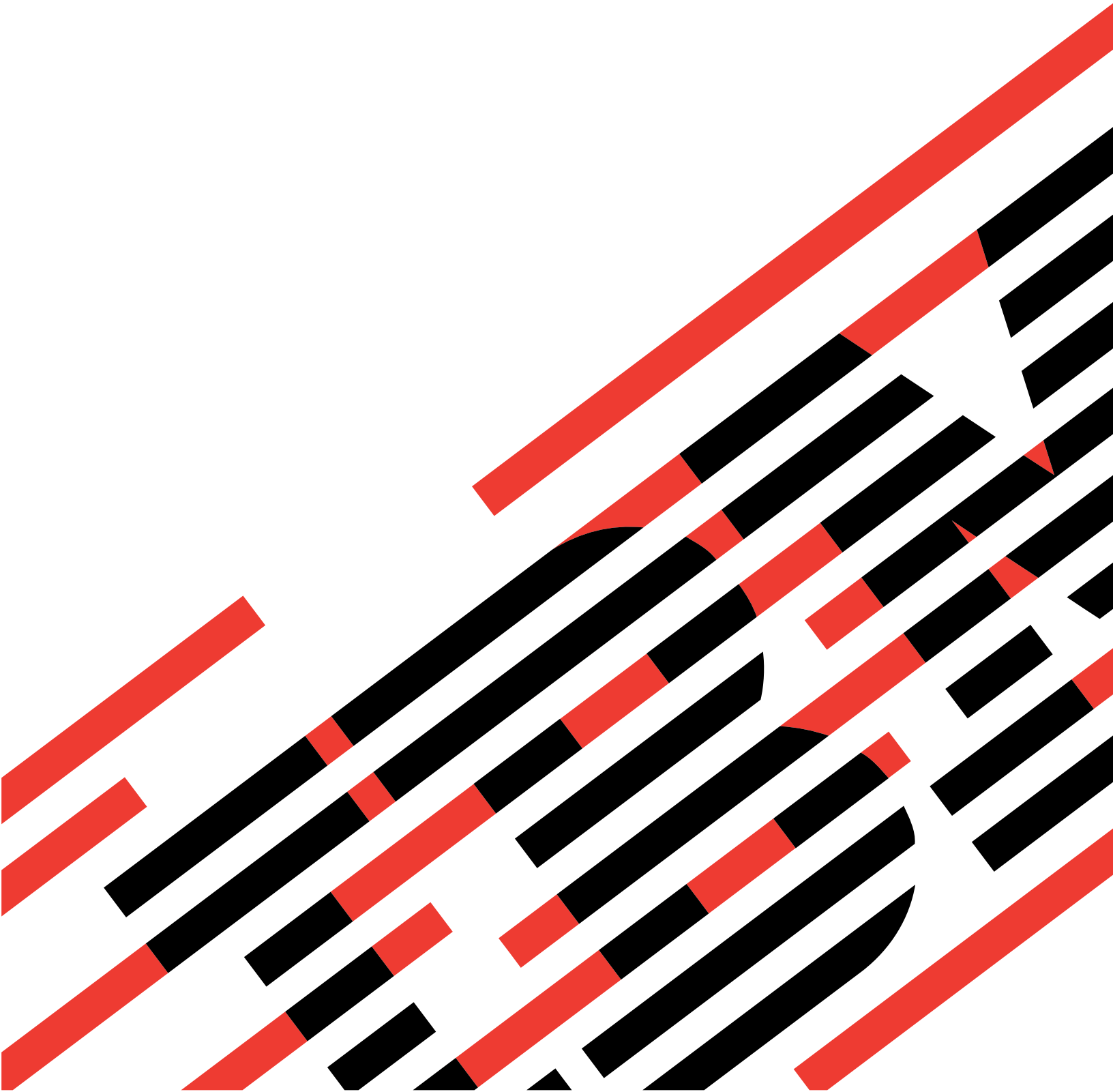
IBM

eserver

iSeries

Сеть - Настройка TCP/IP

Версия 5, выпуск 3



IBM

@server

iSeries

Сеть - Настройка TCP/IP

Версия 5, выпуск 3

Часть 1. Настройка TCP/IP

Вы уже получили заказанный сервер и готовы начать работу с ним. В этом разделе описаны инструменты и процедуры настройки протокола TCP/IP в системе OS/400. Например, с помощью приведенной информации вы сможете создать описание линии, интерфейс TCP/IP или маршрут. Кроме того, этом документе рассказано о настройке TCP/IP с помощью Навигатора iSeries, а также приведены дополнительные сведения о TCP/IP, которые позволят вам управлять потоками данных в вашей сети.

Перед началом настройки TCP/IP ознакомьтесь с разделом Установка и применение аппаратного обеспечения и убедитесь, что установлены все необходимые аппаратные компоненты. Выполнив начальные действия по настройке TCP/IP, вы сможете расширить возможности сервера с помощью приложений, протоколов и служб TCP/IP, что позволит вам успешно решать возникающие задачи.

Новое в выпуске V5R3
Этот раздел содержит информацию о новых и измененных функциях TCP/IP.

Как напечатать этот раздел
В этом разделе приведена информация о том, как напечатать или загрузить документ о настройке TCP/IP в формате PDF.

Протокол Internet версии 6 (IPv6)
Новая версия протокола Internet, IPv6, играет ключевую роль в развитии Internet. Этот протокол может применяться на сервере iSeries. Данный раздел содержит информацию о протоколе IPv6 и его реализации на сервере iSeries.

Планирование настройки TCP/IP
Этот раздел содержит информацию о подготовке к установке и настройке протокола TCP/IP на сервере iSeries. Здесь перечислены основные требования к процедуре установки и настройки. Перед тем как приступить к этой процедуре, вы должны убедиться, что располагаете всей необходимой информацией. Основные термины и понятия снабжены ссылками на их подробное объяснение.

Установка TCP/IP
В этом разделе приведена информация об установке продуктов, необходимых для работы сервера iSeries.

Настройка TCP/IP
Этот раздел содержит инструкции по настройке TCP/IP на сервере iSeries. Дополнительно рекомендуется ознакомиться с информацией о настройке IPv6.

Настройка TCP/IP с помощью Навигатора iSeries
В этом разделе рассказано, какие изменения можно внести в существующую конфигурацию TCP/IP с помощью Навигатора iSeries.

TCP/IP в виртуальной сети Ethernet
В этом разделе приведены сведения возможностях виртуальной сети Ethernet в системе OS/400.

Устранение неполадок TCP/IP
Если при настройке соединения TCP/IP или передаче данных по этому соединению возникнут ошибки, обратитесь к разделу Устранение неполадок TCP/IP за информацией об их исправлении. В этом разделе приведены инструкции по устранению неполадок для обеих версий протокола: IPv4 и IPv6.

Дополнительная информация о настройке TCP/IP
Этот раздел посвящен ответу на вопрос о возможных дополнительных действиях. Приведены ссылки на службы и приложения, позволяющие повысить производительность сервера.

