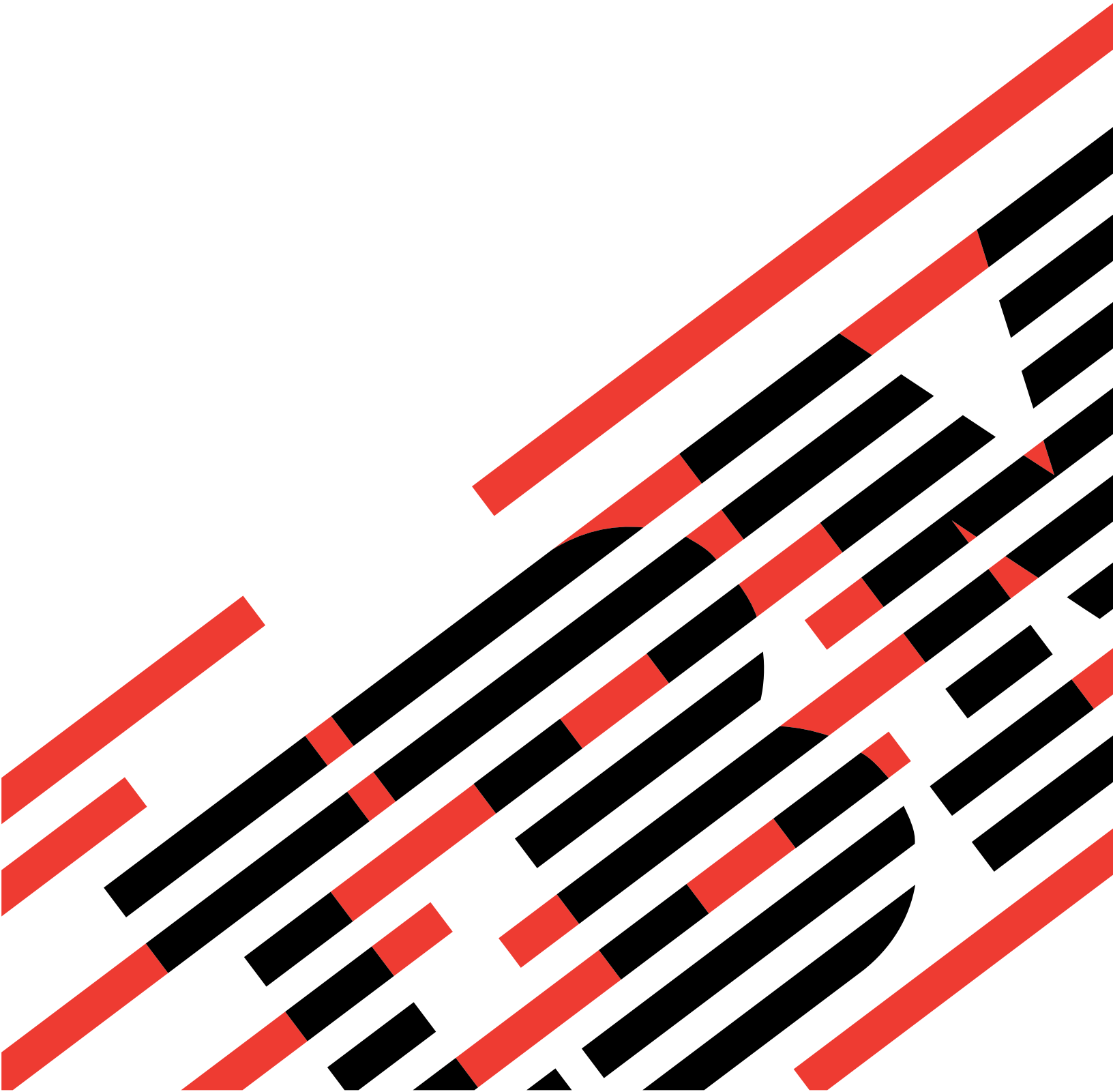
IBM

eserver

iSeries

DNS

Версия 5, выпуск 3



IBM

@server

iSeries

DNS

Версия 5, выпуск 3

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 39.

Пятый выпуск (август 2005 года)

Это издание относится к версии 5, выпуску 3, модификации 0 IBM Operating System/400 (код продукта–5722-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

Содержание

DNS

Система имен доменов (DNS) - это система распределенных баз данных, предназначенная для управления именами хостов и связанными с ними IP-адресами. DNS позволяет применять для идентификации хостов символьные имена, например ″www.jkltoys.com″, которые намного легче запомнить, чем IP-адреса (xxx.xxx.xxx.xxx). Отдельный сервер отвечает за имена и IP-адреса хостов, относящиеся лишь к некоторой части области, однако за счет взаимодействия с другими серверами он может преобразовывать любые имена хостов в IP-адреса. За счет совместной работы серверов DNS компьютеры могут обмениваться данными по Internet.

Служба DNS, предусмотренная в версии V5R1, основана на стандартной реализации DNS, которая называется BIND (Berkeley Internet Name Domain) версии 8. В предыдущих выпусках OS/400(R) служба DNS была основана на стандарте BIND версии 4.9.3. Для работы с новым сервером DNS, основанным на BIND 8, необходимо установить компонент 33 операционной системы OS/400 - Portable Application Solutions Environment (PASE). Если в системе не установлена функция PASE, то вы можете продолжить работу с сервером DNS, основанным на BIND 4.9.3, который применялся в предыдущем выпуске. Однако переход на BIND 8 позволит улучшить работу и повысить уровень безопасности сервера DNS.

Примечание: В этом разделе описаны новые функции, относящиеся к стандарту BIND 8. Если в вашей системе не установлена функция PASE, необходимая для работы DNS BIND 8, то за информацией о сервере DNS на основе BIND 4.9.3 обратитесь к разделу DNS Information Center V4R5

 (около 357 Кб).

- Раздел “Как напечатать этот раздел” на стр. 2 содержит информацию о загрузке и печати раздела, посвященного серверу DNS.

Основные сведения о DNS
В этом разделе описаны основные принципы работы DNS в системе iSeries.

В разделе **“Примеры работы с сервером DNS” на стр. 2** приведены диаграммы, демонстрирующие работу сервера DNS, и пояснения к ним.

Раздел **“Краткая информация о DNS” на стр. 10** содержит определения объектов и процессов, применяемых сервером DNS.

Раздел **“Планирование конфигурации DNS” на стр. 21** содержит инструкции по планированию конфигурации сервера DNS.

Работа с DNS
В этом разделе приведены инструкции по настройке сервера DNS в системе iSeries и работе с ним. Кроме того, в нем описаны новые возможности, предусмотренные в этом выпуске.

“Ресурсы, необходимые для работы с DNS” на стр. 23
В этом разделе приведен список программного обеспечения, которое требуется для работы со службой DNS на сервере iSeries.

“Настройка сервера DNS” на стр. 24
В этом разделе описана процедура настройки сервера имен с помощью Навигатора, а также способ, применяемый сервером DNS для преобразования запросов, не относящихся к его домену.

“Работа с DNS” на стр. 28
В этом разделе описано, как проверить правильность работы сервера DNS, собрать информацию о его производительности и выполнить необходимые действия над данными и файлами DNS.

“Устранение ошибок DNS” на стр. 35
В этом разделе описаны параметры ведения протокола и отладки сервера DNS. Эта информация поможет вам устранить неполадки в работе сервера DNS.

Если вы не смогли найти ответы на некоторые вопросы в Information Center, обратитесь к разделу “Дополнительная информация о DNS” на стр. 38, в котором приведены ссылки на другие источники информации о DNS.

Как напечатать этот раздел

Для просмотра или загрузки этого раздела в формате PDF выберите ссылку DNS (примерно 357 Кб).

Для сохранения документа PDF на рабочей станции для дальнейшего просмотра или печати выполните следующие действия:

1. Откройте документ PDF в окне браузера (для этого щелкните на приведенной выше ссылке).
2. В окне браузера откройте меню **Файл**.
3. Нажмите кнопку **Сохранить как...**
4. Перейдите в каталог, в котором вы хотите сохранить файл PDF.
5. Нажмите кнопку **Сохранить**.

Для просмотра и печати документов PDF применяется программа Adobe Acrobat Reader. Ее можно загрузить с Web-сайта фирмы Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Примеры работы с сервером DNS

DNS - это система распределенных баз данных, предназначенная для управления именами хостов и связанными с ними IP-адресами. Ниже приведены примеры, которые позволяют понять принципы работы сервера DNS и функции, которые он выполняет в сети. В этих примерах описана конфигурация сервера и его назначение. Кроме того, в них приведены ссылки на определения некоторых понятий, которые позволят вам лучше понять приведенные рисунки.

“Пример: Сервер DNS для внутренней сети” на стр. 3
В этом примере описана простая подсеть, для которой настроен сервер DNS.

“Пример: Сервер DNS, подключенный к Internet” на стр. 4
В этом разделе описана простая подсеть, в которой настроен сервер DNS, подключенный к Internet.

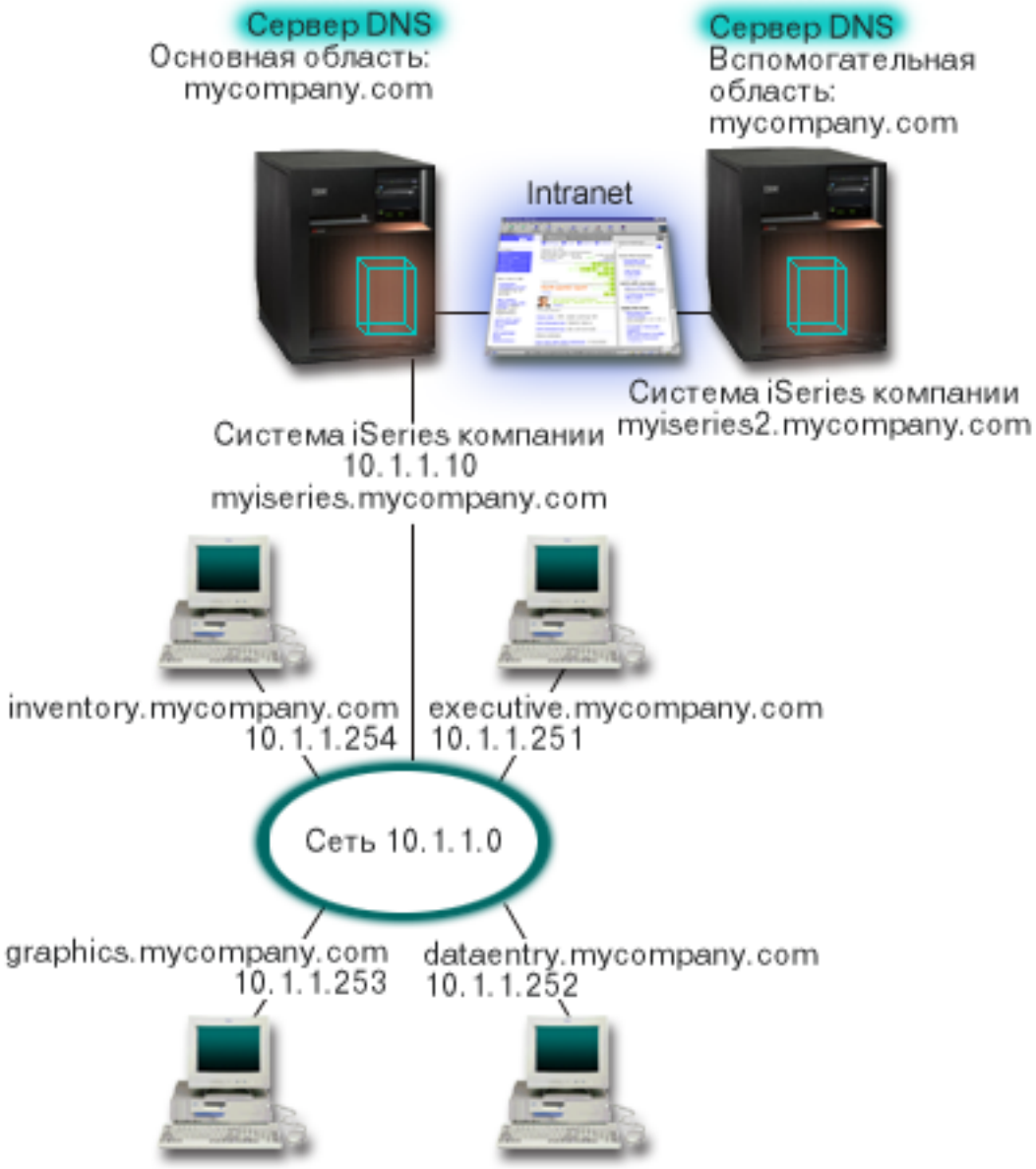
“Пример: Серверы DNS и DHCP, расположенные в одной системе iSeries(TM)” на стр. 6
В этом примере описана работа серверов DNS и DHCP, расположенных в одной системе. Такая конфигурация позволяет серверу DHCP автоматически обновлять информацию об области на сервере DNS каждый раз, когда хосту присваивается новый IP-адрес. Если вы планируете создать сервер DHCP в другой системе, обратитесь к разделу Пример: Серверы DNS и DHCP, расположенные на разных серверах iSeries за дополнительными рекомендациями по настройке DHCP.

“Пример: Сервер DNS в сети с брандмауэром” на стр. 8
В этом примере описана настройка сервера DNS в сети с брандмауэром, который защищает данные внутренних хостов от внешних пользователей, не ограничивая доступ внутренних пользователей к Internet.

Пример: Сервер DNS для внутренней сети

На приведенном ниже рисунке изображен сервер DNS, настроенный в системе iSeries(TM) для внутренней сети. Этот экземпляр сервера получает запросы через все интерфейсы IP. Он играет роль основного сервера имен для области ″mycompany.com″.

Рисунок 1. Сервер DNS для внутренней сети.



Каждому хосту области присвоены IP-адрес и имя хоста. Администратор должен вручную создать “Записи о ресурсах DNS” на стр. 16 для хостов области DNS. Записи об адресе (A) служат для преобразования имени хоста в его IP-адрес. Это позволяет другим хостам сети отправлять серверу DNS запросы на получение IP-адреса, связанного с указанным именем хоста. Записи обратного

преобразования (PTR) служат для преобразования IP-адреса компьютера в имя хоста. Это позволяет другим хостам сети отправлять серверу DNS запросы на получение имени хоста, связанного с указанным IP-адресом.

