернета) — организация, отвечающая за поддержку RFC.

ICMP, Internet Control Message Protocol (протокол управляющих сообщений Интернета) — протокол, используемый IP и другими высокоуровневыми протоколами для отправки и получения сообщений о статусе передаваемой информации.

IGMP, Internet Group Management Protocol (протокол управления группами Интернета) — протокол, используемый для отправки широковещательных IP-сообщений. Используется для отправки сообщения определенной группе получателей.

IIS, Internet Information Server (информационный сервер Интернета) — Web-сервер, разработанный Microsoft и входящий в состав Windows NT Server.

INETSTP — имя программы установки IIS. Эта программа находится в каталоге *processor*\INETSRV.

input/output system (система ввода/вывода) — система, отвечающая за получение данных с устройства ввода (такого, как клавиатура), и вывод их на устройство вывода.

interface (интерфейс) — столбец данных в таблице маршрутизации, в котором указаны аппаратные адреса сетевых интерфейсов.

Internet (Интернет) — сеть, состоящая из множество публично доступных TCP/IP-сетей по всему миру.

Internet layer (межсетевой уровень) — уровень модели TCP/IP, грубо соответствующий уровню сети модели OSI. На этом уровне расположен протокол IP.

InterNIC, Internet Network Information Center (Сетевой информационный центр Интернета) — организация, отвечающая за выделение и назначение IP-адресов тем, кто хочет соединить свою сеть с Интернетом.

intranet (интрасеть) — внутренняя частная сеть, использующая те же протоколы и стандарты, что и Интернет.

IP address (IP-адрес) — четыре десятичных числа, разделенных точками, являющихся числовым адресом компьютера в TCP/IP-сети, такой как Интернет.

IPCONFIG — текстовая утилита Windows NT, позволяющая получить информацию о настройках TCP/IP без использования приложения Network панели управления.

IPX/SPX, Internetwork Packet eXchange/Sequenced Packet eXchange (*межсетевой обмен пакетами/последовательный обмен пакетами*) — протокол Novell NetWare, реализованный Microsoft в Windows NT под именем NWLink. NWLink полностью совместим с версией Novell и во многих случаях лучше оригинала.

ISM, Internet Service Manager (диспетчер служб Интернета) — утилита для настройки служб IIS и наблюдения за их работой.

ISO, International Standards Organization (международная организация по стандартам) — международная организация, сформированная для развития стандартов на сетевые протоколы и создавшая модель OSI (модель взаимодействия открытых систем).

ISP, Internet Service Provider (провайдер Интернета) — организация, предоставляющая доступ в Интернет и родственные услуги за плату.

iterative name query (итеративный запрос на определение имени) — запрос, отправляемый одним сервером имен другому и используемый при частичном определении имен.

JETPACK — утилита, используемая для сжатия баз данных Windows NT, включая базы данных WINS и DHCP.

LAN, local area network (локальная сеть) — сеть, расположенная в небольшом здании или географической области и состоящая из серверов, рабочих станций, периферийных устройств, сетевой операционной системы и коммуникационных связей.

leased line (выделенная линия) — коммуникационная линия, арендованная у провайдера коммуникационных услуг — обычно у провайдера Интернета или телефонной компании.

LFN, long file names (длинные имена файлов) — имена файлов, содержащие до 256 символов.

LLC, Logical Link Control sublayer (подуровень управления логической связью) — один из подуровней канального уровня модели OSI, отвечающего за помещение пакетов в сеть и получение пакетов из сети.

LMHOSTS — предшественник WINS. LMHOSTS является статическим списком соответствий между именами NetBIOS и IP-адресами.

LMHOSTS file (файл LMHOSTS) — статический текстовый файл, хранящийся на локальном узле и используемый для определения IP-адресов, соответствующих именам NetBIOS.

logoff (выход из системы) — процесс завершения работы пользователя с компьютерной системой.

logon (вход в систему) — процесс регистрации пользователя в компьютерной системе перед началом работы.

loopback address (локальный адрес) — IP-адрес, первый октет которого равен 127. Такой адрес не может использоваться в качестве адреса узла в сети. Он используется для тестирования работы семейства протоколов TCP/IP внутри одного компьютера, без отправки данных в сеть.

LPD, Line Printer Daemon (демон печати) — служба печати TCP/IP.

LPQ, Line Printer Queue (очередь печати) — утилита, используемая для вывода состояния удаленной очереди печати.