Глава 1. Новое в выпуске V5R3

Дополнительные возможности настройки TCP/IP

Если разделы вашей системы обмениваются данными с помощью виртуальной сети Ethernet, то может возникнуть необходимость и в передаче информации между разделами и внешней сетью. Дополнительная информация о подключении виртуальной сети Ethernet к внешней локальной сети приведена в разделе Подключение виртуальной сети Ethernet к внешним локальным сетям с помощью TCP/IP. Этот документ содержит примеры, иллюстрирующие три различных способа передачи данных между внешними локальными сетями и виртуальной сетью Ethernet.

Сведения о новых возможностях, появившихся в этом выпуске, приведены в разделе Информация для пользователей.

Как получить информацию о новых возможностях и изменениях

Данный документ содержит следующие обозначения, указывающие на внесенные изменения:

- Значок  указывает на начало новой или измененной информации.
- Значок указывает на конец новой или измененной информации.

Глава 2. Как напечатать этот раздел

Для просмотра или загрузки документа в формате PDF (около 362 Кб) щелкните на ссылке Настройка TCP/IP.

Прочая информация

Кроме того, можно просмотреть или напечатать один из следующих документов в формате PDF:

- Справочники:
  - **Справочник по настройке TCP/IP** (592 Кб)
    Эта книга содержит информацию о настройке протокола TCP/IP, а также о работе в сети и об управлении сетью.
  - **Советы по организации защиты iSeries** (1 Мб)
    Данное руководство содержит рекомендации по защите сервера iSeries.
- Руководства по выполнению задач (Redbook):
  - **TCP/IP Tutorial and Technical Overview** (7 Мб)
    Это руководство содержит основную информацию о стеке протоколов TCP/IP.
  - **TCP/IP for AS/400: More Cool Things Than Ever** (9 Мб)
    Это руководство содержит расширенный список стандартных приложений и служб TCP/IP.

Сохранение файлов PDF

Для сохранения документа в формате PDF на рабочей станции:

1. В окне браузера щелкните правой кнопкой мыши на имени документа PDF (на приведенной выше ссылке).
2. Если вы работаете с браузером Internet Explorer, выберите опцию **Сохранить объект как...** Если вы работаете с браузером Netscape Navigator, выберите опцию **Сохранить ссылку как...**
3. Перейдите в каталог, выбранный для хранения документа PDF.
4. Нажмите кнопку **Сохранить**.

Загрузка программы Adobe Acrobat Reader

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

Глава 3. Протокол Internet версии 6 (IPv6)

Протокол Internet версии 6 (IPv6) - это модификация Протокола Internet версии 4 (IPv4), которая постепенно приходит ему на смену в качестве стандарта сети Internet.

Возможно, вам будет интересно узнать о том, каким образом с помощью протокола IPv6 можно повысить эффективность электронного бизнеса или создаваемых вами приложений. Ознакомьтесь с перечисленными ниже разделами, в которых приведена основная информация о протоколе IPv6 и его применении на сервере iSeries:

Что такое IPv6?
Содержит информацию о том, почему протокол IPv6 становится стандартом сети Internet вместо протокола IPv4, и какими особенностями обладает этот протокол.

Функции протокола IPv6
Содержит информацию о текущей реализации протокола IPv6 на сервере iSeries.

Сценарии применения IPv6
В этом разделе приведены примеры применения протокола IPv6 в различных ситуациях.

Принципы работы IPv6
В этом разделе приведена информация об основных принципах работы протокола IPv6. Если вы не знаете, чем отличается протокол IPv4 от IPv6, ознакомьтесь со сравнительным анализом свойств этих протоколов, в частности, адресов и заголовков пакетов.

Настройка протокола IPv6
Этот раздел содержит список программных и аппаратных требований, которые должны быть выполнены для настройки протокола IPv6 на сервере, а также инструкции по настройке.

Устранение неполадок IPv6
Этот раздел содержит рекомендации по устранению неполадок, которые могут возникнуть при работе с протоколом IPv6.

Дополнительная информация об IPv6
Ссылки на дополнительные источники информации о протоколе IPv6.

Что такое IPv6?

Протокол Internet версии 6 (IPv6) - это следующее поколение протокола IP. В настоящее время большинство компьютеров в сети Internet применяют протокол IPv4, который считался достаточно надежным и гибким на протяжении 20 лет. Однако в связи со стремительным ростом сети Internet протокол IPv4 становится все менее удобным из-за предусмотренных в нем ограничений.

Например, в настоящее время уже ощущается недостаток адресов IPv4, которые требуется присваивать всем новым устройствам, подключаемым к сети Internet. Основное достоинство протокола IPv6 заключается в увеличении размера адреса с 32 бит до 128 бит, что дает практически неисчерпаемый запас уникальных IP-адресов. В текстовом формате адреса IPv6 записываются в следующем виде:

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

где x - это шестнадцатеричная цифра, представляющая 4 бита адреса.

Расширенный диапазон адресов протокола IPv6 позволяет решить проблему нехватки адресов. Это особенно важно в связи с тем, что все больше людей начинает использовать мобильные устройства, например,

мобильные телефоны и карманные компьютеры. Стремительное увеличение числа беспроводных устройств приводит к дальнейшему исчерпанию запаса адресов IPv4. За счет применения IP-адресов большего размера в протоколе IPv6 значительно увеличивается число доступных IP-адресов, что позволит предоставить уникальные адреса всем беспроводным устройствам.

Помимо применения более длинных адресов, в IPv6 предусмотрен ряд новых функций, которые упрощают выполнение задач по настройке адресов в сети и управлению ими. На настройку и обслуживание сетей затрачивается значительное время. Протокол IPv6 упрощает работу администратора сети, предоставляя средства для автоматического выполнения некоторых задач.

Если применяется протокол IPv6, то после изменения провайдера Internet (ISP) вам не потребуется изменять адреса устройств. Вы сможете оставить прежние адреса, так как они уникальны на глобальном уровне.

В протоколе IPv6 предусмотрена функция автоматической настройки адресов интерфейсов и маршрутизаторов. Обычно при автоматической настройке протокол IPv6 создает новый уникальный IP-адрес на основе адреса MAC компьютера и префикса сети, заданного на локальном узле. Наличие такой функции позволяет не использовать сервер DHCP, что сэкономит время администратора и деньги вашей фирмы.

Другие источники информации о протоколе IPv6 перечислены в разделе Дополнительная информация о протоколе IPv6

В разделе Функции протокола IPv6 можно найти информацию о применении протокола IPv6 на сервере iSeries.

Функции протокола IPv6

Уже на протяжении нескольких выпусков фирма IBM предлагает реализацию протокола IPv6 для сервера iSeries. В настоящее время реализация протокола IPv6 предназначена для разработки и тестирования приложений IPv6. Функции IPv6 не влияют на работу существующих приложений TCP/IP и могут применяться наряду с функциями IPv4.