Помимо записей типа A и PTR сервер DNS поддерживает многие другие записи о ресурсах, запросы на получение которых могут отправлять клиенты. Набор создаваемых записей зависит от того, какие приложения, применяющие TCP/IP, используются пользователями внутренней сети. Например, если в сети применяется программа электронной почты, то на сервере потребуется создать записи системы обмена почтой (MX), для того чтобы служба SMTP могла получать от сервера DNS информацию о том, в каких системах установлены почтовые серверы.

Если бы данная сеть входила в более крупную корпоративную сеть, то потребовалось бы определить внутренние корневые серверы.

Вспомогательные серверы
Вспомогательные серверы загружают информацию об области с сервера, ответственного за эту область. Процедура загрузки информации об области на вспомогательный сервер называется передачей информации об области ответственности. При запуске вспомогательный сервер загружает с основного сервера имен всю информацию о домене. Затем вспомогательный сервер имен загружает обновленную информацию с основного сервера, когда он получает соответствующее уведомление от основного сервера (если включена функция NOTIFY), либо когда он обращается к основному серверу и обнаруживает, что информация была изменена.
На приведенном выше рисунке сервер myiseries подключен к внутренней сети. Другой сервер iSeries, myiseries2, играет роль вспомогательного сервера DNS для области mycompany.com. Вспомогательный сервер уменьшает нагрузку на основной сервер и заменяет его в случае сбоя. Для каждой области рекомендуется создавать по крайней мере по одному вспомогательному серверу.

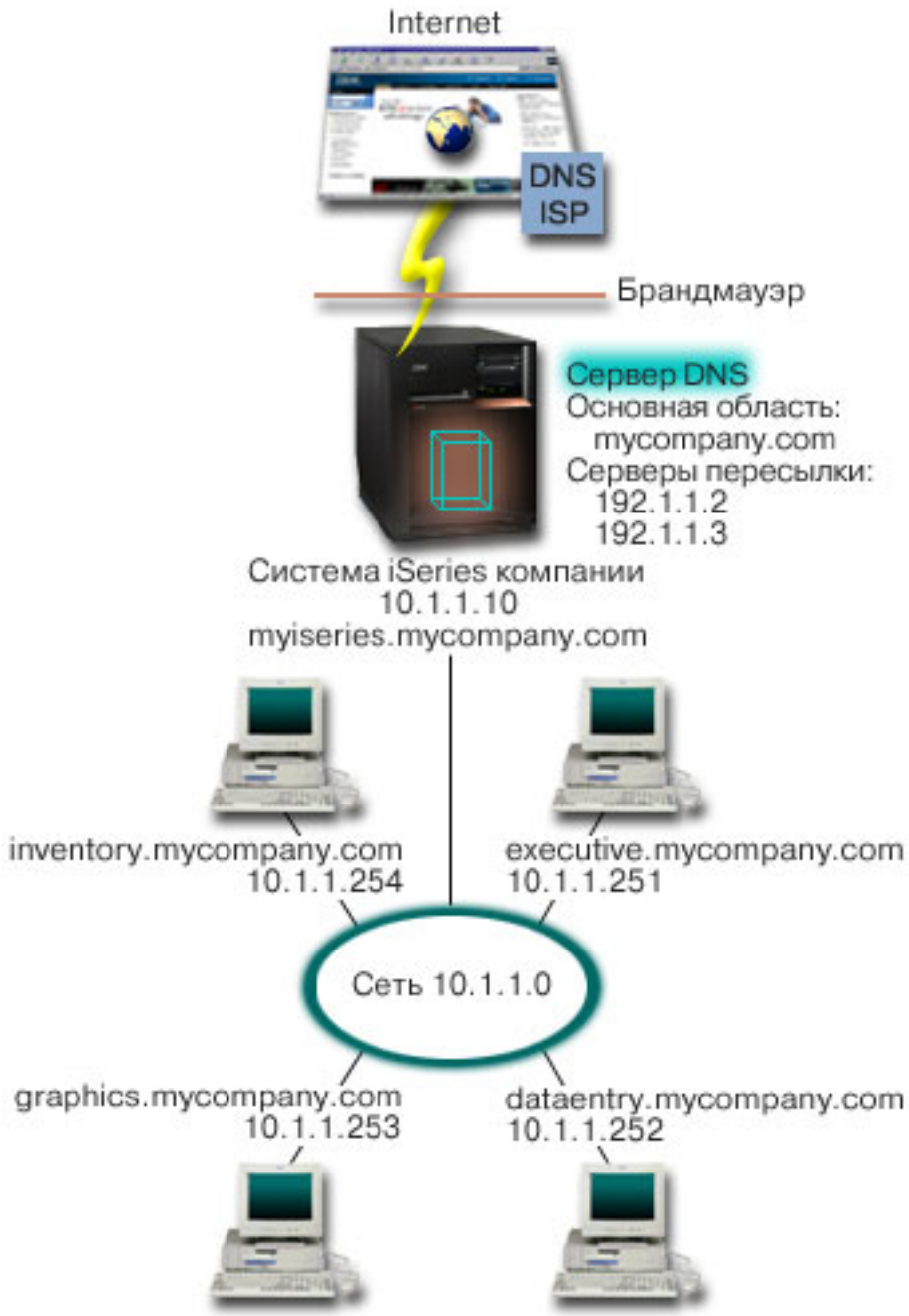
Дополнительная информация об объектах, описанных в этом примере, приведена в следующих разделах:

- Раздел “Основные сведения о DNS” на стр. 11 содержит определение службы DNS и описание принципов ее работы.Кроме того, в этом разделе приведены определения различных типов областей, которые могут быть созданы на сервере DNS.
- Раздел “Записи о ресурсах DNS” на стр. 16 содержит информацию о назначении различных записей о ресурсах сервера DNS.

Пример: Сервер DNS, подключенный к Internet

На приведенном ниже рисунке приведена та же схема сети, что и в примере “Пример: Сервер DNS для внутренней сети” на стр. 3, однако теперь предполагается, что эта сеть подключена к Internet.Рассмотрим случай, когда пользователям внутренней сети разрешено работать в Internet, однако брандмауэр блокирует все данные, поступающие из Internet во внутреннюю сеть.

Рисунок 1. Сервер DNS, подключенный к Internet.



Для того чтобы у сервера появилась возможность преобразовывать адреса хостов Internet, выполните по крайней мере одно из следующих действий:

Определите корневые серверы Internet
Список корневых серверов Internet, применяемых по умолчанию, можно загрузить автоматически, однако вам может потребоваться обновить этот список. Эти серверы позволяют отвечать на запросы, связанные с адресами, не входящими в локальную область. Инструкции по получению текущего списка корневых серверов Internet приведены в разделе “Получение информации от внешних серверов DNS” на стр. 28.

Разрешите пересылку запросов
Вы можете настроить сервер таким образом, чтобы все запросы, не относящиеся к области

mycompany.com, пересылались внешним серверам DNS, например, серверам DNS вашего провайдера Internet (ISP). Если поиск необходимых записей должен выполняться как на корневых серверах, так и на серверах пересылки, укажите в параметре **forward** значение **first**. В этом случае сервер вначале обратится к серверам пересылки, а затем, если от них не будет получен ответ, к корневым серверам.

Помимо этого, может потребоваться внести следующие изменения в конфигурацию:

Присвойте свободные IP-адреса
В приведенном выше примере указаны адреса 10.x.x.x. Однако эти адреса могут применяться только во внутренней сети. Они приведены только в качестве примера. Адреса в вашей сети назначаются ISP и зависят от конфигурации сети.

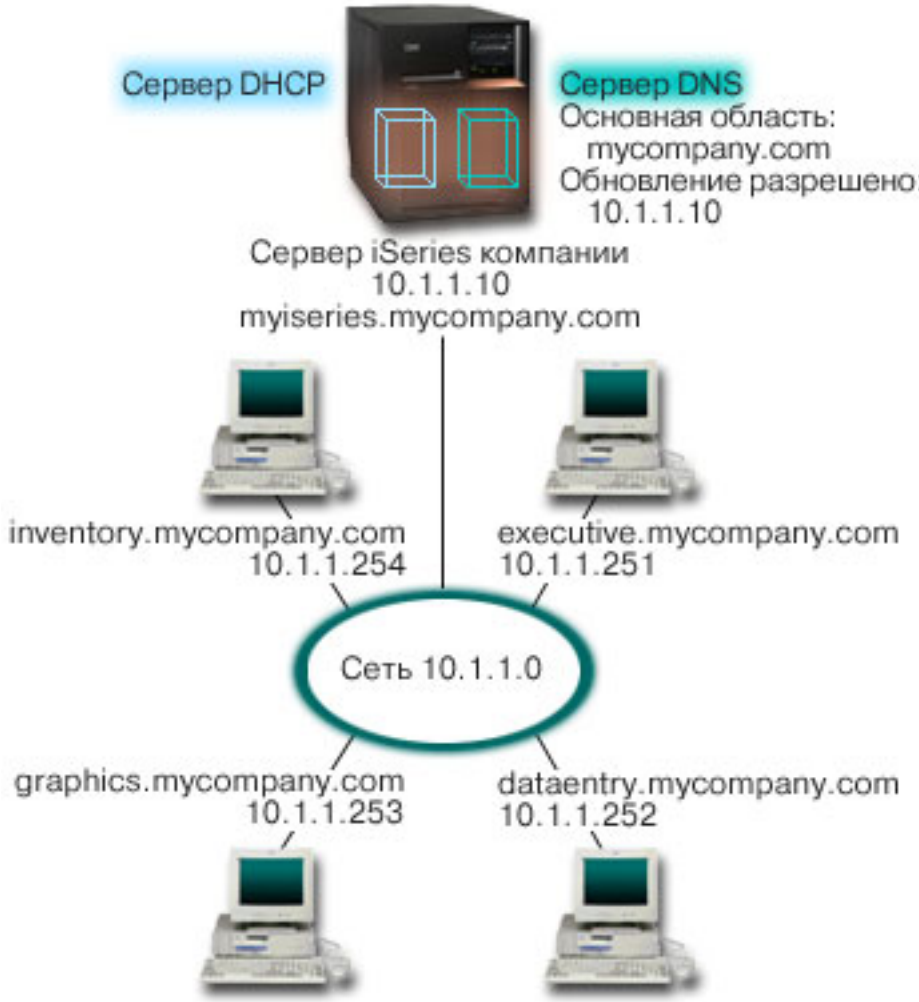
Зарегистрируйте имя домена
Если вы хотите, чтобы ваш домен был доступен в Internet, “Настройка домена DNS” на стр. 14.

Настройте брандмауэр
Не рекомендуется напрямую подключать сервер DNS к Internet. Вам следует настроить брандмауэр или принять какие-либо другие меры по защите системы iSeries(TM). Дополнительная информация по этому вопросу приведена в разделе IBM Secureway: iSeries и Internet справочной системы Information Center.

Пример: Серверы DNS и DHCP, расположенные в одной системе iSeries(TM)

На приведенном ниже рисунке показана схема небольшой подсети, к которой подключен один сервер iSeries, выполняющий роль сервера DNS и DHCP. Предположим, что в этой подсети программы учета и приложения для администрирования, играющие роль клиентов, создают документы, которые содержат графические данные и хранятся на сервере графических файлов. Для получения данных с сервера графических файлов они подключают сетевой диск, указывая имя хоста этого сервера.

Рисунок 1. Серверы DNS и DHCP, расположенные в одной системе iSeries.



В предыдущих версиях серверы DHCP и DNS не были связаны друг с другом. Когда сервер DHCP присваивал клиенту новый IP-адрес, администратор должен был вручную обновлять соответствующие записи на сервере DNS. В данном примере при обновлении IP-адреса сервера графических файлов сервером DHCP клиенты не смогут подключить сетевой диск, так как в записях DNS будет храниться старый IP-адрес сервера.

В версии V5R1 сервер DNS основан на стандарте BIND 8, поэтому вы можете разрешить “Динамическое обновление данных DNS” на стр. 14 информации об области, чтобы записи DNS автоматически обновлялись сервером DHCP при изменении адреса.Например, когда истечет время выделения адреса для сервера графических файлов, и сервер DHCP присвоит ему новый IP-адрес 10.1.1.250, соответствующие записи DNS будут автоматически изменены. В результате сразу после изменения адреса клиенты получат от сервера DNS правильный ответ на запрос об IP-адресе, связанном с именем хоста сервера графических файлов.

Для настройки функции динамического обновления области DNS выполните следующие действия:

Определите динамическую область
Динамическую область нельзя обновлять вручную во время работы сервера. Это может привести к конфликту с поступившими запросами на динамическое обновление. Для внесения обновлений вручную нужно остановить сервер. Однако при этом все запросы на динамическое обновление, полученные во время простоя сервера, не будут обработаны. В связи с этим рекомендуется создать отдельную динамическую область, выбрав ее таким образом, чтобы

записи DNS нужно было редко изменять вручную. Дополнительная информация о настройке областей для работы с функцией динамического обновления информации приведена в разделе “Определение структуры домена” на стр. 21.

Настройте опцию allow-update
Если для области задана опция allow-update, то она считается динамической областью. Эта опция устанавливается индивидуально для каждой области. Запросы на динамическое обновление области будут приниматься сервером только в том случае, если для этой области задана опция allow-update. В данном примере опцию allow-update обязательно нужно установить для области mycompany.com. Остальные области могут быть настроены как статические или как динамические по вашему усмотрению.

Настройте функцию динамического обновления на сервере DHCP
Серверу DHCP необходимо предоставить права на динамическое обновление записей DNS при изменении IP-адреса. Дополнительная информация приведена разделе Настройка функции динамического обновления на сервере DHCP.

Настройте параметры обновления информации на вспомогательном сервере
Для своевременного обновления информации на вспомогательных серверах настройте функцию NOTIFY на сервере DNS. В результате сервер DNS будет отправлять вспомогательным серверам сообщения обо всех изменениях записей области mycompany.com. Кроме того, настройте функцию передачи измененной информации об области (IXFR), для того чтобы вспомогательные серверы, поддерживающие IXFR, загружали только измененную информацию об области, а не всю информацию целиком.