LPR, Line Printer Remote client (клиент печати) — программа для постановки заданий в удаленную очередь печати.

management console (управляющая консоль) — любой компьютер, на котором запущен графический интерфейс диспетчера SNMP.

managers — *см.* management console.

master name server (мастер-сервер имен) — любой сервер имен, передающий файл зоны дополнительному серверу имен.

MCP, Microsoft Certified Professional (сертифицированный Microsoft профессионал) — индивидуум, сдавший как минимум один сертификационный экзамен Microsoft и имеющий статус Microsoft Cerified Trainer, или Microsoft Certified Solution Developer, или Microsoft Certified Systems Engineer или Microsoft Certified Product Specialist.

MCPS, Microsoft Certified Product Specialist (сертифицированный Microsoft специалист по программному продукту) — индивидуум, сдавший как минимум один из сертификационных экзаменов Microsoft по операционным системам.

MCSD, Microsoft Certified Solution Developer (сертифицированный Microsoft разработчик решений) — индивидуум, признанный способным разрабатывать бизнес-решения на базе инструментов разработки, технологий и платформ Microsoft.

MCSE, Microsoft Certified Systems Engineer (сертифицированный Microsoft системный инженер) — индивидуум, являющий экспертом по Windows NT и интегрированному семейству продуктов Microsoft BackOffice. MCSE способен планировать, реализовывать и поддерживать информационные системы на базе этих программных продуктов.

MCT, Microsoft Certified Trainer (сертифицированный Microsoft преподаватель) — индивидуум, признанный Microsoft способным вести учебные курсы, авторизованные Microsoft.

MAC, Media Access Control sublayer (подуровень управления доступом к устройствам) — один из подуровней канального уровня модели OSI, отвечающего за отправку пакетов в сеть и получение их из сети.

metric (метрика) — столбец данных в таблице маршрутизации, в котором указано количество ретрансляций для достижения каждой подсети.

MIB, Message Information Base (информационная база сообщений) — файл данных, содержащий значения объектов и описания управляемых объектов.

Microsoft certification exam (сертификационный экзамен Microsoft) — экзамен, проводимый Microsoft для проверки уровня знаний по данному программному продукту, технологии или теме.

Microsoft official curriculum (официальный учебный план Microsoft) — образовательные курсы Microsoft, поддерживающие программы сертификационных экзаменов.

Microsoft Roadmap to Education and Certification (путеводитель Microsoft по образованию и сертификации) — приложение, основанное на Microsoft Windows, помогающее вам решить, каковы ваши сертификационные цели и каков наилучший способ их достигнуть.

Microsoft Solution Provider (провайдер решений Microsoft) — организация, не обязательно непосредственно связанная с Microsoft, предлагающая услуги по интеграции, консультационные услуги, техническую поддержку и прочие услуги, связанные с продуктами Microsoft.

Microsoft Technical Information Network (TechNet) (сеть технической информации Microsoft) — ежемесячно выходящий CD, содержащий полезную информацию о продуктах Microsoft. TechNet — важнейший источник технической информации для тех, кто занимается поддержкой и/или обучением конечных пользователей, созданием автоматизированных решений или администрированием сетей и/или баз данных.

MPR, Multiprotocol Router (многопротокольный маршрутизатор) — служба, позволяющая динамически маршрутизировать TCP/IP-трафик между различными подсетями, а также поддерживать IPX-маршрутизацию и агентов ретрансляции DHCP.

MSDN, Microsoft Developer Network (сеть Microsoft разработчика) — официальный источник пакетов разработки программного обеспечения (Software Development Kit, SDK), пакетов драйверов устройств (Device Driver Kit, DDK), операционных систем и информации, связанной с разработкой приложений для Microsoft Windows и Windows NT.

multihomed computer (система с несколькими сетевыми интерфейсами) — компьютер, в котором установлено две или более сетевых карт.

name registration (регистрация имени) — процесс, при помощи которого компьютер проверяет, что используемое им имя NetBIOS уникально.

NBTSTAT — утилита, позволяющая просмотреть статистическую информацию, связанную с NetBIOS поверх TCP/IP (NBT).

NDIS, Network Device Interface Specification (Спецификация интерфейса сетевого устройства) — программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов и соответствующими драйверами сетевых интерфейсов. NDIS позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта. Версия TCP/IP, разработанная Microsoft, имеет расширенную поддержку этого интерфейса.

negative name (отказ в регистрации) — ответ, отправляемый на запрос регистрации имени в том случае, если данное имя уже используется.