Ниже перечислены основные функции сервера iSeries, которые изменились с появлением протокола IPv6:

- **Настройка**
  Обратите внимание, что процедура настройки протокола IPv6 отличается от аналогичной процедуры для IPv4. Для применения функций IPv6 необходимо добавить в конфигурацию TCP/IP на сервере линию связи для IPv6. Такой линией может быть линия связи Ethernet или линия связи туннеля.

  Линия связи Ethernet может служить для передачи пакетов IPv6 по сети IPv6. Примеры с описанием различных ситуаций, в которых для IPv6 можно настроить линию связи Ethernet, приведены в разделе Создание локальной сети (LAN) IPv6.

  Если вы настроите линию связи туннеля, то пакеты IPv6 можно будет передавать по существующей сети IPv4. Примеры двух ситуаций, в которых для IPv6 можно настроить линию связи туннеля, приведены в разделах Отправка пакетов IPv6 по локальной сети (LAN) IPv4 и Отправка пакетов IPv6 по глобальной сети (WAN) IPv4.

  Информация о настройке сети для применения протокола IPv6 приведена в разделе Настройка протокола IPv6.
- **Сокеты**
  В протоколе IPv6 предусмотрены различные функции и API для создания и тестирования приложений с использованием сокетов. С помощью IPv6 приложения с использованием сокетов могут применять новое семейство адресов: AF_INET6. Это изменение не влияет на работу существующих приложений IPv4. Вы можете создать приложения, которые будут поддерживать передачу данных IPv6 и IPv4, либо только IPv6. Дополнительная информация о поддержке сокетов в протоколе IPv6 приведена в разделе Применение семейства адресов AF_INET6.

- **DNS**
  Система имен доменов (DNS) поддерживает адреса AAAA и новый домен обратного преобразования: IP6.ARPA. Хотя сервер DNS принимает информацию IPv6, для подключения к этому серверу система iSeries должна применять протокол IPv4.
- **Устранение неполадок TCP/IP**
  Для устранения неполадок в сетях и туннелях IPv6 можно использовать такие традиционные средства, как PING, netstat, трассировка маршрутов и соединений. Все перечисленные средства поддерживают адреса в формате IPv6. Информация об исправлении ошибок в сетях IPv4 и IPv6 приведена в разделе Устранение неполадок TCP/IP.

Другие источники информации о протоколе IPv6 перечислены в разделе Дополнительная информация о протоколе IPv6.

Сценарии применения IPv6

Ознакомьтесь с различными сценариями применения протокола IPv6, включающими информацию о настройке сети:

- Создание локальной сети (LAN) IPv6
- Отправка пакетов IPv6 по локальной сети (LAN) IPv4
- Отправка пакетов IPv6 по глобальной сети (WAN) IPv4

Примечание: В этих сценариях IP-адреса вида 10.x.x.x представляют внешние IP-адреса. Все адреса приведены только в качестве примера.

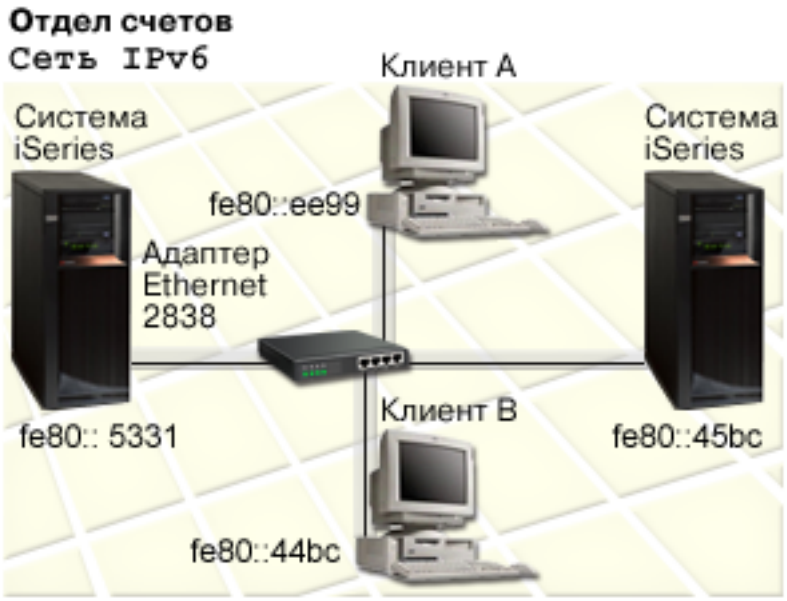
Информация о настройке протокола IPv6 на сервере приведена в разделе Настройка протокола IPv6.

Описание основных принципов работы протокола IPv6 приведено в разделе Принципы работы протокола IPv6.

Создание локальной сети (LAN) IPv6

Задача

Протокол IPv6 постепенно заменяет протокол IPv4 в качестве стандарта сети Internet. В связи с этим ваша фирма решила применять протокол IPv6 при выполнении финансовых операций и заказала новое бухгалтерское приложение, в котором используется протокол связи IPv6. Приложение будет подключаться к другому экземпляру приложения, расположенному на удаленном сервере, который подключен к локальной сети (LAN) Ethernet фирмы. Ваша задача - настроить протокол IPv6 таким образом, чтобы можно было работать с бухгалтерским приложением. На приведенном ниже рисунке показана конфигурация сети в данном сценарии.



Решение

Для создания локальной сети IPv6 необходимо создать описание линии Ethernet для IPv6. При работе с бухгалтерским приложением по сетевому соединению, установленному между сервером iSeries и клиентами, будут передаваться пакеты IPv6.

Ниже перечислены требования к настройке протокола:

- OS/400 версии 5, выпуска 2 или более поздней версии
- Адаптеры Ethernet 2838 или 2849 - только эти типы адаптеров поддерживают протокол IPv6.
- Программы iSeries Access for Windows и Навигатор iSeries (сетевой компонент Навигатора iSeries)
- Перед настройкой линии связи Ethernet для IPv6 на сервере необходимо создать отдельный физический интерфейс IPv4, так как на сервере необходимо запустить TCP/IP. Если протокол IPv4 еще не настроен на сервере, то перед настройкой линии связи для IPv6 выполните инструкции из раздела Начальная настройка TCP/IP.

Настройка

Для создания описания линии Ethernet для протокола IPv6 воспользуйтесь мастером **Настройка протокола IPv6**, который предусмотрен в программе Навигатор iSeries. Протокол IPv6 можно настроить только с помощью Навигатора iSeries. Для этого нельзя использовать текстовый интерфейс.

При работе с мастером вам потребуется указать имя аппаратного ресурса связи сервера iSeries, на котором планируется настроить протокол IPv6, например, CMN01. В качестве такого ресурса необходимо указать адаптер Ethernet 2838 или 2849, который еще не настроен для протокола IPv4.