Если вы планируете настроить серверы DNS и DHCP в разных системах, следует учесть дополнительные требования к конфигурации сервера DHCP. Дополнительная информация по этому вопросу приведена в разделе Пример: Серверы DNS и DHCP, расположенные в разных системах iSeries.

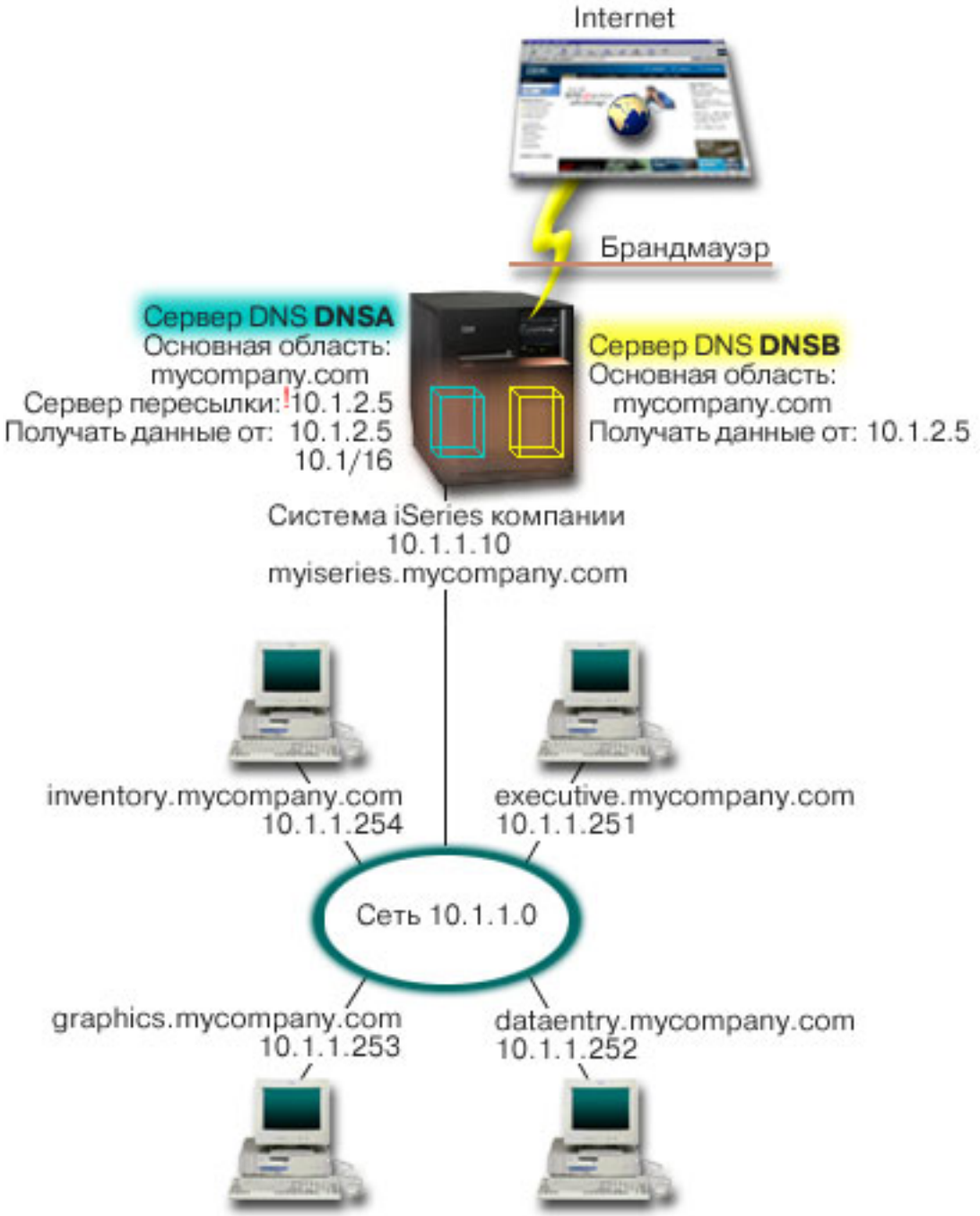
Пример: Сервер DNS в сети с брандмауэром

На приведенном ниже рисунке показана схема небольшой подсети, для защиты которой применяется брандмауэр. В версии V5R1 служба DNS основана на стандарте BIND 8, поэтому она позволяет создать в системе iSeries(TM) несколько серверов DNS. Предположим, что в корпоративной сети есть внутренняя подсеть с зарезервированным пространством IP-адресов, и внешняя подсеть, которая доступна внешним пользователям.

Для работы внутренним пользователям необходимо обмениваться почтой с пользователями внешней сети и подключаться к внешним хостам. Кроме того, у внутреннего сервера DNS должен быть доступ только к некоторым внутренним областям, которые недоступны внешним хостам. В то же время внешним серверам DNS также запрещается доступ к внутренней сети.

Для выполнения указанных требований необходимо настроить два экземпляра сервера DNS в одной системе iSeries: один для внутренней, и один для внешней сети. Такая конфигурация называется DNS с разделенной областью ответственности.

Рисунок 1. DNS с разделенной областью ответственности в сети с брандмауэром.



В качестве основной области внешнего сервера, DNSB, выбирается mycompany.com. Однако информация об этой области будет включать только те записи о ресурсах, которые относятся к внешнему домену. Основной областью внутреннего сервера, DNSA, также служит mycompany.com, однако информация об этой области содержит только те записи о ресурсах, которые относятся к внутренней сети. В качестве адреса сервера пересылки выбирается 10.1.2.5. В результате сервер DNSA будет пересылать запросы, которые он не может обработать, серверу DNSB.

Если вы хотите обеспечить целостность брандмауэра или принять другие меры защиты, настройте опцию listen-on для защиты внутренних данных. Для этого разрешите внутренним хостам отправлять внутреннему серверу только те запросы, которые относятся к внутренней области mycompany.com.

Для работы описанной конфигурации необходимо, чтобы внутренние клиенты отправляли запросы только серверу DNSA. Для настройки DNS с разделенной областью ответственности рекомендуется настроить следующие параметры:

Адреса для получения запросов
В предыдущих примерах в системе iSeries был только один сервер DNS. Он получал запросы через все интерфейсы IP системы. Если в системе iSeries создано несколько серверов DNS, для каждого из них нужно задать набор IP-адресов интерфейсов, через которые они будут получать запросы. Эти наборы не должны пересекаться. В данном случае предположим, что все запросы, поступающие через брандмауэр, будут отправляться через интерфейс 10.1.2.5. Эти запросы должны быть отправлены внешнему серверу. Следовательно, сервер DNSB должен работать с IP-адресом 10.1.2.5. Внутренний сервер, DNSA, может принимать запросы через любой интерфейс 10.1.x.x, *за исключением* 10.1.2.5. Для того чтобы исключить этот адрес, укажите его в списке адресов для сравнения (AML) перед разрешенным префиксом адреса.

Порядок элементов в списке адресов для сравнения (AML)
Всегда применяется тот элемент AML, который был найден первым. Например, для того чтобы разрешить прием запросов от всех адресов 10.1.x.x, за исключением 10.1.2.5, элементы в списке должны быть расположены в следующем порядке: (!10.1.2.5; 10.1/16). В данном случае для адреса 10.1.2.5 первой будет найдена запись, запрещающая доступ.

Если элементы будут стоять в обратном порядке (10.1/16; !10.1.2.5), то для IP-адреса 10.1.2.5 первой будет найдена запись, разрешающая доступ. Поскольку остальные записи списка не проверяются, запрос от этого адреса будет принят.

Краткая информация о DNS

В выпуске V5R1 служба DNS предоставляет некоторые дополнительные функции, предусмотренные в стандарте BIND 8. Ниже приведены ссылки на разделы с информацией об основных принципах работы службы DNS и новых функциях этой службы:

Основные функции DNS:

“Основные сведения о DNS” на стр. 11
Этот раздел содержит вводную информацию о службе DNS и принципах организации данных DNS, а также описание различных типов областей.

“Основные сведения о запросах DNS” на стр. 12
В этом разделе описана процедура обработки запросов сервером DNS.

“Настройка домена DNS” на стр. 14
В этом разделе описана процедура регистрации домена и приведены ссылки на другие источники информации о настройке домена.

Новые функции DNS:

“Динамическое обновление данных DNS” на стр. 14
В выпуске V5R1 служба DNS основана на стандарте BIND 8, поэтому она поддерживает динамическое обновление данных. Запросы на динамическое обновление отправляются некоторыми внешними службами, в частности, сервером DHCP.

“Новые возможности BIND 8” на стр. 15
Помимо динамического обновления данных, в стандарте BIND 8 предусмотрен еще ряд новых возможностей, позволяющих повысить производительность сервера DNS.

Описание записей о ресурсах:

“Записи о ресурсах DNS” на стр. 16
В записях о ресурсах хранится информация об именах хостов и IP-адресах. В этом разделе приведен полный список записей о ресурсах, поддерживаемых в выпуске V5R1.

“Записи о почтовом шлюзе и записи MX” на стр. 20
Служба DNS предоставляет дополнительные возможности по настройке пересылки почты с помощью этих записей.

Подробную информацию о DNS можно найти и во многих других публикациях. Ссылки на некоторые из них приведены в разделе “Дополнительная информация о DNS” на стр. 38.

Основные сведения о DNS

Система имен доменов (DNS) - это система распределенных баз данных, предназначенная для управления именами хостов и связанными с ними IP-адресами. DNS позволяет применять для идентификации хостов символьные имена, например ″www.jkltoys.com″, которые намного легче запомнить, чем IP-адреса (xxx.xxx.xxx.xxx). Отдельный сервер отвечает за имена и IP-адреса хостов, относящиеся лишь к некоторой части области, однако за счет взаимодействия с другими серверами он может преобразовывать любые имена хостов в IP-адреса. За счет совместной работы серверов DNS компьютеры могут обмениваться данными по Internet.

Вся информация DNS хранится в виде иерархии доменов. Каждый сервер отвечает за небольшую часть этой информации, например, за один субдомен. Часть домена, за которую отвечает сервер, называется областью. Сервер DNS, на котором хранится вся информация о хостах, относящихся к области, называется ответственным за эту область. Ответственный сервер отвечает на запросы, связанные с хостами из его области, с помощью собственных записей о ресурсах. Процесс обработки запроса зависит от ряда факторов. Описание различных способов обработки запросов приведено в разделе “Основные сведения о запросах DNS” на стр. 12.

Основные сведения об областях

Вся информация DNS поделена на наборы данных, называемые областями. В области хранится часть информации об именах и IP-адресах, относящихся к домену DNS. Сервер, на котором хранится вся информация об области, является ответственным за область. Иногда право на обработку запросов DNS, относящихся к какому-то субдомену, желательно передать другому серверу DNS. В этом случае в конфигурации сервера DNS, ответственного за домен, необходимо указать, что запросы, связанные с субдоменом, должны пересылаться другому серверу.

Довольно часто информация об области хранится не только на ответственном сервере DNS, но и на нескольких резервных серверах. Такие серверы называются вспомогательными. Они загружают информацию об области с ответственного сервера. Настройка вспомогательных серверов позволяет распределить нагрузку по нескольким серверам и получить резервную копию в случае сбоя основного сервера. Процедура загрузки информации об области на вспомогательный сервер называется передачей информации об области ответственности. После инициализации вспомогательный сервер загружает всю информацию об области с основного сервера. Впоследствии вспомогательный сервер загружает информацию об области с основного или другого вспомогательного сервера при изменении этой информации.

Типы областей DNS

Служба DNS системы iSeries(TM) позволяет создавать области нескольких типов:

Основная область

Информация об этой области загружается из файла хоста. В основной области можно создать подобласть, или дочернюю область. Кроме того, эта область может содержать записи о ресурсах, например, записи с информацией о хосте, записи псевдонимов (CNAME), записи об адресе (A) и

записи с указателем для обратного преобразования (PTR).
Примечание: В другой документации по BIND основные области иногда называются ″главными областями″.

Подобласть
Подобласть - это область внутри основной области. Подобласти позволяют разделить всю информацию об области на более мелкие части.

Дочерняя область
Дочерняя область - это подобласть, права на управление которой переданы одному или нескольким серверам имен.

Псевдоним (CNAME)
Псевдоним - это альтернативное имя домена основного сервера.

Хост
Такой объект позволяет определить записи A и PTR, связанные с хостом. Для хоста могут быть определены дополнительные “Записи о ресурсах DNS” на стр. 16.

Вспомогательная область
Информация об этой области загружается с основного сервера или другого вспомогательного сервера. На вспомогательном сервере хранится полная копия информации об области.
Примечание: В другой документации по BIND вспомогательные области иногда называются ″подчиненными″.