NetBIOS — протокол, исходно разработанный компанией IBM в 1980-х годах. Этот протокол обеспечивает механизм для работы некоторых основных функций NT, таких как просмотр и взаимодействие между процессами на сетевых серверах.

NetBIOS name (имя NetBIOS) — имя, используемое приложениями и процессами NetBIOS для установления соединения с другими приложениями NetBIOS на удаленных узлах.

NetBIOS name cache (кэш имен NetBIOS) — область хранения данных, содержащая соответствия между именами NetBIOS и IP-адресами. Кэш имен NetBIOS не содержит имен узлов.

netmask (маска подсети) — столбец данных в таблице маршрутизации, содержащий маску для каждой подсети.

NETSTAT — утилита, выводящая статистическую информацию для протоколов (TCP, IP, ICMP или UDP) и информацию об IP-соединениях.

network ID (идентификатор сети) — подсеть (или сегмент), в которой физически расположен узел.

network address (адрес сети) — столбец данных в таблице маршрутизации, задающий адреса всех известных подсетей, включая локальный адрес 0.0.0.0 и широковещательный адрес 255.255.255.255.

Network layer (уровень сети) — третий уровень модели OSI. Этот уровень отвечает за маршрутизацию пакетов между различными сетями.

Network Neighbourhood (сетевое окружение) — при помощи программ Explorer или My Computer вы сможете найти в этой папке другие компьютеры вашей сети.

NSLOOKUP — утилита для поиска неисправностей DNS.

NWLink — реализация протоколов IPX/SPX фирмы Microsoft.

OS, operating system (операционная система) — программа, управляющая поведением компьютерной системы.

OSI, Open Systems Interconnection Reference Model (справочная модель взаимодействия открытых систем) — идеальная модель, разработанная ISO, определяющая этапы, на которые разбивается сетевое взаимодействие. Большинство современных протоколов основано на этой модели.

OSPF, Open Shortest Path First (открой кратчайший путь первым) — протокол TCP/IP-маршрутизации. Этот протокол является протоколом второго поколения.

PDC, Primary Domain Controller (основной контроллер домен) — сервер, на котором хранится и поддерживается база данных SAM в NT-сети.

Performance Monitor (монитор производительности) — графическая утилита, позволяющая наблюдать за производительностью системы, а также выдавать предупреждения при превышении некоторыми параметрами заранее определенных порогов.

peripheral device (периферийное устройство) — аппаратное устройство, подключенное к компьютеру.

Physical layer (физический уровень) — первый уровень модели OSI. На этом уровне определяются спецификации на аппаратное обеспечение, соединители, длину кабелей и сигналы.

PING — команда TCP/IP, используемая для проверки существования и доступности по сети удаленных узлов.

PPP, Point-To-Point Protocol (протокол «точка-точка») — стандартный протокол, используемый для установления поддерживающего сетевые протоколы соединения по телефонной линии с использованием модема.

PPTP, Point-To-Point Tunneling Protocol (туннельный протокол «точка-точка») — протокол, позволяющий «туннелирование» IPX, NetBEUI или TCP/IP в PPP-пакетах с целью установления безопасного соединения между клиентом и сервером через Интернет.

Presentation layer (уровень представления) — шестой уровень модели OSI. Этот уровень отвечает за то, чтобы данные, передаваемые уров-

ню приложения, были преобразованы в формат, требуемый процессами уровня приложения.

primary name server (основной сервер имен) — сервер имен, на котором создается и поддерживается зона. Основной сервер имен также выполняет запросы на определение имен от клиентов.

protocol (протокол) — набор правил, определяющих, как информация передается через сеть.

Proxy ARP (ARP-прокси) — процесс, при котором маршрутизатор помогает сопоставлению адреса, ретранслируя запросы на получение аппаратного адреса узла-адресата.

PTR, Pointer record (запись PTR) — тип записи ресурсов DNS, используемой для поиска в обратной зоне имени узла, соответствующего данному IP-адресу.

pull partner (тянущий партнер) — сервер WINS, настроенный на получение от партнера изменений в базе данных через фиксированные промежутки времени.

push partner (тянущий партнер) — сервер WINS, настроенный на отправку партнеру изменений в своей базе данных.

RARP, Reverse Address Resolution Protocol (протокол обратного сопоставления адреса) — протокол, обратный ARP: он позволяет определить IP-адрес системы по ее аппаратному адресу. Используется для назначения IP-адресов бездисковым рабочим станциям.

RAS, Remote Access Service (служба удаленного доступа) — служба Windows NT, позволяющая клиентам подключаться к сети с использованием телекоммуникационных линий. RAS-соединение отличается от непосредственного подключения к сети только более низкой скоростью.