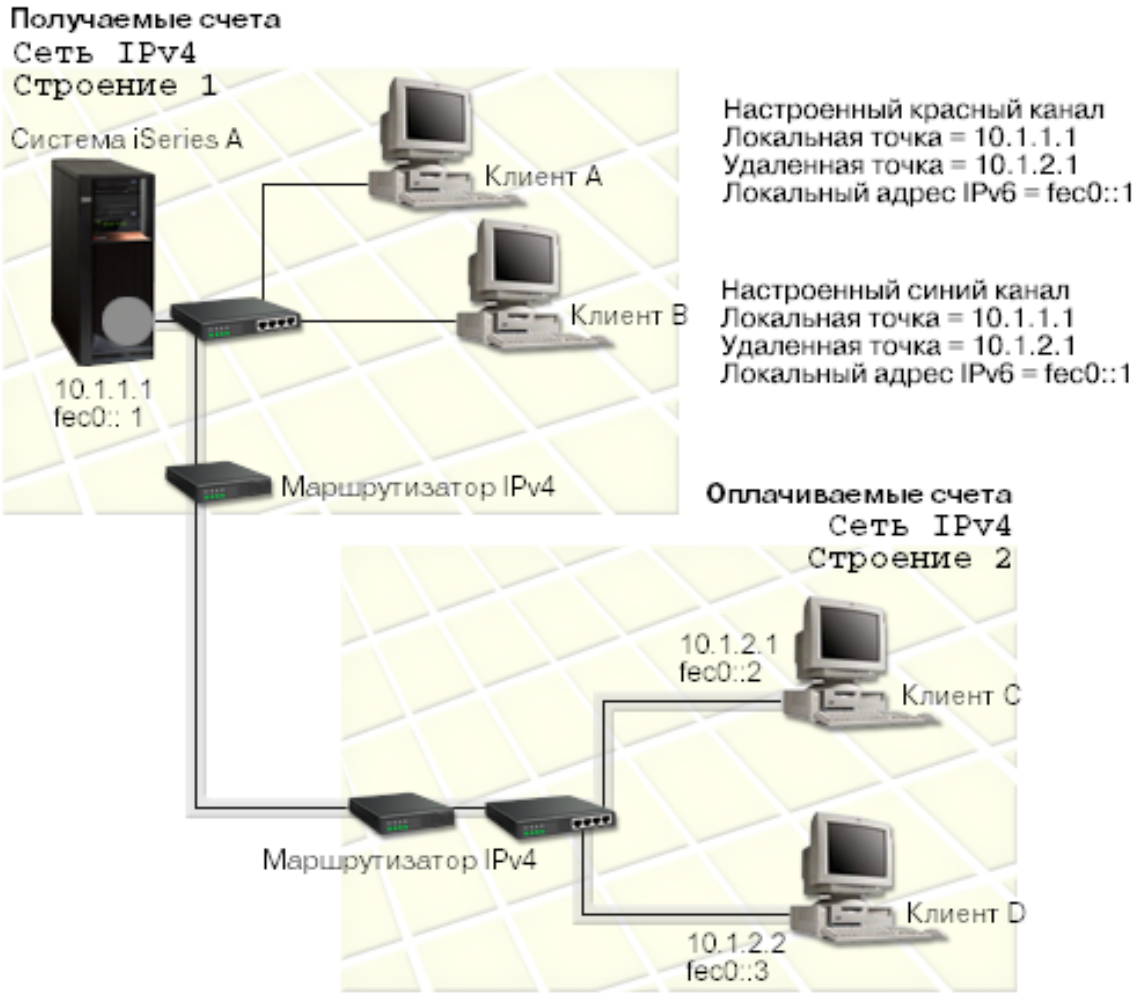
Для запуска мастера **Настройка IPv6** выполните следующие действия:

1. В окне Навигатора iSeries выберите **Сервер —> Сеть —> Настройка TCP/IP**.
2. Щелкните правой кнопкой мыши на пункте **IPv6**, выберите опцию **Настройка IPv6** и следуйте инструкциям мастера по настройке линии Ethernet для IPv6.

Отправка пакетов IPv6 по локальной сети (LAN) IPv4

Задача

В вашей фирме было создано новое бухгалтерское приложение, применяющее протокол IPv6. Это приложение предназначено для внутреннего использования. Оно основано на архитектуре клиент-сервер. Приложение взаимодействует с другими экземплярами приложения, запущенными на серверах фирмы, расположенных в других зданиях и локальных сетях. Хотя в этом приложении применяется протокол IPv6, в сетях фирмы протокол IPv4 еще не полностью заменен на протокол IPv6. Ваша задача - настроить линии связи туннелей IPv6, по которым пакеты IPv6 можно будет передавать через сеть IPv4. На приведенном ниже рисунке показана конфигурация сети в данном сценарии.



Решение

Для передачи данных IPv6 по локальным сетям IPv4 необходимо создать два туннеля и несколько маршрутов. Один туннель отмечен на рисунке красным цветом, а второй - синим.

Вначале рассмотрим красный туннель:

- Красный туннель соединяет систему iSeries A (локальная конечная точка 10.1.1.1), расположенную в здании 1, с клиентом C (удаленная конечная точка 10.1.2.1), расположенным в здании 2.

- Система iSeries A включает пакет IPv6 в пакет IPv4 и передает этот пакет по туннелю. Клиент C извлекает пакет IPv6 из полученного пакета. Таким образом приложение в системе iSeries может обмениваться данными с другим экземпляром приложения IPv6.

Теперь рассмотрим синий туннель:

- Синий туннель соединяет систему iSeries A (локальная конечная точка 10.1.1.1) в здании 1 с клиентом D (удаленная конечная точка 10.1.2.2) в здании 2.
- Система iSeries A включает пакет IPv6 в пакет IPv4 и передает этот пакет по туннелю. Клиент D извлекает пакет IPv6 из полученного пакета. Таким образом приложение в системе iSeries может обмениваться данными с другим экземпляром приложения IPv6.

Каждый туннель представляет собой двухточечное соединение, то есть для каждого туннеля необходимо определить его удаленную конечную точку. Для этого требуется создать два маршрута. Эти маршруты будут связаны с одной линией связи туннеля, однако в качестве следующего транзитного узла в них будут указаны разные удаленные конечные точки. Другими словами, создание двух маршрутов позволяет определить разные удаленные конечные точки туннелей.

Такие маршруты определяют конечные точки туннелей и позволяют передавать данные клиентам из здания 2. Помимо них необходимо создать еще два маршрута, по которым данные будут возвращаться на сервер, расположенный в здании 1.

Ниже перечислены требования к настройке протокола:

- OS/400 версии 5, выпуска 2 или более поздней версии
- Программы iSeries Access for Windows и Навигатор iSeries (сетевой компонент Навигатора iSeries)
- Перед настройкой линии связи туннеля на сервере необходимо настроить TCP/IP (с использованием протокола IPv4). Если протокол IPv4 еще не настроен на сервере, то перед созданием линии связи для туннеля IPv6 выполните инструкции из раздела Начальная настройка TCP/IP.