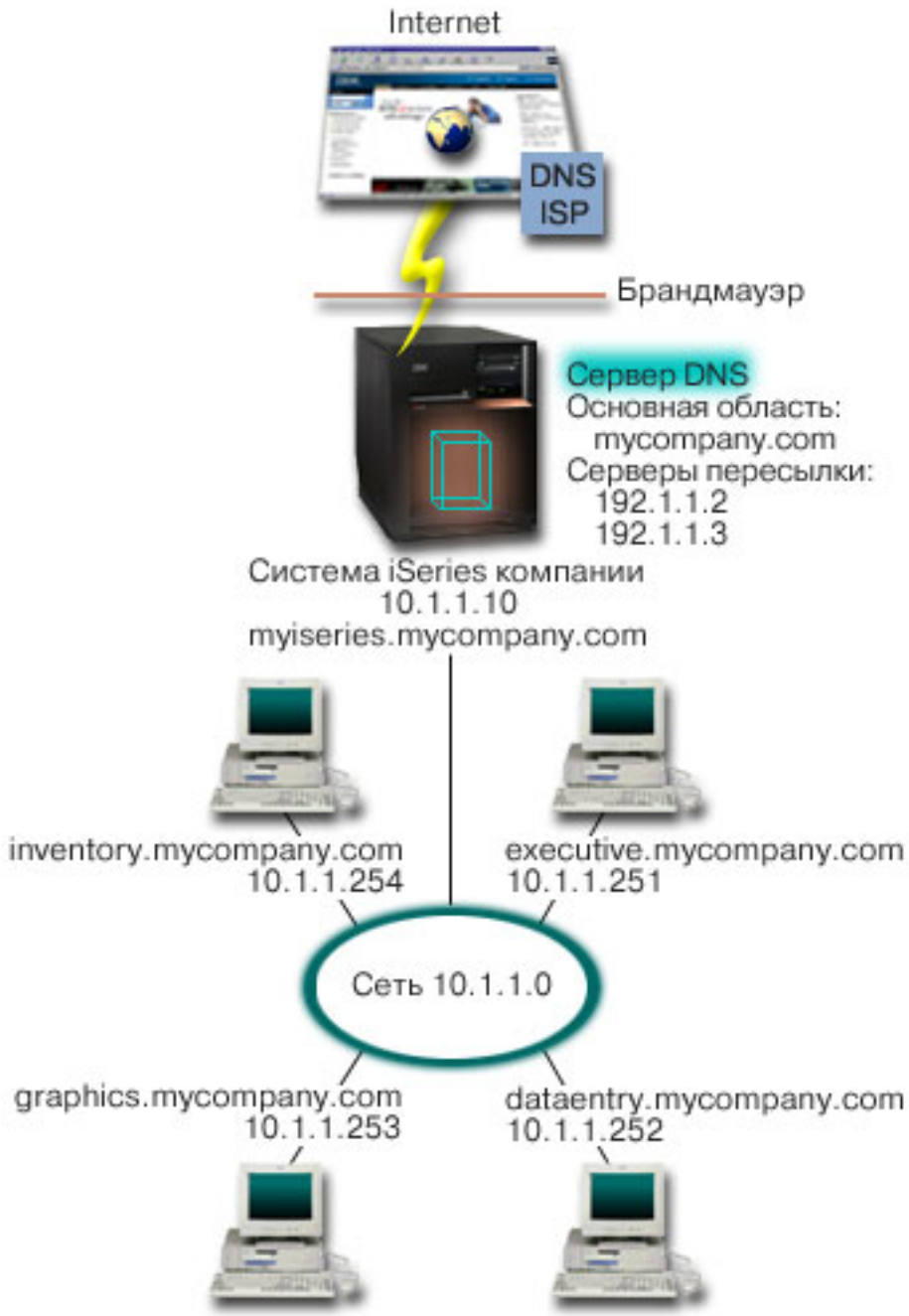
Ограниченная область
Ограниченная область во многом аналогична вспомогательной области, однако в ней хранятся только копии записей NS из основной области.

Область пересылки
Областью пересылки называется область, все запросы к которой пересылаются другим серверам.

Основные сведения о запросах DNS

С помощью серверов DNS клиенты получают информацию о других хостах сети. Запросы серверу могут отправляться как самими клиентами, так и другими работающими приложениями. Такой запрос содержит полное имя хоста (FQDN), тип запроса, например, тип записи, которая необходима клиенту, и класс имени домена (большинство имен относятся к классу Internet - IN). На приведенном ниже рисунке показан пример сети, описанный в разделе “Пример: Сервер DNS, подключенный к Internet” на стр. 4.

Рисунок 1. Сервер DNS, подключенный к Internet.



Предположим, что хост *dataentry* отправляет серверу DNS запрос на получение информации о хосте ″graphics.mycompany.com″. Сервер DNS просмотрит собственную информацию об области и отправит клиенту ответ с информацией о том, что IP-адрес хоста равен 10.1.1.253.

Теперь предположим, что хост *dataentry* отправил запрос на получение IP-адреса хоста ″www.jkl.com.″.. Сведения об этом хосте отсутствуют в информации об области сервера DNS. Такой запрос может быть обработан двумя способами: рекурсивным и циклическим. Если на сервере DNS настроен рекурсивный способ обработки запросов, то сервер обратится с запросом на преобразование имени к другим серверам DNS от имени клиента, отправившего исходный запрос, а затем перешлет клиенту полученный ответ. Сервер DNS сохранит полученный ответ в своем кэше, поэтому в будущем для обработки аналогичных запросов ему не потребуется обращаться к другим серверам. Клиент может попытаться самостоятельно обратиться к другим серверам DNS для

преобразования имени хоста. При таком способе обработки запроса, который называется циклическим, клиент отправляет запросы серверам из имеющегося списка, а затем - дополнительным серверам, которым был переадресован запрос исходными серверами.

Настройка домена DNS

Вы можете настроить сервер DNS, который будет обслуживать запросы на преобразование имен и адресов хостов во внутренней сети. Кроме того, если сервер будет подключен к Internet, то он сможет обрабатывать запросы, поступающие от внешних хостов. Для настройки домена в Internet необходимо зарегистрировать имя домена.

Для обработки внутренних запросов не требуется регистрировать имя домена. Однако вы можете зарегистрировать имя домена для того, чтобы никто не мог зарегистрировать домен Internet с таким именем. Это имеет смысл сделать в том случае, если в дальнейшем вы планируете использовать этот домен во внешней сети.

Для регистрации домена можно обратиться в специальную службу регистрации имен доменов, либо к провайдеру Internet (ISP), оказывающему такие услуги. Некоторые ISP могут зарегистрировать домен от имени клиента. Список служб регистрации имен доменов, уполномоченных организацией ICANN, можно найти на Web-сайте Internet Network Information Center (InterNIC)  .

Процедура регистрации домена DNS и подготовки к его обслуживанию подробно описана во многих публикациях. Некоторые из этих публикаций перечислены в разделе “Дополнительная информация о DNS” на стр. 38.

Динамическое обновление данных DNS

Протокол динамической настройки хостов (DHCP) - это стандартный протокол TCP/IP, который позволяет настроить центральный сервер, предоставляющий IP-адреса и другую информацию о конфигурации всем остальным компьютерам, подключенным к сети.В ответ на запросы клиентов сервер DHCP отправляет динамически созданное описание конфигурации. Вы можете определить параметры конфигурации хостов на центральном сервере DHCP, который будет автоматически сообщать эти параметры хостам. Этот протокол обычно применяется для выделения временных IP-адресов клиентам, когда число клиентов в сети превосходит число доступных IP-адресов.

Раньше вся информация DNS хранилась в статической базе данных. Все “Записи о ресурсах DNS” на стр. 16 вручную создавались и обслуживались администратором. В настоящее время серверы DNS, поддерживающие BIND 8, могут принимать запросы на динамическое обновление информации об области от различных служб.

В конфигурации сервера DHCP можно указать, что при выделении адреса хосту должен отправляться запрос на обновление информации DNS. В быстро растущих или постоянно изменяющихся сетях TCP/IP, а также в сетях с часто изменяющейся топологией такая функция позволяет значительно сэкономить время администратора сервера DNS. Информация о том, что клиент получил от сервера DHCP некоторый IP-адрес, немедленно отправляется серверу DNS. За счет этого сервер DNS может обрабатывать запросы на получение IP-адресов хостов даже тогда, когда эти адреса часто меняются.

Сервер DHCP может обновлять от имени клиента записи об адресе (A), записи обратного преобразования (PTR) или оба типа записей. В записи типа A хранится IP-адрес, связанный с именем хоста. В записи PTR хранится имя хоста, связанное с IP-адресом. При изменении адреса клиента сервер DHCP может автоматически отправить запрос на обновление информации DNS, для того чтобы другие хосты сети могли узнать новый IP-адрес клиента от сервера DNS. Для каждой обновленной записи будет создана текстовая запись (TXT), содержащая информацию о том, от кого был получен запрос на обновление (в данном случае - от DHCP).
Примечание: Если сервер DHCP будет обновлять только записи PTR, клиентам должно быть

разрешено обновлять информацию на сервере DNS. В этом случае каждый клиент самостоятельно обновит свою запись типа A. Обратите внимание, что не все клиенты DHCP поддерживают обновление собственной записи типа A. Перед настройкой такого способа динамического обновления ознакомьтесь с документацией по операционной системе, установленной на компьютерах-клиентах.

Для защиты динамически обновляемых областей создается список служб, которым предоставлены права на отправку запросов на обновление. Такие права могут быть предоставлены отдельным IP-адресам, целым подсетям, а также службам, знающим общий секретный ключ (который называется подписью транзакции, или TSIG). Перед обновлением записей о ресурсах сервер DNS проверяет, что пакет с запросом на обновление отправлен службой с соответствующими правами доступа.

Функция динамического обновления может применяться в том случае, когда серверы DNS и DHCP расположены в одной системе iSeries(TM), в разных системах iSeries, а также когда один из них расположен в системе другого типа, поддерживающей динамическое обновление. Дополнительная информация о настройке функции динамического обновления в системе iSeries приведена в следующих разделах:

- “Настройка функции динамического обновления на сервере DNS” на стр. 26
- Настройка функции динамического обновления на сервере DHCP
- Для отправки запросов на динамическое обновление информации DNS в системе должен быть установлен API QTOBUPT. Этот API автоматически устанавливается вместе с компонентом 31 (DNS) лицензионной программы OS/400(R).

Новые возможности BIND 8

В версии V5R1 служба DNS была обновлена, и теперь она поддерживает стандарт BIND 8. Если в системе не установлена функция PASE, то вы можете продолжить работать с сервером DNS, предназначенным для предыдущего выпуска OS/400(R), который основан на BIND 4.9.3. Требования, которые должны быть выполнены в системе iSeries(TM) для работы с сервером DNS, основанным на BIND 8, описаны в разделе “Ресурсы, необходимые для работы с DNS” на стр. 23. Ниже перечислены некоторые возможности новой версии DNS:

В системе iSeries можно запустить несколько серверов DNS
В предыдущих выпусках в системе можно было настроить только один сервер DNS. Теперь появилась возможность настроить несколько серверов DNS, иначе говоря - экземпляров сервера. За счет этого вы можете логически разграничить область ответственности между серверами. Для каждого экземпляра сервера необходимо определить IP-адрес интерфейса, по которому он будет получать запросы. Эти адреса не должны совпадать.

Данная возможность, в частности, может применяться для создания DNS с разделенной областью ответственности. В такой реализации один сервер отвечает за внутреннюю сеть, а второй применяется для обработки внешних запросов. Дополнительная информация о DNS с разделенной областью ответственности приведена в разделе “Пример: Сервер DNS в сети с брандмауэром” на стр. 8.

Условная пересылка
В этой версии предусмотрена более гибкая настройка параметров пересылки сервера DNS. В частности, сервер может пересылать все запросы, на которые он не может ответить самостоятельно. Вы можете настроить пересылку на глобальном уровне, исключив те домены, для которых должна выполняться обычная рекурсивная процедура обработки запросов. С другой стороны, вы можете настроить на глобальном уровне обычную рекурсивную процедуру обработки запросов, исключив домены, запросы к которым должны пересылаться.

Защищенное динамическое обновление данных
Серверы DHCP и некоторые другие службы могут динамически обновлять записи о ресурсах на сервере DNS, используя в качестве идентификационной информации подпись транзакции (TSIG) или

IP-адрес отправителя. За счет этого уменьшается объем информации об области, которую нужно обновлять вручную. Кроме того, все автоматические обновления вносятся только теми службами, у которых есть права на обновление DNS.

Дополнительная информация о динамическом обновлении информации приведена в разделе “Динамическое обновление данных DNS” на стр. 14. Дополнительная информация об обновлении данных DNS внешними службами с соответствующими правами доступа приведена в разделе “Планирование мер защиты” на стр. 22.

NOTIFY
Если опция NOTIFY включена, то при обновлении информации об области на основном сервере автоматически активируется функция NOTIFY сервера DNS. При этом основной сервер рассылает сообщение об обновлении данных всем известным вспомогательным серверам. После получения такого сообщения вспомогательный сервер может отправить запрос на передачу обновленной информации об области. Эта функция предназначена для синхронизации вспомогательных серверов. Она позволяет поддерживать все копии информации об области в согласованном состоянии.

Передача информации об области (IXFR и AXFR)
В прошлых выпусках при изменении информации об области вспомогательный сервер должен был загрузить всю информации об области, отправив запрос AXFR (Передать полную информацию об области). BIND 8 поддерживает новый способ передачи информации об области: IXFR (Передача измененной информации об области). Отправив запрос IXFR, сервер может загрузить вместо всей информации об области только измененные данные.

При изменении данных на основном сервере может устанавливаться специальный флаг. При получении запроса IXFR от вспомогательного сервера основной сервер отправляет только измененные данные. Функция IXFR особенно полезна в том случае, когда информация об области обновляется динамически. Кроме того, она позволяет сократить объем данных, передаваемых по сети.
Примечание: Для применения функции IXFR ее должны поддерживать как основной, так и вспомогательный сервер.

Записи о ресурсах DNS

База данных об области DNS содержит набор записей о ресурсах. Запись о ресурсе содержит информацию о некотором объекте. Например, запись об адресе (A) содержит IP-адрес, связанный с именем хоста, а запись обратного преобразования (PTR) содержит имя хоста, связанное с IP-адресом. Эти записи применяются сервером для обработки запросов на получение информации о хостах, относящихся к его области. Для того чтобы ознакомиться с описаниями различных записей о ресурсах DNS, выберите тип записи в приведенной ниже таблице.

Запись	Аббревиатура	Описание
Записи преобразования адресов	A	Запись A задает IP-адрес этого хоста. С помощью записей A выполняется запрос на преобразование имени домена в IP-адрес. Этот тип записей определен в RFC 1035.