RCP, Remote Copy (удаленное копирование) — утилита, позволяющая копировать файлы с одного TCP/IP-узла на другой без аутентификации пользователя.

recursive name query (рекурсивный запрос на определение имени) — запрос, отправляемый резольвером. Клиент (резольвер) запрашивает абсолютное определение имени, что означает, что он хочет получить полный IP-адрес.

Registry Editor (редактор реестра) — утилита, позволяющая просматривать и изменять реестр.

relay agent (агент ретрансляции) — утилита, ретранслирующая DHCP-сообщения между сервером DHCP и клиентами DHCP, находящимися не в подсети сервера.

remote host (удаленный узел) — IP-узел в удаленной подсети.

reserved client (зарезервированный клиент) — клиент, который всегда получает один и тот же IP-адрес при обращении к серверу DHCP.

resolver (резольвер) — компьютер-клиент, отправляющий запрос на определение имени.

Resource Kit — дополнительная документация и утилиты, распространяемые Microsoft с целью обеспечить пользователей информацией и инструкциями по правильной работе и изменению программных продуктов Microsoft.

REXEC — утилита, выполняющая команду на удаленной системе (на которой должна быть запущена служба REXEC).

RFC, Request For Comments (запрос комментариев) — свободно доступные, опубликованные стандарты TCP/IP.

RIP, Routing Information Protocol (маршрутизирующий информационный протокол) — протокол, позволяющий маршрутизаторам в сети обмениваться таблицами маршрутизации.

router (маршрутизатор) — устройство или программное обеспечение, позволяющее взаимодействие и коммуникации между сетями.

routing table (таблица маршрутизации) — база данных, описывающая соответствия между IP-адресами сетевых сегментов и IP-адресами интерфейсов маршрутизатора.

RSH, Remote Shell (удаленный интерпретатор командной строки) — утилита, позволяющая пользователям выполнять команды на удаленной системе не регистрируясь на ней.

scope (контекст) — диапазон IP-адресов, которые сервер DHCP присваивает клиентам.

Scope ID (идентификатор контекста) — идентификатор, присоединяемый к имени NetBIOS при сетевых взаимодействиях. Только компьютеры, имеющие одинаковый контекст NetBIOS, смогут взаимодействовать друг с другом.

secondary name server (дополнительный сервер имен) — сервер имен, поддерживающий копию файла зоны, полученную с основного сервера имен или с другого дополнительного сервера имен.

Session layer (уровень сеанса) — пятый уровень модели OSI. Этот уровень отвечает за установление, поддержку и завершение соединений между приложениями или процессами, работающими на различных узлах сети.

set — запрос на выполнение агентом действия; ответ не обязателен.

sliding window (скользящее окно) — термин, используемый для описания изменяющегося размера буферов приема и передачи TCP, а также механизма управления этими буферами.

SNMP, Simple Network Management Protocol (простой протокол управления сетью) — протокол, используемый для наблюдения за удаленными TCP/IP-узлами.

sockets (сокеты) — технология адресации, используемая службами и приложениями, которые нуждаются в установлении соединения с другими узлами.

static routing (статическая маршрутизация) — маршрутизация, основанная на статических изменяемых вручную таблицах маршрутизации.

subnet (подсеть) — часть или сегмент сети.

subnet mask (маска подсети) — 32-разрядное двоичное число, указывающее, сколько бит в адресе используется для идентификатора сети.

supernetting — функция CIDR; процесс, используемый для объединения нескольких адресов класса C в одну подсеть при помощи изменения количества используемых бит в маске подсети.

System Policy Editor — административная утилита, используемая для создания и модификации системной политики безопасности для компьютеров, групп и пользователей.

TCP/IP — семейство протоколов, наиболее широко используемое в современных сетях. TCP/IP предоставляет наиболее гибкий транспортный протокол и может использоваться в глобальных сетях.

TCP/IP Model (модель TCP/IP) — четыре уровня семейства протоколов TCP/IP: уровень сетевого интерфейса, межсетевой уровень, уровень транспорта и уровень приложения.

Telnet — очень полезная программа эмуляции удаленного терминала, использующая свой собственный транспортный протокол (определенный в RFC 854).

topology (топология) — конфигурация сети. Две наиболее распространенных топологии сетей — звезда и общая шина.

TRACERT — диагностическая утилита TCP/IP, определяющая путь к указанному узлу при помощи отправки эхо-пакетов ICMP с увеличивающимся значением времени жизни (TTL).