Настройка

Для создания и настройки линии связи туннеля воспользуйтесь мастером **Настройка IPv6** и мастером **Создать маршрут IPv6**, предусмотренным в программе Навигатор iSeries. Протокол IPv6 можно настроить только с помощью Навигатора iSeries. Для этого нельзя использовать текстовый интерфейс.

Для создания линии связи красного туннеля с помощью мастера **Настройка IPv6** выполните следующие действия:

1. В окне Навигатора iSeries выберите **Сервер —> Сеть —> Настройка TCP/IP**.
2. Щелкните правой кнопкой мыши на пункте **IPv6**, выберите опцию **Настройка IPv6** и выполните инструкции мастера по настройке линии связи для туннеля IPv6. После выполнения всех необходимых действий мастер **Настройка IPv6** предложит вам создать маршрут для новой линии связи туннеля. При этом будет запущен мастер **Создать маршрут IPv6**. Этот маршрут позволит передавать пакеты IPv6 по красному туннелю.
3. С помощью мастера **Создать маршрут IPv6** создайте маршрут для красного туннеля. В качестве следующего транзитного узла укажите адрес удаленной конечной точки туннеля (10.1.2.1), а в качестве адреса получателя - значение fec0::2.

Снова запустите мастер **Создать маршрут IPv6** и создайте маршрут для синего туннеля. Обратите внимание, что синий туннель не обязательно создавать с помощью мастера **Настройка IPv6**. Этот туннель будет автоматически создан после определения его удаленной конечной точки с помощью мастера **Создать маршрут IPv6**. Для запуска мастера **Создать маршрут IPv6** выполните следующие действия:

1. В окне программы Навигатор iSeries выберите **свой сервер —> Сеть —> Настройка TCP/IP —> IPv6**.

2. Щелкните правой кнопкой мыши на пункте **Маршруты**, выберите опцию **Создать маршрут** и выполните инструкции мастера по настройке маршрута IPv6 для синего туннеля. В качестве следующего транзитного узла укажите адрес удаленной конечной точки туннеля (10.1.2.2), а в качестве адреса получателя - значение fec0::3.

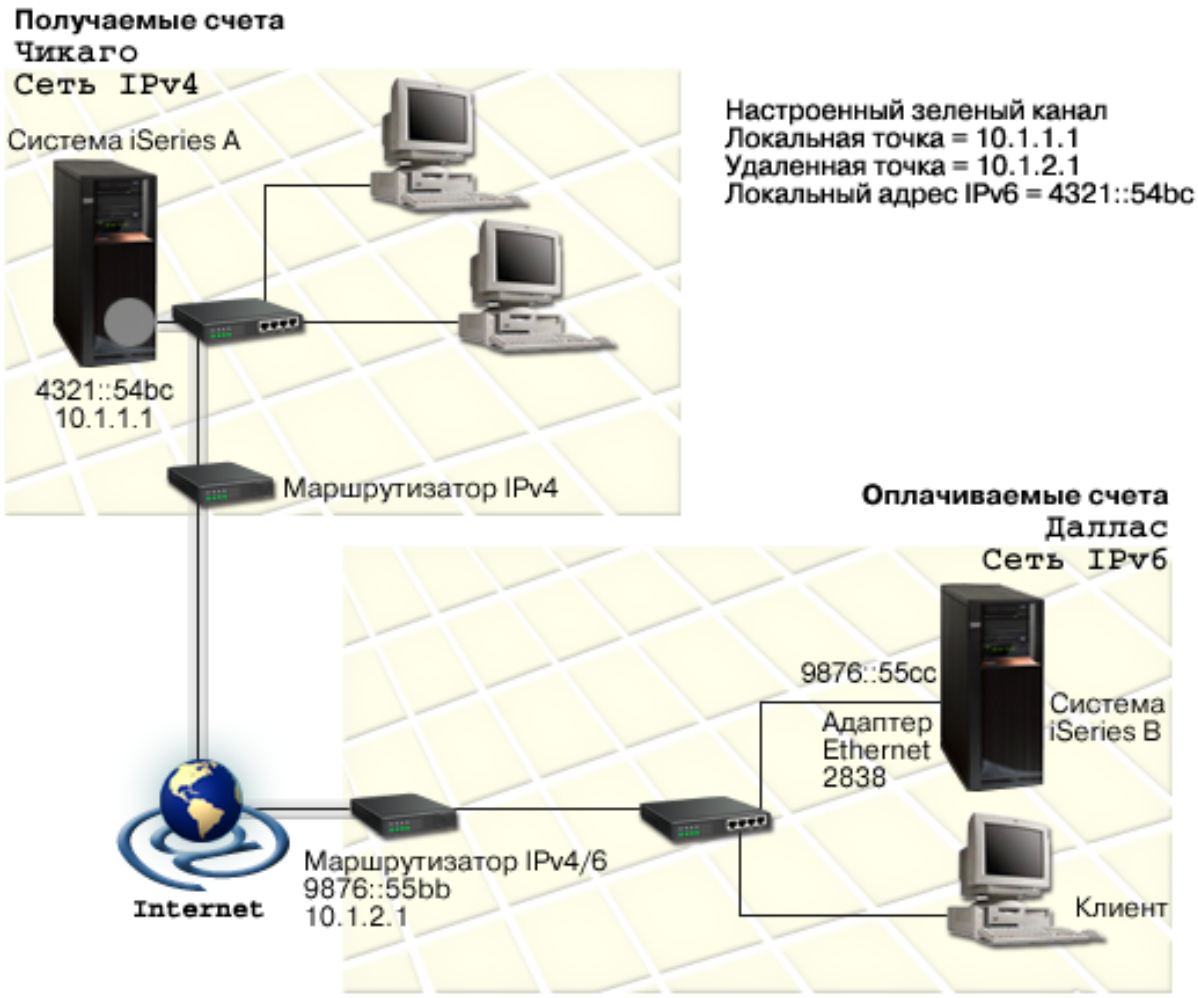
После создания линий связи туннеля и маршрутов, определяющих конечные точки туннеля, создайте маршруты на клиентах C и D, позволяющие передавать пакеты на сервер из здания 1. При определении этих маршрутов укажите в качестве следующего транзитного узла адрес 10.1.1.1, а в качестве адреса получателя - значение fec0::1.

Отправка пакетов IPv6 по глобальной сети (WAN) IPv4

Задача

В офисе фирмы, расположенном в Чикаго, находится сервер, на котором установлена бухгалтерская программа для обработки поступающих счетов. Эта программа должна подключаться к серверу, расположенному в Далласе. Для обращения к обоим серверам в программе применяются адреса Ipv6. Поскольку ISP не может предоставить маршрутизаторы IPv6 для передачи данных между двумя серверами, вам необходимо настроить туннель, соединяющий эти серверы. По этому туннелю, проходящему через глобальную сеть IPv4, будут передаваться пакеты программы. На приведенном ниже рисунке показана конфигурация сети в данном сценарии.