Запись	Аббревиатура	Описание
Записи базы данных файловой системы Andrew	AFSDB	Запись AFSDB содержит адрес AFS или DCE объекта. Записи AFSDB, как и записи A, применяются для преобразования имени домена в адрес AFSDB; либо для преобразования имени домена кластера в адрес сервера идентифицируемого имени кластера. Этот тип записей определен в RFC 1183.
Записи полных имен	CNAME	Запись CNAME содержит фактическое имя домена данного объекта. Если DNS при обращении к псевдониму обнаруживает запись CNAME, содержащую полное имя, DNS затем запрашивает полное имя домена. Этот тип записей определен в RFC 1035.
Записи информации о хосте	HINFO	Запись HINFO содержит общую информацию о хосте. Стандартные имена процессоров и операционных систем определены в RFC 1700. Использование стандартных номеров не является обязательным. Этот тип записей определен в RFC 1035.
Записи Цифровой сети с комплексными услугами	ISDN	Запись ISDN содержит адрес этого объекта. Эта запись предназначена для преобразования имен хостов в адреса ISDN. Они используются только в сетях ISDN. Этот тип записей определен в RFC 1183.
Записи IP-адресов версии 6	AAAA	Запись AAAA содержит 128-разрядный адрес хоста. Записи AAAA, так же как и записи A, предназначены для преобразования имени хоста в его IP-адрес. Записи AAAA содержат IP-адреса версии 6, размер которых больше записи A. Этот тип записей определен в RFC 1886.
Записи расположения	LOC	Запись LOC содержит информацию о физическом расположении элементов сети. Такие записи применяются в приложениях для оценки эффективности работы сети или построения схемы физического расположения узлов сети. Этот тип записей определен в RFC 1876.

Запись	Аббревиатура	Описание
Записи Системы обмена почтой	MX	Записи MX содержат определение хоста системы обмена почтой для почтовых сообщений, отправляемых в этот домен. С помощью записей этого типа и значений параметров конфигурации хостов системы обмена почтой в SMTP (Простой протокол передачи почты) определяются адреса хостов, обрабатывающих и перенаправляющих почту для этого домена. Каждому хосту системы обмена почтой должна соответствовать запись адреса хоста (A) в существующей области. Этот тип записей определен в RFC 1035.
Записи почтовой группы	MG	Записи MG указывают имя домена почтовой группы. Этот тип записей определен в RFC 1035.
Записи почтового ящика	MB	Запись MB содержит имя домена хоста, на котором расположен почтовый ящик данного объекта. Почтовые сообщения, отправляемые в этот домен, перенаправляются на хост, который указан в записи MB. Этот тип записей определен в RFC 1035.
Записи информации о почтовом ящике	MINFO	Запись MINFO указывает почтовый ящик, в который должны направляться сообщения об ошибках для данного объекта. Записи MINFO чаще применяются для списков рассылки, чем для отдельных почтовых ящиков. Этот тип записей определен в RFC 1035.
Записи нового имени почтового ящика	MR	Запись MR указывает новое имя домена почтового ящика. Запись MR позволяет пользователям, сменившим почтовый ящик, перенаправлять входящие почтовые сообщения. Этот тип записей определен в RFC 1035.
Записи сервера имен	NS	Запись NS указывает ответственный сервер для данного хоста. Этот тип записей определен в RFC 1035.
Запись протокола доступа к сетевым службам	NSAP	Запись NSAP содержит адрес ресурса NSAP. Записи NSAP предназначены для преобразования имен доменов в адреса NSAP. Этот тип записей определен в RFC 1706.
Записи общих ключей	KEY	Запись KEY содержит общий ключ, связанный с именем DNS. Ключ может относиться к области, пользователю или хосту. Этот тип записей определен в RFC 2065.

Запись	Аббревиатура	Описание
Записи ответственных работников	RP	Запись RP содержит электронный адрес и описание лица, ответственного за область или хост. Этот тип записей определен в RFC 1183.
Записи указателей обратного преобразования	PTR	Запись PTR содержит имя домена хоста, для которого необходимо определить запись PTR. Запись PTR позволяет преобразовать IP-адрес в имя хоста. Этот тип записей определен в RFC 1035.
Записи маршрутизации	RT	Запись RT указывает имя домена хоста, который может перенаправлять IP-пакеты для данного хоста. Этот тип записей определен в RFC 1183.
Запись начала области ответственности	SOA	Запись SOA означает, что данный сервер является ответственным за область. Ответственный сервер - это лучший источник для сбора данных внутри области. Запись SOA содержит общую информацию об области и правила перезагрузки для резервных серверов. Для каждой области создается только одна запись SOA. Этот тип записей определен в RFC 1035.
Текстовые записи	TXT	Запись TXT состоит из нескольких строк текста, связанных с именем домена, каждая длиной до 255 символов. Записи TXT можно использовать наряду с записями ответственных работников (RP) для хранения информации о лице, ответственном за область. Этот тип записей определен в RFC 1035. Записи TXT используются протоколом динамической настройки хостов (DHCP) iSeries для динамического обновления. Сервер DHCP создает запись TXT для каждого внесенного им обновления записей A и PTR. Записи сервера DHCP начинаются с символов **AS400DHCP:**.
Записи стандартных служб	WKS	Записи WKS указывают стандартные службы, поддерживаемые объектом. Чаще всего записи WKS содержат информацию о поддержке протоколов TCP и UDP для данного адреса. Этот тип записей определен в RFC 1035.

Запись	Аббревиатура	Описание
Записи преобразования адресов X.400	PX	Запись PX содержит указатель на информацию о преобразовании X.400/RFC 822. Этот тип записей определен в RFC 1664.
Записи преобразования адресов X25	X25	Запись X25 содержит адрес ресурса X25. Записи X25 предназначены для преобразования имен хостов в адреса PSDN. Они используются только в сетях X25. Этот тип записей определен в RFC 1183.

Записи о почтовом шлюзе и записи MX

Записи о почтовом шлюзе и записи MX применяются программой пересылки почты, например, SMTP. За дополнительной информацией о типах записей о почтовом шлюзе, поддерживаемых сервером DNS системы iSeries(TM), обратитесь к таблице “Записи о ресурсах DNS” на стр. 16.

Для организации обмена почтой на сервере DNS предусмотрены записи Системы обмена почтой. В сети с DNS приложение SMTP доставляет почту, адресованную хосту TEST.IBM.COM, не просто открывая соединение TCP с TEST.IBM.COM. Сначала SMTP отправляет на сервер DNS запрос о том, какие серверы хоста можно использовать для доставки почтового сообщения.

Маршрутизация почты

Серверы DNS работают с записями ресурсов, называемыми записями Системы обмена почтой (MX). В этих записях имени домена или хоста ставятся в соответствие имя хоста и коэффициент предпочтения. Обычно в записях типа MX указывается хост, который будет обрабатывать почту для некоторого хоста, а также другой, вспомогательный хост для случая, если первый хост окажется недоступен. Таким образом, записи типа MX позволяют направлять почту, адресованную одному хосту, на другой хост.

Для одного домена или имени хоста могут существовать несколько записей типа MX. Порядок, в котором они выбираются, определяется коэффициентом предпочтения (или приоритетом) каждой записи. Наименьший коэффициент обозначает наиболее предпочтительный вариант - запись, которая будет выбрана первой. Если наиболее предпочтительный хост недоступен, приложение, отправляющее почту, попытается подключиться к следующему по приоритету хосту. Приоритет задается администратором домена или создателем записи типа MX.

Если имя, указанное в запросе, находится в области ответственности сервера DNS, но для него нет ни одной записи типа MX, то сервер может вернуть пустой список записей типа MX. В этом случае приложение, отправляющее почту, попытается установить прямое соединение с целевым хостом.
Примечание: В записях MX не рекомендуется указывать имена доменов с символами подстановки (например, `*.mycompany.com`).

Пример записи типа MX для хоста

В следующем примере для доставки почты хосту fsc5.test.ibm.com приложение сначала (согласно установленным приоритетам) попытается установить прямое соединение с этим хостом. Если хост окажется недоступен, то почта должна быть доставлена на psfred.test.ibm.com или (если и он будет недоступен) - на mvs.test.ibm.com. Записи типа MX будут выглядеть следующим образом:

```
fsc5.test.ibm.com   IN MX 0 fsc5.test.ibm.com
                       IN MX 2 psfred.test.ibm.com
                       IN MX 4 mvs.test.ibm.com
```

Планирование конфигурации DNS

Существует множество вариантов настройки DNS. Перед настройкой сервера DNS нужно заранее продумать, какие функции он будет выполнять в сети. Кроме того, необходимо предварительно спланировать структуру сети, нагрузку на сервер и параметры его защиты. Дополнительная информация о планировании конфигурации сервера DNS приведена в следующих разделах:

“Определение прав доступа для работы с DNS”
Администратору сервера DNS должны быть предоставлены особые права доступа. Следует тщательно продумать, какие именно права доступа можно предоставить администратору без ущерба для защиты сервера. В этом разделе описаны требования, которые необходимо учесть при выборе прав доступа.

“Определение структуры домена”
Перед настройкой домена необходимо определить, каким образом он будет разбит на области.

“Планирование мер защиты” на стр. 22
В службе DNS предусмотрен ряд средств защиты, позволяющих ограничить доступ внешних пользователей к серверу. В этом разделе описаны как сами средства защиты, так и их применение для управления доступом.

Определение прав доступа для работы с DNS

При настройке сервера DNS следует принять меры по защите конфигурации сервера. Укажите, каким пользователям разрешено изменять эту конфигурацию.

Для настройки и обслуживания сервера DNS администратору системы iSeries(TM) достаточно минимальных прав доступа. Если администратору будут предоставлены права доступа ко всем объектам, то он сможет выполнять любые задачи по администрированию сервера DNS. Пользователям, отвечающим за настройку сервера DNS, рекомендуется предоставить права администратора защиты и права доступа ко всем объектам (*ALLOBJ). Для предоставления этих прав доступа воспользуйтесь Навигатором. За дополнительной информацией по этому вопросу обратитесь к разделу **Предоставление прав доступа администратору сервера DNS** электронной справки по серверу DNS.

Примечание: Если профайлу администратора не предоставлены права доступа ко всем объектам, то ему должны быть предоставлены права доступа ко всем “Работа с файлами конфигурации DNS” на стр. 31.

Определение структуры домена

Заранее спланируйте, каким образом домен или субдомен будет разделен на области, каким образом лучше обрабатывать запросы, будет ли сервер DNS подключен к Internet, и каким образом сервер DNS будет работать через брандмауэр. Последовательно рассмотрите несколько вариантов настройки сервера. За более подробными сведениями обратитесь к дополнительным источникам информации, например, к книге “Дополнительная информация о DNS” на стр. 38.

Если вы создадите динамическую область, вы не сможете обновлять эту область во время работы сервера. Это может привести к конфликту с поступившими запросами на динамическое обновление. Для внесения изменений вручную остановите сервер, обновите информацию об области, а затем перезапустите сервер. При этом запросы на динамическое обновление, полученные во время простоя сервера DNS, обработаны не будут. По этой причине рекомендуется настроить две области: статическую и динамическую. Для этого нужно создать две отдельные области или определить субдомен для тех клиентов, записи о которых будут обновляться динамически, например, dynamic.mycompany.com.

Для настройки серверов DNS системы iSeries(TM) предусмотрен графический интерфейс. Названия некоторых объектов в этом интерфейсе отличаются от тех, которые принято использовать в других публикациях. Если при планировании конфигурации DNS вы будете обращаться к другим источникам информации, учтите следующее:

- Все области и объекты, определенные на сервере, расположены в папках **Области прямого преобразования** и **Области обратного преобразования**. Области прямого преобразования применяются для преобразования имен хостов в IP-адреса, например, с помощью записей типа A. Области обратного преобразования применяются для преобразования IP-адресов в имена хостов, например, с помощью записей PTR.
- На сервере DNS системы iSeries могут быть определены **основные** и **вспомогательные области**. В другой документации по стандарту BIND такие области иногда называются главными и подчиненными.
- Термин **подобласть** аналогичен субдомену. Дочерней областью называется подобласть, права на управление которой переданы одному или нескольким серверам имен.

Планирование мер защиты

Необходимо тщательно спланировать меры по защите сервера DNS. Помимо перечисленных ниже разделов с рекомендациями по защите, существует множество других источников информации о защите сервера DNS и системы iSeries(TM). В частности, такая информация приведена в разделе IBM(R) Secureway: iSeries и Internet справочной системы Information Center. Подробную информацию о защите DNS можно найти в книге “Дополнительная информация о DNS” на стр. 38.

Списки адресов для сравнения

Список адресов для сравнения применяется сервером DNS для управления доступом внешних клиентов к некоторым функциям DNS. В таком списке могут быть заданы IP-адреса, адреса подсети (с помощью префикса IP), либо ключи Подписи транзакции (TSIG). В списке адресов для сравнения перечисляются объекты, которым разрешен или запрещен доступ к функциям сервера. Если вы планируете многократно использовать список адресов для сравнения, сохраните его как список управления доступом (ACL). Если вам впоследствии потребуется этот список, вам нужно будет указать только имя ACL.

Порядок элементов в списке адресов для сравнения

Всегда применяется тот элемент списка адресов для сравнения, который был найден первым. Следовательно, для того чтобы разрешить доступ для всех хостов сети 10.1.1.x, за исключением 10.1.1.5, элементы в списке должны быть расположены в следующем порядке: (!10.1.1.5; 10.1.1/24). В этом случае для адреса 10.1.1.5 первой будет найдена запись, запрещающая доступ.

Если элементы будут стоять в обратном порядке (10.1.1/24; !10.1.1.5), то для IP-адреса 10.1.1.5 первой будет найдена запись, разрешающая доступ. Поскольку остальные записи списка не проверяются, хосту будет разрешен доступ к функции сервера.

Опции управления доступом

Сервер DNS позволяет настроить ряд ограничений доступа, в частности, задать список клиентов, которым разрешено отправлять запросы на динамическое обновление, запрашивать информацию и загружать информацию об области. Для ограничения доступа к серверу с помощью списков управления доступом предусмотрены следующие опции:

allow-update
Включите эту опцию, для того чтобы сервер DNS принимал запросы на динамическое обновление информации от внешних клиентов.

allow-query
Указывает, каким хостам разрешено отправлять запросы к этому серверу. По умолчанию доступ к серверу предоставляется всем хостам.

allow-transfer
Указывает, каким хостам разрешено загружать информацию об области с сервера. По умолчанию это разрешено всем хостам.

allow-recursion
Указывает, каким хостам разрешено отправлять рекурсивные запросы данному серверу. По умолчанию это разрешено всем хостам.

blackhole
Задает список адресов хостов, от которых сервер не принимает запросы и которым сервер не пересылает запросы для обработки. Сервер не отвечает на запросы, поступающие от указанных хостов.