Transport layer (уровень транспорта) — четвертый уровень модели OSI. Этот уровень отвечает за передачу сообщений от узла-отправителя узлу-адресату.

traps (захваты) — предупреждения, отправляемые агентом SNMP при превышении указанными величинами заданных значений.

TTL, time to live (время жизни) — время, которое пакет может находиться в сети.

UDP, User Datagram Protocol (пользовательский протокол датаграмм) — транспортный протокол TCP/IP, передающий данные без установления соединения.

UNC, Universal Naming Convention (универсальное соглашение об именовании) — стандартизированный метод именования сетевых ресурсов в форме \\имя_сервера\имя_ресурса.

Unix — интерактивная операционная система с разделением времени, разработанная в 1969 году хакером для того, чтобы играть в игры. Эта система развилась в одну из наиболее широко применяемых в мире операционных систем и сыграла важнейшую роль в образовании Интернета.

user name (имя пользователя) — имя учетной записи пользователя. Имя пользователя — одна из двух необходимых при процессе входа в NT-систему строк. Однако NT распознает учетные записи не по их именам, а по соответствующим SID.

WAN, wide area network (глобальная сеть) — сеть, состоящая из географически удаленных друг от друга сегментов. Часто при определении глобальной сети исходят из расстояния в одну или две мили. Однако Microsoft считает, что глобальной сетью является любая сеть, использующая RAS.

Windows NT Workstation — операционная система Microsoft — клиентская версия NT. Она отличается от NT Server отсутствием возможности запуска многих служб и предоставления ресурсов в сети.

WINS, Windows Internet Name Service (служба определения имен Интернета) — сетевая служба Windows, используемая для определения IP-адресов, соответствующих именам NetBIOS.

WINS Proxy Agent (прокси-агент WINS) — компьютер, работающий под управлением Windows NT и настроенный на ретрансляцию широковещательных запросов на определение имени от не-WINS клиентов серверу WINS.

WinSock, Windows Sockets (сокеты Windows) — сетевой программный интерфейс, разработанный для поддержки соединений между различными TCP/IP-приложениями и семействами протоколов.

World Wide Web (Всемирная паутина) — распределенная информационная система, расположенная в TCP/IP-сетях. WWW поддерживает текст, графику и мультимедиа. IIS, входящий в состав NT, является Web-сервером, способным предоставлять клиентам Web-документы.

zone (зона) — Часть иерархии доменного пространства имен, используемая для управления службой DNS.

Сертификационный ЭКЗАМЕН ЭКСТЕРНОМ

Эта книга даст вам уверенность в себе, необходимую для успешной сертификации

Здесь содержится вся необходимая и достаточная информация, которая действительно нужна для сдачи экзамена.

Вы ищете по-настоящему эффективный и надежный путь изучения экзаменационного курса **Microsoft TCP/IP**? Тогда приобретите эту книгу — и вы уже на пути к успеху!

Отличительные особенности серии

- Подробные сжатые конспекты
- Все, что нужно, и ничего лишнего
- Проверенные методики обучения
- Отдельный раздел, посвященный стратегии и тактике сдачи экзамена
- Бонус: отрывная шпаргалка (в конце книги)
- Пример экзамена: проверьте свои знания

Серия **«Сертификационный экзамен — экстерном»** разработана ведущими американскими экспертами, преподавателями и психологами. **Эд Титтел**, создатель серии, является президентом LANWrights Inc., крупнейшего центра обучения и сертификации. **Курт Хадсон** — опытный преподаватель подготовительных курсов. **Дж. М. Стюарт** — системный инженер, крупнейший специалист по продуктам Microsoft.

Уровень пользователя:

опытный

профессионал

ISBN 5-8046-0025-7

Certification Insider Press

ПИТЕР
WWW.PITER-PRESS.RU

Информация, которую вы найдете в книге:

- Установка TCP/IP в Windows NT
- Определение класса сети, необходимой предприятию
- Маршрутизация TCP/IP
- Статическая и динамическая маршрутизация
- Локальная и удаленная адресация
- Файлы HOSTS: конфигурация и возможные проблемы
- Различные методы определения имен в NetBIOS
- Работа DHCP
- Оптимизация скорости TCP/IP
- Техника подготовки к экзамену

Информация об экзамене

Название:
Microsoft TCP/IP on Microsoft Windows NT 4

Количество вопросов:
58

Необходимое количество баллов:
750

Время:
90 минут

Сложность экзамена:

1	2	3	4	5

Простой — Сложный