Примечание: В этом сценарии IP-адреса вида 10.x.x.x представляют внешние IP-адреса, которые распознаются во всей глобальной сети. Все адреса приведены только в качестве примера.



Решение

Для передачи данных IPv6 по глобальной сети IPv4 необходимо создать и настроить линию связи туннеля и несколько маршрутов. Ниже приведено более подробное описание:

- Туннель соединяет систему iSeries A (локальную конечную точку 10.1.1.1), расположенную в Чикаго, и маршрутизатор IPv4/6 (удаленную конечную точку 10.1.2.1), расположенный в Далласе.
- Приложение в системе iSeries A будет подключаться к приложению, расположенному в системе iSeries B. Система iSeries A включает пакеты IPv6 в пакеты IPv4 и передает их по туннелю маршрутизатору IPv4/6. Этот маршрутизатор извлекает пакеты IPv6 и пересылает их системе iSeries B.
- При передаче пакетов в Чикаго описанные выше действия выполняются в обратном порядке.

Туннель представляет собой двухточечное соединение, поэтому для него необходимо определить удаленную конечную точку. Для этого нужно создать маршрут, связанный с линией связи туннеля. Удаленная конечная точка (10.1.2.1) должна быть определена в качестве следующего транзитного узла маршрута. Таким образом, удаленная конечная точка задается при создании маршрута. В качестве адреса получателя в определении маршрута необходимо указать значение 9876::55cc (адрес системы iSeries B в формате IPv6).

Этот маршрут определяет конечную точку туннеля и позволяет передавать пакеты на сервер iSeries B, расположенный в Далласе. Помимо него нужно создать еще два маршрута, по которым данные будут возвращаться в систему iSeries A, расположенную в Чикаго.

Ниже перечислены требования к настройке протокола:

- OS/400 версии 5, выпуска 2 или более поздней версии
- Программы iSeries Access for Windows и Навигатор iSeries (сетевой компонент Навигатора iSeries)
- Перед настройкой линии связи туннеля на сервере необходимо настроить TCP/IP (с использованием протокола IPv4). Если протокол IPv4 еще не настроен на сервере, то перед созданием линии связи для туннеля IPv6 выполните инструкции из раздела Начальная настройка TCP/IP.

Настройка

Для создания и настройки линии связи туннеля воспользуйтесь мастером **Настройка IPv6** и мастером **Создать маршрут IPv6**, предусмотренным в программе Навигатор iSeries. Туннели можно настроить только с помощью Навигатора iSeries. Для этого нельзя использовать текстовый интерфейс.

Для создания линии связи туннеля с помощью мастера **Настройка IPv6** выполните следующие действия:

1. В окне Навигатора iSeries выберите **Сервер —> Сеть —> Настройка TCP/IP**.
2. Щелкните правой кнопкой мыши на пункте **IPv6**, выберите опцию **Настройка IPv6** и выполните инструкции мастера по созданию линии связи туннеля для IPv6. После выполнения всех необходимых действий мастер **Настройка IPv6** предложит вам создать маршрут для новой линии связи туннеля. При этом будет запущен мастер **Создать маршрут IPv6**. Этот маршрут позволит передавать пакеты IPv6 по туннелю.
3. С помощью мастера **Создать маршрут IPv6** создайте маршрут для туннеля. В качестве следующего транзитного узла укажите адрес удаленной конечной точки (10.1.2.1), а в качестве адреса получателя задайте значение 9876::55cc.

После создания линии связи туннеля и маршрута, определяющего конечную точку туннеля, необходимо создать маршруты в системе iSeries B и на маршрутизаторе IPv4/6, необходимые для передачи пакетов обратно в Чикаго. В системе iSeries B укажите в качестве следующего транзитного узла маршрута значение 9876::55bb, а в качестве адреса получателя - значение 4321::54bc. На маршрутизаторе IPv4/6 укажите в качестве следующего транзитного узла маршрута значение 10.1.1.1, а в качестве адреса получателя - значение 4321::54bc.

Примечание: На маршрутизаторе IPv4/6, расположенном в Далласе, должен быть определен прямой маршрут до системы 9876::55cc. Этот маршрут создается автоматически.

Принципы работы протокола IPv6

Основные принципы работы протокола IPv6 описаны в следующих разделах:

Сравнение протоколов IPv4 и IPv6
Этот раздел содержит сравнительный анализ атрибутов протоколов IPv4 и IPv6. Приведенная таблица позволит вам быстро сравнить функции протоколов Internet.

Форматы адреса IPv6
В этом разделе приведена информация о различных форматах адреса IPv6 и их размере.

Типы адресов IPv6
Содержит информацию о новых типах адресов, применяемых в протоколе IPv6.

Туннели IPv6
В этом разделе приведена информация о применении туннелей IPv6 для передачи пакетов IPv6 по сети IPv4.

Поиск соседей
Этот раздел содержит информацию о том, каким образом функция поиска соседей позволяет хостам и маршрутизаторам взаимодействовать друг с другом.

Автоматическая настройка адресов
Описание функции автоматической настройки адресов, упрощающей выполнение некоторых задач администрирования сети.

Форматы адреса IPv6

В протоколе IPv6 размер адреса составляет 128 бит. Обычно адрес IPv6 представляется в виде xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где x - это шестнадцатеричная цифра, занимающая 4 бита. Диапазон адресов IPv6 составляет от 0000:0000:0000:0000:0000:0000:0000:0000 до ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Помимо обычного формата, адреса IPv6 могут быть представлены в двух других форматах:

- **С пропуском начальных нулей**
  Адрес IPv6 записывается с пропуском начальных нулей. Например, адрес IPv6 вида 1050:0000:0000:0000:0005:0600:300c:326b можно записать в формате 1050:0:0:0:5:600:300c:326b.
- **Двойное двоеточие**
  В адресе IPv6 на месте нескольких нулей ставится двойное двоеточие (::). Например, адрес IPv6 вида ff06:0:0:0:0:0:0:c3 можно записать в формате ff06::c3. В одном IP-адресе двойное двоеточие может использоваться только один раз.

В альтернативном формате адреса IPv6 совмещаются формат с двоеточиями и формат с точками, поэтому адреса IPv4 можно вставлять в адреса IPv6. В первых 96 битах указываются шестнадцатеричные значения, а в последних 32 битах указываются десятичные значения, задающие адрес IPv4. Такой формат обеспечивает совместимость между узлами IPv6 и IPv4.