Ресурсы, необходимые для работы с DNS

Компонент DNS (компонент 31) не устанавливается автоматически вместе с базовой операционной системой. Вы должны самостоятельно установить DNS. Новая реализация сервера DNS, предусмотренная в версии V5R1, основана на стандарте BIND 8. В предыдущих выпусках OS/400(R) сервер DNS был основан на стандарте BIND 4.9.3. Этот стандарт по-прежнему поддерживается в версии V5R1.

После установки службы DNS по умолчанию вам будет предоставлена возможность создать один сервер DNS, основанный на стандарте BIND 4.9.3, который поддерживался и в предыдущих версиях. Для того чтобы создать один или несколько серверов DNS, основанных на стандарте BIND 8, необходимо установить продукт Portable Application Solutions Environment (PASE). Продукт PASE - это компонент 33 программы SS1. После установки PASE Навигатор автоматически настроит сервер на основе правильной реализации BIND.

Стандарт BIND 8 предоставляет много дополнительных возможностей, для применения которых нужно установить функцию PASE. Если вы не планируете устанавливать функцию PASE, вы можете продолжить работу с сервером DNS, основанным на BIND 4.9.3, который применялся в предыдущем выпуске. Документация по BIND 4.9.3 приведена в разделе DNS справочной системы Information Center V4R5  (примерно 357 Кб).

Если вы планируете настроить в другой системе iSeries сервер DHCP, который будет динамически обновлять информацию на локальном сервере DNS, то в ней необходимо установить компонент 31. Для динамического обновления информации сервер DHCP применяет программные интерфейсы, которые предоставляются компонентом 31.

Для того чтобы узнать, установлена ли служба DNS в системе, выполните следующие действия:

1. В командной строке введите **GO LICPGM** и нажмите **Enter**.
2. Введите **10** (Показать установленные лицензионные программы) и нажмите **Enter**.
3. Найдите запись **5722SS1 OS/400 - Domain Name System** (Компонент 31 SS1)
   Если служба DNS установлена, то в поле **Состояние** будет указано значение ***COMPATIBLE**, как показано ниже:

```
Программа   Состояние          Описание
5722SS1    *COMPATIBLE         OS/400 - Domain Name System
```

4. Для выхода из меню нажмите **F3**.

Для установки DNS выполните следующие действия:

1. В командной строке введите **GO LICPGM** и нажмите **Enter**.
2. Введите **11** (Установить лицензионные программы) и нажмите **Enter**.

3. В поле **Опция** напротив записи OS/400 - Domain Name System введите **1** (Установить) и нажмите **Enter**.
4. Нажмите **Enter** еще раз для подтверждения установки.

Настройка сервера DNS

Перед настройкой сервера DNS ознакомьтесь со “Ресурсы, необходимые для работы с DNS” на стр. 23 и установите все требуемые компоненты DNS. Инструкции по настройке сервера DNS приведены в следующих разделах:

“Работа с сервером DNS в Навигаторе”
Содержит инструкции по работе с сервером DNS с помощью Навигатора.

“Настройка серверов имен” на стр. 25
Вы можете создать несколько экземпляров серверов имен. В этом разделе приведены инструкции по настройке сервера имен.

“Настройка функции динамического обновления на сервере DNS” на стр. 26
Серверы DNS, поддерживающие BIND 8, могут принимать запросы на динамическое обновление информации об области от различных служб. В этом разделе приведены инструкции по настройке функции динамического обновления на сервере DNS.

“Импорт файлов DNS” на стр. 27
На сервер DNS можно импортировать файлы с информацией об областях. В этом разделе описана процедура создания области на основе существующего файла конфигурации, позволяющая значительно сэкономить время при создании области.

“Получение информации от внешних серверов DNS” на стр. 28
Сервер DNS может отвечать на запросы о той области, которая для него создана. В этом разделе описано, каким образом можно настроить сервер DNS, чтобы он мог отвечать на запросы, не относящиеся к его домену.

Работа с сервером DNS в Навигаторе

Ниже приведены инструкции по работе с интерфейсом для настройки DNS, предусмотренным в Навигаторе.Если вы применяете функцию PASE, то вы сможете настроить серверы DNS с учетом возможностей, предусмотренных в стандарте BIND 8. Если функция PASE не применяется, вы сможете работать с сервером DNS, основанным на BIND 4.9.3, как и в предыдущих выпусках. Информация о работе с серверами DNS на основе BIND 4.9.3 приведена в разделе DNS справочной системы Information Center V4R5  (примерно 60 страниц).

Если вы впервые настраиваете сервер DNS, выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries** —> **Сеть** —> **Серверы** —> **DNS**.
2. Щелкните правой кнопкой мыши на пункте **DNS** и выберите **Создать конфигурацию**.

Если в системе уже есть сервер DNS, применявшийся в одном из предыдущих выпусков, выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries** —> **Сеть** —> **Серверы** —> **DNS**.
2. В правой панели дважды щелкните на значке сервера DNS. Появится окно **Конфигурация сервера DNS**.
3. Если в системе применяется функция PASE, вам будет предложено преобразовать существующую конфигурацию сервера DNS в конфигурацию, поддерживающую BIND 8. Учтите, что после такого преобразования вы не сможете восстановить исходную конфигурацию,

основанную на BIND 4.9.3. Если вы не знаете, нужно ли преобразовывать конфигурацию, выберите значение **Нет**. Для того чтобы преобразовать конфигурацию, выберите значение **Да**.

4. Для того чтобы позднее преобразовать конфигурацию сервера DNS в конфигурацию, поддерживающую BIND 8, щелкните правой кнопкой мыши на значке **DNS**, расположенном в левой панели, и выберите опцию **Преобразовать к версии 8**.

Настройка серверов имен

В системе iSeries(TM) служба DNS основана на стандарте BIND 8, поэтому она позволяет создать несколько экземпляров серверов имен. Ниже описана процедура создания экземпляра сервера имен, включающая настройку свойств и областей сервера.

1. “Создание экземпляра сервера имен”
   Для выполнения этой задачи предусмотрен мастер **Создать конфигурацию DNS**.
2. “Настройка свойств сервера DNS” на стр. 26
   Задайте глобальные свойства нового экземпляра сервера.
3. “Настройка областей сервера имен” на стр. 26
   Создайте области, за которые будет отвечать сервер имен, и добавьте в них записи.

Для того чтобы создать дополнительный экземпляр сервера, повторите описанную выше процедуру. Свойства экземпляров сервера не обязательно должны совпадать - для каждого из них вы можете задать свой уровень отладки, опцию автоматического запуска и т.д. Для каждого экземпляра сервера создаются свои файлы конфигурации. Дополнительная информация об этих файлах приведена в разделе “Работа с файлами конфигурации DNS” на стр. 31.

Создание экземпляра сервера имен

Для запуска мастера **Создать конфигурацию сервера DNS** выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries(TM)** —> **Сеть** —> **Серверы** —> **DNS**.
2. В левой панели щелкните правой кнопкой мыши на пункте **DNS** и выберите опцию **Создать сервер имен...**
3. Выполните инструкции мастера по настройке сервера.

В окнах мастера потребуется указать следующие значения:

Имя сервера DNS: Введите имя сервера DNS. Оно может содержать не более 5 символов, первым из которых должна быть буква. Если вы планируете создать несколько серверов, присвойте им различные имена. Иногда это имя называют именем ″экземпляра″ сервера DNS.

IP-адреса для приема запросов: Наборы IP-адресов серверов DNS не должны пересекаться. По умолчанию сервер работает со всеми IP-адресами. Однако если в системе будет работать несколько экземпляров серверов, ни один из них не должен работать со всеми адресами. В этом случае для каждого сервера необходимо указать свой список IP-адресов.

Корневые серверы: Загрузите список корневых серверов Internet по умолчанию, либо укажите собственные корневые серверы, например, внутренние корневые серверы для своей корпоративной сети.
Примечание: Список корневых серверов Internet следует загружать только в том случае, если сервер подключен к Internet и будет применяться для получения произвольных имен Internet.

Запуск сервера: Укажите, следует ли автоматически запускать сервер вместе с TCP/IP. Если в системе создано несколько экземпляров сервера, каждый из них запускается и останавливается независимо от остальных.

Дальнейшие действия: “Настройка свойств сервера DNS” на стр. 26.

Настройка свойств сервера DNS

Во время создания сервера имен вы можете настроить его свойства, в том числе разрешить обновление информации на сервере и задать уровни отладки. Эти значения относятся только к тому экземпляру сервера, с которым вы в данный момент работаете. Для того чтобы изменить свойства экземпляра сервера DNS, выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries(TM)** —> **Сеть** —> **Серверы** —> **DNS**.
2. В правой панели щелкните правой кнопкой мыши на **значке сервера DNS** и выберите пункт **Конфигурация**.
3. Щелкните правой кнопкой мыши на пункте **Сервер DNS** и выберите опцию **Свойства**.

Дальнейшие действия: “Настройка областей сервера имен”.

Настройка областей сервера имен

После создания сервера имен перейдите в главное окно **Навигатора**. В правой панели будет указано имя созданного сервера. Для того чтобы настроить области этого сервера, щелкните правой кнопкой мыши на имени сервера и выберите пункт **Конфигурация**. Появится окно **Конфигурация DNS**.

Настройка всех областей выполняется с помощью мастеров. Создайте **область прямого** или **обратного преобразования**, щелкнув правой кнопкой мыши на соответствующей папке. Появится окно со списком типов областей. Выберите тип области, которую вы хотите создать, - будет запущен мастер создания этой области.

Описания типов объектов, которые можно создать для сервера DNS в выпуске V5R1, приведено в разделе “Основные сведения о DNS” на стр. 11.

После создания областей ознакомьтесь с перечисленными ниже разделами, в которых приведена дополнительная информация о настройке областей:

“Настройка функции динамического обновления на сервере DNS”
Некоторым внешним серверам можно разрешить динамически обновлять информацию об области путем отправки записей о ресурсах. Это позволит сократить число записей, которые придется обновлять вручную.

“Импорт файлов DNS” на стр. 27
Вы можете загрузить на свой сервер файл с информацией об области, хранящийся на другом сервере DNS.

“Получение информации от внешних серверов DNS” на стр. 28
Сервер может применяться для обработки запросов, не относящихся к тем областям, которые хранятся на этом сервере. Такие запросы могут передаваться другим серверам, ответственным за требуемую область, либо корневым серверам из имеющегося списка.

Настройка функции динамического обновления на сервере DNS

При создании динамических областей следует учесть структуру сети. Если некоторые компоненты домена по-прежнему будут обновляться вручную, рекомендуется поделить домен на статическую и динамическую области. Для того чтобы вручную обновить динамическую область, вам потребуется остановить сервер, отвечающий за эту область, и перезапустить его после внесения всех изменений. При завершении работы сервера выполняется синхронизация всех динамических обновлений, внесенных с момента загрузки информации об области из базы данных. Если вы внесете изменения, не завершая работу сервера, то будут утеряны все динамические изменения, внесенные с момента запуска сервера. Однако завершив работу сервера, вы рискуете потерять те динамические обновления, которые были сделаны во время простоя сервера.

Динамическая область отличается от остальных тем, что в ней определены объекты в операторе allow-update. Для того чтобы определить такие объекты, выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries** —> **Сеть** —> **Серверы** —> **DNS**.
2. В правой панели щелкните правой кнопкой мыши на **значке сервера DNS** и выберите пункт **Конфигурация**.
3. В окне **Конфигурация DNS** разверните значок **Область прямого преобразования** или **Область обратного преобразования**.
4. Щелкните правой кнопкой мыши на основной области, в которую нужно внести изменения, и выберите пункт **Свойства**.
5. На странице **Свойства основной области** щелкните на вкладке **Опции**.
6. На странице **Опции** разверните **Управление доступом** —> **allow-update**.
7. Для проверки запросов на обновление сервер DNS применяет список адресов для сравнения. Для добавления объектов в этот список выберите тип элемента списка и нажмите кнопку **Добавить...**. Вы можете добавить IP-адрес, префикс IP, список управления доступом или ключ.
8. После изменения списка адресов для сравнения нажмите кнопку **OK**, чтобы закрыть окно **Опции**.

Если вы планируете применять функцию динамического обновления информации DNS для работы с сервером DHCP системы iSeries, ознакомьтесь с разделом Настройка функции динамического обновления на сервере DHCP.

Импорт файлов DNS

Основную область можно создать путем импорта файла с информацией об области или путем преобразования существующих таблиц хостов. Для того чтобы узнать, как преобразовать таблицу хостов в файл с информацией об области, обратитесь к разделу *Преобразование таблиц хостов* справочной системы Information Center (примерно 357 Кб).

Для импорта можно выбрать любой файл конфигурации области, поддерживающий синтаксис BIND. Этот файл должен быть расположен в каталоге IFS. После импорта файла с информацией об области DNS проверит, что он не содержит ошибок, и добавит его имя в файл NAMED.CONF для соответствующего экземпляра сервера.

Для того чтобы импортировать файл с информацией об области, выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries(TM)** —> **Сеть** —> **Серверы** —> **DNS**.
2. На правой панели дважды щелкните на значке экземпляра сервера DNS, для которого нужно импортировать область.
3. В левой панели щелкните правой кнопкой мыши на значке **сервера DNS** и выберите опцию **Импортировать область**.
4. Выполните инструкции мастера по импорту основной области.

Проверка записей

Функция Импортировать данные домена проверяет все записи импортируемого файла. Неправильные записи можно исправить по окончании импорта, перейдя на страницу свойств **Прочие записи** импортированной области.

- **Примечание:**
- Импорт большого основного домена может занять несколько минут.
- Функция импорта данных домена не поддерживает директиву $include. При проверке строки с директивой $include считаются неправильными.

Получение информации от внешних серверов DNS

Корневые серверы необходимы для работы сервера DNS, напрямую подключенного к Internet или большой внутренней сети. Для ответа на запросы о хостах, не входящих в его домен, сервер DNS обращается к корневому серверу.

В сети Internet, если серверу DNS нужно получить дополнительную информацию, он обращается к корневым серверам. Корневые серверы передают запрос сервера DNS выше по иерархической структуре до тех пор, пока нужная информация не будет найдена или не выяснится, что она отсутствует.