Ниже указаны два типа адресов IPv6, которые задаются в альтернативном формате:

- **Адреса IPv4, преобразованные в адреса IPv6**
  Такие адреса представляют узлы IPv4 в сети IPv6. С их помощью приложение IPv6 может напрямую взаимодействовать с приложением IPv4. Примером могут служить адреса 0:0:0:0:0:ffff:192.1.56.10 и ::ffff:192.1.56.10/96 (сокращенный формат).
- **Адреса IPv6, совместимые с адресами IPv4**
  Такие адреса применяются в туннелях. Они позволяют узлам IPv6 передавать данные по сети IPv4. Примером могут служить адреса 0:0:0:0:0:0:192.1.56.10 и ::192.1.56.10/96 (сокращенный формат).

Все перечисленные форматы являются допустимыми форматами адреса IPv6. Адрес IPv6 в Навигаторе iSeries можно указывать в любом из этих форматов.

Типы адресов IPv6

Адреса IPv6 делятся на три основных типа:

Обычный адрес
Обычный адрес обозначает одиночный интерфейс. Пакет, направленный на обычный адрес, проходит путь от одного хоста к другому.

Обычные адреса делятся на три типа:

Адрес уровня линии связи
Адреса уровня линии связи используются в локальных сетях. Они автоматически настраиваются на всех интерфейсах. Префикс такого адреса равен fe80::/10. Маршрутизаторы не пересылают пакеты, содержащие в качестве адреса отправителя или получателя адрес уровня линии связи.

Адрес уровня сайта
Адреса этого типа используются на определенном сайте. Префикс такого адреса равен `fec0::/10`. Маршрутизаторы не пересылают в другие системы пакеты, содержащие в качестве адреса отправителя адрес уровня сайта.

Глобальный адрес
Глобальные адреса могут применяться в любой сети. Префикс адресов такого типа начинается с цифр `001`.

Кроме того, существует два особых типа обычного адреса:

Неопределенный адрес
Неопределенный адрес - это адрес `0:0:0:0:0:0:0:0`, который иногда сокращается до двух двоеточий (`::`). Такой адрес обозначает отсутствие адреса и не может быть связан с хостом. Адрес этого типа используется для обозначения хоста IPv6, с которым не связан никакой адрес. Например, при отправке пакета для определения адреса другого узла в качестве адреса отправителя указывается неопределенный адрес.

Циклический адрес
Циклический адрес - это адрес `0:0:0:0:0:0:0:1`, который в сокращенном виде можно записать как `::1`. Такой адрес применяется узлом для отправки пакета самому себе.

Нечеткий адрес
Нечеткий адрес обозначает набор интерфейсов, возможно, с разным расположением, использующих один адрес. Пакет с нечетким адресом доставляется только ближайшему из членов группы. В настоящий момент сервер iSeries не поддерживает нечеткие адреса.

Групповой адрес
Групповой адрес обозначает набор интерфейсов, возможно, с разным расположением, использующих один адрес. Префикс группового адреса равен `ff`. Пакет с групповым адресом доставляется всем членам группы. В настоящий момент сервер iSeries обеспечивает минимальную поддержку групповых адресов. Создание интерфейсов и приложений с использованием групповых адресов не поддерживается.

Туннели IPv6

Туннели IPv6 позволяют серверу iSeries подключаться к узлам IPv6 (хостам и маршрутизаторам) через домены IPv4. Таким образом, туннели позволяют изолированным узлам и сетям IPv6 устанавливать соединения друг с другом по существующим сетям IPv4. Создание туннелей позволяет параллельно использовать протоколы IPv4 и IPv6, что дает возможность постепенно переходить к протоколу IPv6, продолжая применять соединения IPv4.

Туннель создается между двумя узлами сети IPv4, в которых установлено по два стека протоколов (IPv4 и IPv6). Такие узлы поддерживают как соединения IPv4, так и соединения IPv6. Один из узлов должен быть расположен на границе между сетями IPv6 и IPv4. Он добавляет заголовок IPv4 к каждому пакету IPv6 и отправляет пакет по существующим каналам связи как обычный пакет IPv4. Дальнейшей пересылкой пакетов занимаются маршрутизаторы IPv4. Узел, расположенный на другом конце туннеля, удаляет лишний заголовок IP из пакета IPv6 и пересылает пакет получателю, используя обычный протокол IPv6.

Туннели IPv6 на сервере iSeries устанавливаются по настроенным линиям связи туннелей, которые представляют собой виртуальные линии связи. Такие линии связи позволяют передавать пакеты IPv6 любому узлу с адресом IPv4, к которому задан маршрут, при условии, что этот узел поддерживает туннели IPv6. Такие узлы могут находиться как в локальном, так и в удаленном домене IPv4.

Настроенные соединения туннелей являются двухточечными. Для настройки линии связи туннеля необходимо задать локальную конечную точку туннеля (адрес IPv4), например, `124.10.10.150`, и локальный адрес IPv6, например, `1080:0:0:0:8:800:200c:417a`. Кроме того, для передачи данных по туннелю

необходимо создать маршрут IPv6. При создании маршрута в качестве следующего транзитного узла нужно задать адрес IPv4 одной из конечных точек туннеля. Вы можете настроить любое число туннелей, задав любое число конечных точек.

Сценарии применения туннелей IPv6 и иллюстрации к этим сценариям приведены в разделах Отправка пакетов IPv6 по локальной сети (LAN) IPv4 и Отправка пакетов IPv6 по глобальной сети (WAN) IPv4.

Поиск соседей

Функции поиска соседей применяются хостами и маршрутизаторами IPv6 для обнаружения других узлов IPv6, узлов с адресами уровня линии связи и маршрутизаторов, поддерживающих пересылку пакетов IPv6. На основании результатов поиска создается кэш активных соседей IPv6. Для связи друг с другом узлы IPv6 используют следующие пять сообщений протокола ICMPv6:

Опрос маршрутизаторов
Хосты отправляют такое сообщение для получения извещений от маршрутизаторов. Первый опрос маршрутизаторов проводится хостом как только он становится доступным в сети.

Извещение маршрутизатора
Маршрутизаторы отправляют такие сообщения периодически, либо при проведении опроса. Информация, предоставленная маршрутизатором в извещении, применяется хостами для автоматического создания интерфейсов уровня сайта, глобальных интерфейсов и связанных с ними маршрутов. Кроме того, извещение маршрутизатора содержит другую полезную информацию, в том числе максимальный размер блока передачи и ограничение на число транзитных участков.

Опрос соседей
Узлы отправляют такие сообщения для определения адреса соседнего узла, относящегося к уровню линии связи, или для проверки доступности соседнего узла.

Извещение соседа
Такие сообщения отправляются узлами при проведении опроса соседей или после изменения адреса.

Перенаправление
С помощью этих сообщений маршрутизаторы извещают хосты об оптимальном первом транзитном узле на пути к целевому узлу.

Дополнительная информация о функциях поиска соседей и маршрутизаторов приведена в документе RFC 2461. Этот документ можно найти на Web-сайте RFC Editor (http://www.rfc-editor.org/rfcsearch.html)  .