Стандартные корневые серверы программы **Навигатор iSeries(TM)**.
Корневые серверы должны применяться в том случае, если система подключена к Internet, и вы хотите, чтобы сервер DNS отправлял в Internet запросы о хостах, которые он не может обработать самостоятельно. В программе Навигатор определен ряд корневых серверов Internet, применяемых по умолчанию. Список серверов был текущим на момент выпуска Навигатора. Для того чтобы убедиться, что этот список не устарел, сравните его со списком серверов, приведенном на Web-сайте InterNIC. При необходимости обновите список корневых серверов.

Получение адресов корневых серверов Internet
Адреса корневых серверов иногда меняются, и обновление их списка на сервере локального домена является обязанностью администратора DNS. Текущий список адресов корневых серверов Internet расположен на сайте InterNIC. Для получения этого списка выполните следующие действия:

1. Подключитесь к серверу InterNIC по протоколу FTP как анонимный пользователь:
   `FTP.RS.INTERNIC.NET`
2. Загрузите файл `/domain/named.root`
3. Сохраните файл в каталоге `Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE`.

Сервер DNS, защищенный брандмауэром, может работать без корневых серверов. Такой сервер DNS отвечает на запросы, пользуясь только записями из собственной базы данных основного домена и кэша. Запросы, касающиеся внешних сайтов, он может отправлять серверу DNS, расположенному на брандмауэре, где должен быть установлен сервер пересылки.

Внутренние корневые серверы
Если сервер DNS расположен в большой внутренней сети, то рекомендуется настроить внутренние корневые серверы. Если сервер DNS не будет обращаться к серверам Internet, то список серверов Internet по умолчанию загружать не нужно. Вместо этого необходимо задать имена внутренних корневых серверов, с помощью которых сервер DNS будет выполнять запросы о хостах, не относящихся к его домену.

Работа с DNS

После настройки сервера DNS ознакомьтесь со следующими разделами:

“Проверка работы сервера DNS с помощью команды NSLookup” на стр. 29
С помощью команды NSLookup можно убедиться, что сервер DNS активен.

“Работа с секретными ключами” на стр. 29
Вы можете ограничить доступ к данным DNS с помощью секретных ключей.

“Статистическая информация о сервере DNS” на стр. 30
Для получения информации о работе сервера и его производительности создайте дамп базы данных или воспользуйтесь средствами сбора статистики.

“Работа с файлами конфигурации DNS” на стр. 31
В этом разделе описаны служебные файлы сервера DNS и приведены рекомендации по обслуживанию этих файлов (в том числе, по резервному копированию).

“Дополнительные функции DNS” на стр. 33
В этом разделе приведена информация о работе с дополнительными функциями, предназначенная для опытных пользователей.

Проверка работы сервера DNS с помощью команды NSLookup

Запросите у сервера DNS IP-адрес с помощью команды NSLookup. Это позволит убедиться в том, что сервер DNS отвечает на запросы. Запросите имя хоста, связанное с циклическим IP-адресом (127.0.0.1). Вы должны получить имя хоста localhost. Кроме того, проверьте, что сервер правильно отвечает на запросы о получении имен хостов, определенных в записях сервера. Там самым вы убедитесь, что экземпляр сервера работает правильно.

Для проверки работы сервера DNS с помощью команды NSLookup выполните следующие действия:

1. Введите в командной строке `NSLOOKUP DMNNAMSVR(n.n.n.n)`, где n.n.n.n - адрес, указанный в конфигурации экземпляра сервера.
2. Введите в командной строке `NSLOOKUP` и нажмите **Enter**. Будет открыт сеанс работы с NSLookup.
3. Введите команду `server` и имя сервера, а затем нажмите **Enter**. Например: `server myiseries.mycompany.com`.
   Будет показана следующая информация:

   ```
   Server:  myiseries.mycompany.com
   Address:  n.n.n.n
   ```

   Вместо `n.n.n.n` будет указан IP-адрес сервера DNS.
4. Введите в командной строке `127.0.0.1` и нажмите **Enter**.
   Должна быть показана следующая информация, содержащая имя хоста с циклическим адресом:

   ```
    > 127.0.0.1
   Server:  myiseries.mycompany.com
   Address:  n.n.n.n

   Name:    localhost
   Address:  127.0.0.1
   ```

   Правильный ответ сервера должен содержать имя **localhost** в качестве имени хоста с циклическим адресом.
5. Введите `exit` и нажмите **Enter**. Сеанс NSLOOKUP будет закрыт.

Примечание: Для получения справки по команде NSLookup введите ? и нажмите **Enter**.

Работа с секретными ключами

В службе DNS применяются ключи двух типов. Каждый из них играет свою роль для защиты конфигурации сервера DNS. Ниже приведена информация о применении этих ключей для защиты сервера DNS.

Ключи DNS

Ключ DNS - это ключ, определенный для стандарта BIND. Он применяется сервером DNS при проверке запросов на обновление информации. Вы можете задать ключ и присвоить ему имя. Для того чтобы настроить защиту объекта DNS, например, динамической области, укажите этот ключ в Списке адресов для сравнения.

Для работы с ключами DNS выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries(TM)** —> **Сеть** —> **Серверы** —> **DNS**.

2. В правой панели щелкните правой кнопкой мыши на имени экземпляра сервера DNS и выберите пункт **Конфигурация**.
3. В окне **Конфигурация DNS** выберите **Файл** > **Работа с ключами...**

Ключи для динамического обновления
Ключи для динамического обновления применяются сервером DHCP, выполняющим динамическое обновление информации об области. Эти ключи используются, когда серверы DNS и DHCP установлены в одной системе iSeries. Если сервер DHCP расположен в другой системе iSeries, то для применения функции динамического обновления вам нужно создать одинаковые ключи для динамического обновления в обеих системах iSeries.

Для работы с ключами для динамического обновления выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries** —> **Сеть** —> **Серверы** —> **DNS**.
2. Щелкните правой кнопкой мыши на пункте **DNS** и выберите опцию **Работа с ключами для динамического обновления...**

Статистическая информация о сервере DNS

Сервер DNS предоставляет несколько средств диагностики. С их помощью можно получить информацию о работе сервера.

Статистическая информация о сервере
Служба DNS позволяет получить статистическую информацию о работе экземпляра сервера. Эта информация содержит итоговое число запросов и ответов, полученных сервером с момента его запуска или загрузки его базы данных. Файл статистики непрерывно пополняется. С помощью этой информации можно получить представление о нагрузке на сервер и найти причину ошибки. Дополнительная информация о статистике работы сервера приведена в разделе **Статистическая информация о сервере DNS** электронной справки по серверу DNS.

Для просмотра статистики работы сервера выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries(TM)** —> **Сеть** —> **Серверы** —> **DNS**.
2. В правой панели щелкните правой кнопкой мыши на **значке сервера DNS** и выберите пункт **Конфигурация**.
3. В окне **Конфигурация сервера DNS** выберите **Показать** —> **Статистика работы сервера**.

База данных активного сервера
Служба DNS позволяет просмотреть дамп области ответственности, кэша и подсказок экземпляра сервера. Такой дамп содержит информацию обо всех основных и вспомогательных областях прямого и обратного преобразования, а также сведения, полученные сервером из ответов на запросы. База данных содержит информацию об области и хосте, в том числе некоторые свойства области (например, начало области ответственности (SOA)) и хоста (например, система обмена почтой (MX)). Эта информация применяется для анализа неполадок.

Дамп базы данных активного сервера можно просмотреть с помощью Навигатора. Дамп базы данных сохраняется в файле NAMED_DUMP.DB, расположенном в следующем каталоге системы iSeries: **Integrated File System**/**Root**/**QIBM**/**UserData**/**OS400**/**DNS**/**<экземпляр сервера>**, где ″<экземпляр сервера>″ - это имя экземпляра сервера DNS. За дополнительной информацией о базе данных активного сервера обратитесь к разделу **Дамп базы данных сервера DNS** электронной справки по серверу DNS.

Для просмотра дампа базы данных активного сервера выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries** —> **Сеть** —> **Серверы** —> **DNS**.

2. В правой панели щелкните правой кнопкой мыши на **значке сервера DNS** и выберите пункт **Конфигурация**.
3. В окне **Конфигурация DNS** выберите **Показать** —> **База данных активного сервера**.

Работа с файлами конфигурации DNS

Для создания экземпляров сервера DNS в системе iSeries(TM) и работы с ними применяется функция DNS операционной системы OS/400(R). Функции для работы с файлами конфигурации DNS предусмотрены в Навигаторе. Не рекомендуется редактировать эти файлы вручную. Все операции по созданию, изменению и удалению файлов конфигурации DNS нужно выполнять только с помощью Навигатора. Ниже перечислены каталоги Интегрированной файловой системы, в которой хранятся файлы конфигурации DNS.

Примечание: Приведенная ниже структура файлов относится к серверу DNS, поддерживающему BIND 8. Если вы работаете с сервером DNS на основе BIND 4.9.3, обратитесь к разделу *Сохранение файлов конфигурации DNS и работа с файлами протоколов* справочной системы Information Center V4R5 (примерно 60 страниц).

В приведенной ниже таблице описана иерархия каталогов, в которых расположены файлы конфигурации. Файлы, отмеченные значком , необходимо регулярно сохранять для защиты данных. Файлы, отмеченные значком , необходимо регулярно удалять.

Имя		**Описание**
QIBM/UserData/OS400/DNS/		Начальный каталог DNS.
ATTRIBUTES		С помощью этого файла сервер DNS определяет поддерживаемую версию BIND.
QIBM/UserData/OS400/DNS/<*экземпляр-n*>/		Начальный каталог для экземпляра сервера.
ATTRIBUTES		Содержит параметры конфигурации сервера DNS, установленного в системе iSeries.
NAMED.CONF		Этот файл содержит информацию о конфигурации. В нем перечислены области, за которые отвечает сервер, задано расположение файлов с информацией об областях, указаны области, для которых разрешено динамическое обновление, адреса серверов пересылки и другие параметры.

Имя		Описание
BOOT.AS400BIND4		Этот файл содержит параметры конфигурации и стратегии сервера BIND 4.9.3. На его основе был создан файл NAMED.CONF для данного экземпляра сервера, поддерживающего BIND 8. Этот файл создается при переходе от сервера BIND 4.9.3 к серверу BIND 8. Он служит резервной копией старой конфигурации, к которой при необходимости можно вернуться. После того как вы проверите правильность работы сервера BIND 8, этот файл можно удалить.
NAMED.CA		Список корневых серверов для данного экземпляра сервера.
NAMED_DUMP.DB		Дамп “Статистическая информация о сервере DNS” на стр. 30.
NAMED.STATS		“Статистическая информация о сервере DNS” на стр. 30.
NAMED.PID		В этом файле хранится ИД процесса, связанный с активным сервером. Этот файл создается при каждом запуске сервера DNS. Он необходим для работы таких функций сервера, как База данных, Статистика и Обновить сервер. Не удаляйте и не изменяйте этот файл.
QUERYLOG		Протокол запросов, полученных сервером DNS. Этот файл создается, если включен протокол сервера DNS. Размер этот файла быстро увеличивается, поэтому его нужно регулярно удалять.
<имя-области-a>.DB		Файл с информацией об области, связанный с доменом, который будет обслуживаться данным сервером. Этот файл содержит все записи о ресурсах, относящиеся к области.
<имя-области-b>.DB		Файл с информацией об области, связанный с доменом, который будет обслуживаться данным сервером. Этот файл содержит все записи о ресурсах, относящиеся к области. Для каждой области создается отдельный файл .DB.

Имя		Описание
.ixfr.		Файлы с информацией для передачи измененной информации об области (IXFR). Эти файлы применяются вспомогательными серверами для загрузки измененной информации об области. При каждом обновлении информации создается очередной файл IXFR. Периодически удаляйте старые файлы IXFR. Для работы вспомогательных серверов достаточно сохранять файлы, созданные за последние один-два дня. Если вы удалите все файлы, то вспомогательному серверу потребуется загрузить полную информацию об области (AXFR).
TMP		Каталоги, которые применяются экземпляром сервера для хранения временной информации.
QIBM/UserData/OS400/DNS/TMP		Временный каталог, применяемый программой QTOBH2N для создания промежуточной версии файлов дампа таблицы хостов, которые затем будут импортированы в Навигатор.
QIBM/UserData/OS400/DNS/_DYN/		Этот каталог содержит файлы, необходимые для динамического обновления данных.
<имя-ид_ключа-x>._KID		Этот файл содержит оператор для ключа BIND 8 с именем *<имя-ключа-x>*.
<имя-ид_ключа-x>._DUK.*<имя-области-a>*		Ключ, необходимый для динамического обновления информации об *<области-a>* с помощью ключа с именем *<имя-ключа-x>*.
<имя-ид_ключа-y>._KID		Этот файл содержит оператор для ключа BIND 8 с именем *<имя-ключа-y>*.
<имя-ид_ключа-y>._DUK.*<имя-области-a>*		Ключ, необходимый для динамического обновления информации об *<области-a>* с помощью ключа с именем *<имя-ключа-y>*.
<имя-ключа-y>._DUK.*<имя-области-b>*		Ключ, необходимый для динамического обновления информации об *<области-b>* с помощью ключа с именем *<имя-ключа-y>*.

Дополнительные функции DNS

В программе Навигатор предусмотрен интерфейс для настройки сервера DNS и работы с ним. Ниже приведена краткая информация о выполнении некоторых процедур, предназначенная для тех

администраторов, кто уже знаком с графическим интерфейсом для работы с системой iSeries. В частности, здесь описаны эффективные способы изменения состояния и атрибутов сразу нескольких экземпляров серверов.

Изменение атрибутов сервера DNS
В интерфейсе для работы с DNS не предусмотрена возможность одновременного изменения параметров автоматического запуска и уровня отладки для всех экземпляров сервера. Параметры отдельного экземпляра сервера или всех серверов можно изменить с помощью текстового интерфейса. Для этого вызовите команду CHGDNSA:

1. В командной строке введите `CHGDNSA` и нажмите **F4**.
2. На странице Изменить атрибуты сервера DNS (CHGDNSA) введите имя экземпляра сервера или значение `*ALL` и нажмите **Enter**.

   Появится список атрибутов сервера:
   ```
   Авт. запуск сервера . . . . . *SAME *YES, *NO, *SAME
   Уровень отладки . . . . . *SAME 0-11, *SAME, *DFT
   ```
3. **Автоматический запуск** Для того чтобы выбранные серверы DNS автоматически запускались при запуске TCP/IP, выберите значение `*YES`. Если вы не хотите, чтобы сервер запускался одновременно с TCP/IP, укажите значение `*NO`. Для того чтобы оставить текущее значение параметра, выберите `*SAME`.

   Уровень отладки Для того чтобы изменить уровень отладки для выбранных серверов DNS, введите значение от 0 до 11. Если в качестве уровня отладки должно устанавливаться значение, применяемое при запуске сервера, введите `*DFT`. Для того чтобы оставить текущее значение параметра, выберите `*SAME`.

   Для сохранения изменений, внесенных в параметры сервера DNS, нажмите **Enter**.

Запуск и завершение работы серверов DNS
Интерфейс для работы с сервером DNS не позволяет запустить или остановить сразу несколько экземпляров сервера. Для выполнения этой задачи воспользуйтесь текстовым интерфейсом. Для того чтобы запустить все экземпляры сервера DNS, введите команду `STRTCPSVR SERVER(*DNS) DNSSVR(*ALL)`. Для того чтобы остановить все экземпляры сервера DNS, введите команду `ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL)`.

Изменение уровня отладки
Интерфейс для работы с DNS, предусмотренный в Навигаторе, не позволяет изменить уровень отладки для активного сервера. Эту задачу можно выполнить с помощью текстового интерфейса. Такая возможность может применяться в том случае, когда информация об области занимает большой объем памяти, и администратор хочет избежать создания излишней отладочной информации при загрузке данных области во время запуска сервера. Для того чтобы изменить уровень отладки с помощью текстового интерфейса, выполните описанные ниже действия, заменив слово <экземпляр> на имя экземпляра сервера:

1. Введите `ADDLIBLE QDNS` в командной строке и нажмите **Enter**.
2. Измените уровень отладки:
   - Для включения отладки увеличьте уровень отладки на 1. Для этого введите команду `CALL QTOBDRVS ('BUMP' '<экземпляр>')` и нажмите **Enter**.
   - Для выключения отладки введите команду `CALL QTOBDRVS ('OFF' '<экземпляр>')` и нажмите **Enter**.

Устранение ошибок DNS

Принцип работы DNS мало отличается от других функций и приложений TCP/IP. Подобно приложениям SMTP и FTP, задания DNS выполняются в подсистеме QSYSWRK и создают протоколы от имени пользовательского профайла QTCP. С помощью протокола вы можете определить причину завершения работы задания DNS. Если сервер DNS отправляет неверные ответы на запросы, то с помощью протоколов задания вы можете определить причину ошибки.

Информация о конфигурации DNS хранится в нескольких файлах, каждый из которых содержит записи определенного типа. Чаще всего неполадки в работе сервера DNS связаны с ошибками в записях, хранящихся в файлах конфигурации. При возникновении неполадки в первую очередь проверьте правильность этих записей.

“Запись в протокол сообщений DNS”
Служба DNS предоставляет несколько параметров ведения протокола, которые можно изменить для обнаружения причины неполадки. Вы можете настроить эти параметры для получения интересующей вас информации о неполадках, выбрав уровень серьезности, категории сообщений и файлы вывода.

“Параметры отладки сервера DNS” на стр. 37
DNS поддерживает 12 уровней отладки. Обычно для обнаружения неполадок создается протокол сообщений, однако в некоторых случаях требуется включить отладку. Обычно отладка выключена (уровень отладки = 0).

“Дополнительная информация о DNS” на стр. 38
Существует много источников информации об устранении стандартных неполадок DNS. Ответы на многие вопросы можно получить из книги ″DNS and BIND″, изданной O’Reilly. Кроме того, обратитесь к каталогу ресурсов по DNS, в котором приведены ссылки на конференции для администраторов DNS.

Правила именования заданий
Если вы решили просмотреть протокол задания (например, с помощью команды WRKACTJOB) и убедиться в правильности работы сервера DNS, обратите внимание на следующие правила именования заданий:

- Заданию сервера, поддерживающего стандарт BIND 4.9.3, присваивается имя QTOBDNS. Более подробную информацию об отладке DNS 4.9.3 вы найдете в разделе *Устранение неполадок сервера DNS* справочной системы DNS Information Center V4R5  (около 357 Кб).
- Если в системе настроены серверы, основанные на стандарте BIND 8, то для каждого из них будет создано отдельное задание. Имена заданий начинаются с префикса QTOBD, за которым следует имя экземпляра сервера. Например, если в системе создано два экземпляра сервера, INST1 и INST2, то для них будут запущены задания QTOBDINST1 и QTOBDINST2.

Запись в протокол сообщений DNS

В стандарте BIND 8 предусмотрено несколько новых параметров ведения протокола. Теперь вы можете выбрать типы сообщений, которые должны заноситься в протокол; протокол, в который должны заноситься сообщения определенного типа; а также уровень серьезности сообщений, которые должны заноситься в протокол. В общем случае рекомендуется оставить для параметров ведения протокола значения по умолчанию. Если вы решите изменить эти значения, предварительно ознакомьтесь с другими “Дополнительная информация о DNS” на стр. 38 о стандарте BIND 8.

Каналы для записи сообщений
Сервер DNS может записывать сообщения в различные каналы вывода. Канал вывода определяет объект, в котором сохраняются сообщения. Существуют каналы вывода следующих типов:

- **Файл**
  При записи сообщения в такой канал оно сохраняется в файле. По умолчанию применяются два канала типа Файл: as400_debug и as400_QPRINT. В канал as400_debug записываются отладочные сообщения. Этот канал соответствует файлу NAMED.RUN. Вы можете выбрать и другие категории сообщений, которые должны записываться в этот канал. Сообщения из канала as400_QPRINT записываются в буферный файл QPRINT, связанный с пользовательским профайлом QTCP. В дополнение к каналам по умолчанию вы можете создать собственные каналы типа Файл.
- **Системный протокол**
  Сообщения из этого канала записываются в протокол задания сервера. По умолчанию применяется канал as400_joblog. Сообщения из этого канала записываются в протокол задания экземпляра сервера DNS.
- **Фиктивный канал**
  Сообщения, заносимые в этот канал, удаляются. По умолчанию применяется фиктивный канал as400_null. В этот канал следует направлять все сообщения, которые не нужно записывать ни в один протокол.

Категории сообщений
Все сообщения разбиты на несколько категорий. Вы можете выбрать категории сообщений, которые будут заноситься в каждый канал записи сообщений. Ниже перечислены некоторые категории сообщений:

- config: Обработка файла конфигурации
- db: Операции над базами данных
- queries: Краткие сообщения, отправляемые сервером при получении запроса
- lame-servers: Обнаружение неверных записей о передаче прав на обслуживание области
- update: Динамическое обновление
- xfer-in: Получение информации об области
- xfer-out: Передача информации об области

Если вы не будете регулярно удалять файлы протоколов, то они могут достигнуть очень больших размеров. При запуске сервера DNS все файлы протоколов очищаются.

Уровень серьезности сообщений
Сообщения, заносимые в канал, могут отфильтровываться в зависимости от их уровня серьезности. Для каждого канала можно задать уровень серьезности сообщений, которые должны записываться в этот канал. Существуют следующие уровни серьезности сообщений:

- Критическая ситуация
- Ошибка
- Предупреждение
- Извещение
- Информация
- Отладка (укажите уровень отладки от 0 до 11)
- Динамический (соответствует уровню отладки, который устанавливается при запуске сервера)

В канал заносятся все сообщения, уровень серьезности которых не ниже указанного. Например, если вы выберете уровень серьезности Предупреждение, то в канал будут записываться сообщения с уровнем серьезности Предупреждение, Ошибка и Критическая ситуация. Если вы выберете уровень серьезности Отладка, укажите уровень отладки от 0 до 11, сообщения для которого должны записываться в канал.

Изменение параметров ведения протокола
Для изменения параметров ведения протокола выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries(TM)** —> **Сеть** —> **Серверы** —> **DNS**.
2. В правой панели щелкните правой кнопкой мыши на **значке сервера DNS** и выберите пункт **Конфигурация**.
3. В окне **Конфигурация сервера DNS** щелкните правой кнопкой мыши на **значке сервера DNS** и выберите пункт **Свойства**.
4. В окне **Свойства сервера** щелкните на вкладке **Каналы**, чтобы создать новые каналы типа Файл или задать свойства канала, например, уровень серьезности сообщений, записываемых в канал.
5. В окне **Свойства сервера** щелкните на вкладке **Ведение протокола** и выберите категории сообщений, которые должны заноситься в тот или иной канал.

Рекомендация
Для канала as400_joblog по умолчанию установлен уровень серьезности Ошибка. При этом в протокол не заносятся информационные сообщения и предупреждения, которые могут значительно увеличить размер протокола, что может отрицательно сказаться на производительности системы. Если в системе возникла неполадка, однако в протоколе задания не указана причина этой неполадки, то рекомендуется изменить уровень серьезности. Для этого перейдите на страницу Каналы, следуя приведенным выше инструкциям, и измените для канала as400_joblog уровень серьезности на Предупреждение, Извещение или Информация. После устранения неполадки восстановите прежний уровень серьезности, для того чтобы сократить число сообщений, заносимых в протокол задания.

Параметры отладки сервера DNS

Функция отладки сервера DNS позволяет получить информацию, полезную для обнаружения и устранения неполадок сервера DNS. Перед включением этой функции попытайтесь определить причину неполадки с помощью протокола.

Сервер поддерживает уровни отладки от 0 до 11. Выбрать правильный уровень отладки для диагностики возникшей неполадки вам помогут в сервисном представительстве фирмы IBM. Если уровень отладки отличен от нуля, то сервер записывает отладочную информацию в файл NAMED.RUN, расположенный в следующем каталоге системы iSeries: **Integrated File System**/**Root**/**QIBM**/**UserData**/**OS400**/**DNS**/**<экземпляр сервера>**, где ″<экземпляр сервера>″ - имя экземпляра сервера DNS. Во время работы сервера DNS с ненулевым уровнем отладки размер файла NAMED.RUN постоянно увеличивается. Рекомендуется время от времени удалять этот файл, чтобы он не занимал слишком много места на диске. На странице **Свойства сервера** - **Каналы** можно задать максимальный размер и число версий файла NAMED.RUN.

Для того чтобы изменить уровень отладки для экземпляра сервера DNS, выполните следующие действия:

1. В окне **Навигатора** разверните **значок своего сервера iSeries** —> **Сеть** —> **Серверы** —> **DNS**.
2. В правой панели щелкните правой кнопкой мыши на **значке сервера DNS** и выберите пункт **Конфигурация**.
3. В окне **Конфигурация сервера DNS** щелкните правой кнопкой мыши на имени сервера DNS и выберите пункт **Свойства**.
4. На странице **Свойства сервера - Общие** укажите начальный уровень отладки сервера.
5. Если сервер активен, перезапустите его.
   Примечание: Изменение уровня отладки вступает в силу только после перезапуска сервера. Указанный на этой странице уровень отладки устанавливается только при запуске сервера. Информация о том, как изменить уровень отладки активного сервера, приведена в разделе “Дополнительные функции DNS” на стр. 33.

Дополнительная информация о DNS

Существует множество других источников информации о DNS и BIND 8. Ниже перечислены лишь некоторые из них:

- DNS and BIND, third edition. Paul Albitz and Cricket Liu. Издательство O'Reilly and Associates,Inc. Sebastopol, California, 1998. ISBN: 1-56592-512-2. Это наиболее авторитетный источник информации о DNS.
- Web-сайт Internet Software Consortium содержит новости, ссылки на другие источники информации и прочие ресурсы, связанные со стандартом BIND.
- Web-сайт InterNIC содержит каталог зарегистрированных имен доменов, утвержденных организацией ICANN.
- Web-сайт DNS Resources Directory содержит справочные материалы по DNS и ссылки на многие другие ресурсы, в том числе на конференции по DNS. Кроме того, здесь можно найти список RFC, относящихся к DNS .

Руководства IBM Redbook(TM)

- AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support

  В этом руководстве подробно описаны серверы DNS и DHCP в операционной системе OS/400(R). Кроме того, здесь на примерах показаны процедуры установки, настройки и устранения неполадок служб DNS и DHCP.
  Примечание: В этом руководстве не описаны новые возможности BIND 8, появившиеся в версии V5R1. Однако в нем подробно рассмотрены основные принципы работы DNS.

Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

```
IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY  10594-1785
U.S.A.
```

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

```
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan
```

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ КАК ЕСТЬ, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

```
IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.
```

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этой информации лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM или любого другого эквивалентного соглашения.

В электронной версии данной документации фотографии и цветные иллюстрации могут отсутствовать.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:
Application System/400
AS/400
e (логотип)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance, и WordPro являются товарными знаками International Business Machines и Lotus Development Corporation в США и/или других странах.

C-bus является товарным знаком Corollary, Inc. в США и/или других странах.

ActionMedia, LANDesk, MMX, Pentium, и ProShare являются товарными знаками или зарегистрированы как товарные знаки корпорации Intel в США и/или других странах.

Microsoft, Windows, Windows NT и логотип Windows являются товарными знаками корпорации Microsoft в США и/или других странах.

SET и логотип SET являются товарными знаками, принадлежащими SET Secure Electronic Transaction LLC.

Java, а также все товарные знаки, включающие слово Java, являются товарным знаком Sun, Inc. в США и/или других странах.

UNIX является зарегистрированным товарным знаком The Open Group в США и/или других странах.

Названия других компаний продуктов и услуг могут быть товарными или служебными знаками других компаний.

Условия загрузки и печати публикаций

Разрешение на использование выбранных для загрузки публикаций предоставляется в соответствии с следующими условиями и при подтверждении вашего с ними согласия.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах.Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать данные публикации в рамках своей организации при условии сохранения информации об авторских правах.Данные публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в том случае, если по мнению IBM использование этих публикаций может принести ущерб интересам IBM или если IBM будет установлено, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта. IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях ″как есть″, без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности или применения для каких-либо конкретных целей.

Загружая или печатая публикации с этого сайта, вы тем самым подтверждаете свое согласие с приведенными условиями.

Напечатано в Дании