Автоматическая настройка адресов

Автоматическая настройка адресов - это процесс, с помощью которого узлы IPv6 (хосты и маршрутизаторы) автоматически настраивают адреса IPv6 для интерфейсов. Узел создает адрес IPv6 путем объединения префикса с адресом MAC узла или идентификатором интерфейса, заданным пользователем. В число возможных префиксов входит префикс уровня линии связи (`fe80::/10`) и префиксы размером 64 бита, рекомендованные локальными маршрутизаторами IPv6 (если такие маршрутизаторы есть). Во время автоматической настройки адресов дополнительно создаются интерфейсы с групповым адресом, если тип линии связи допускает многоцелевую рассылку.

Перед назначением адреса интерфейсу узел проверяет его уникальность. Для этого узел отправляет по новому адресу сообщение Опрос соседа и ждет ответа. Если узел не получит ответ, то адрес считается уникальным. Если узел получит в ответ извещение соседа, то адрес считается занятым. Если адрес оказался занятым, то автоматическая настройка завершается; необходимо выполнить настройку интерфейса вручную.

Сравнение протоколов IPv4 и IPv6

Уже на протяжении нескольких выпусков фирма IBM предлагает реализацию протокола IPv6 для сервера iSeries. В настоящее время реализация протокола IPv6 предназначена для разработки и тестирования приложений IPv6.

Важно понимать, в чем состоит отличие протокола IPv6 от IPv4. Приведенная ниже таблица позволит вам быстро сравнить атрибуты протокола IPv4 с аналогичными атрибутами протокола IPv6. Выберите атрибут в списке для перехода к сравнительному анализу.

- “виртуальная частная сеть (VPN)” на стр. 25

	IPv4	IPv6
адрес	Длина - 32 бита (4 байта). Адрес состоит из адреса сети и адреса хоста. Длина этих компонентов зависит от класса адреса. Адреса делятся на классы A, B, C, D и E. Класс адреса определяется несколькими начальными битами адреса. Общее число адресов IPv4 составляет 4 294 967 296. В текстовом виде адрес IPv4 записывается как `nnn.nnn.nnn.nnn`, где `0<= nnn<=255`, а каждая буква `n` представляет десятичную цифру. Незначащие нули можно не указывать. Максимальная длина адреса составляет 15 символов, без учета маски.	Длина - 128 бит (16 байт). Обычно первые 64 бита задают номер сети, а вторые 64 бита - номер хоста. Часто в качестве номера хоста или его компонента в адресе IPv6 указывается адрес MAC или другой идентификатор интерфейса. В подсетях с некоторыми префиксами архитектура IPv6 сложнее архитектуры IPv4. Число адресов IPv6 в 10^{28} (79 228 162 514 264 337 593 543 950 336) раз превосходит число адресов IPv4. Адрес IPv6 записывается в форме `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`, где каждый символ `x` - это шестнадцатиричный символ, соответствующий 4 разрядам. Незначащие нули можно не указывать. В текстовом формате вместо любого числа нулей в адресе можно указать двойное двоеточие (`::`). Например, адрес `::ffff:10.120.78.40` представляет собой адрес IPv4, преобразованный в адрес IPv6. (Дополнительная информация приведена в документе RFC 2373. Этот документ можно найти на Web-сайте RFC Editor (http://www.rfc-editor.org/rfcsearch.html).
распределение адресов	Изначально адреса распределялись по классам сетей. Когда число свободных адресов начало стремительно уменьшаться, адреса были разбиты на более мелкие группы с помощью протокола Бесклассовая междоменная маршрутизация (CIDR). Адреса не были равномерно распределены между различными организациями и странами.	Распределение адресов пока находится на начальном этапе. Рабочая группа Internet (IETF) и группа, ответственная за разработку архитектуры Internet (IAB), рекомендовали предоставить каждой организации, домашнему компьютеру или устройству префикс подсети размером `/48` бит. В этом случае еще 16 бит префикса останется для идентификатора подсети. Пространство адресов достаточно велико для того, чтобы предоставить каждому жителю планеты собственный префикс подсети длиной `/48` бит.
срок действия адреса	Обычно этот атрибут задается только для адресов, назначенных службой DHCP.	Для адресов IPv6 задается два срока действия: предпочитаемый и допустимый, причем предпочитаемый срок действия всегда <= допустимого. После истечения предпочитаемого срока действия адрес перестает указываться в качестве IP-адреса отправителя. После истечения допустимого срока действия адрес перестает применяться (распознаваться) в качестве IP-адреса получателя при приеме пакетов. Для некоторых адресов IPv6, например, адресов уровня линии связи, по умолчанию установлен неограниченный предпочитаемый и допустимый срок действия (см. “пространство адресов”).
маска адреса	Применяется для отделения адреса сети от адреса хоста.	Не применяется (см. “префикс адреса”).
префикс адреса	Иногда применяется для отделения адреса сети от адреса хоста. В некоторых случаях указывается в адресе в виде суффикса `/nn`.	Применяется для определения префикса подсети в адресе. Указывается в виде суффикса `/nnn` (максимум 3 десятичные цифры, `0 <= nnn <= 128`). Примером может служить адрес `fe80::982:2a5c/10`, в котором первые 10 бит представляют префикс подсети.
Протокол преобразования адресов (ARP)	Протокол преобразования адресов применяется в протоколе IPv4 для определения физического адреса, например, адреса MAC или адреса канала связи, связанного с адресом IPv4.	В IPv6 эти функции являются встроенными. Они реализованы в алгоритмах автоматической настройки адресов и поиска соседей, в которых применяется протокол ICMPv6. В связи с этим протокол ARP6 не был разработан.
пространство адресов	К обычным адресам этот термин неприменим. Считается, что существуют диапазоны частных адресов и циклические адреса. Все остальные адреса рассматриваются как глобальные.	В IPv6 понятие пространства адресов встроено в архитектуру. Существует три пространства обычных адресов, в том числе адреса уровня линии связи, адреса уровня сайта и глобальные адреса. Групповые адреса относятся к 14 различным пространствам. Пространство, к которому относится адрес, учитывается при выборе адреса отправителя и получателя по умолчанию. Зоной называется экземпляр пространства адресов в отдельной сети. Иногда адреса IPv6 требуется указывать вместе с идентификатором зоны. Этот идентификатор задается в формате `%zid`, где `zid` - это номер (обычно короткий) или имя. Идентификатор зоны указывается после адреса, но до префикса. Например, `2ba::1:2:14e:9a9b:c%3/48`.
типы адресов	Обычные, групповые и оповещение.	Обычные, групповые и нечеткие. Описание различных типов адресов приведено в разделе Типы адресов IPv6.
трассировка соединений	Средство для сбора подробной информации о пакетах TCP/IP и других пакетах, которые принимаются и отправляются сервером iSeries.	То же самое в IPv6. В частности, может применяться для сбора информации о пакетах ICMPv6 и пакетах IPv6, передаваемых по туннелям через сеть IPv4.

	IPv4	IPv6
настройка	Перед тем как новая система сможет устанавливать соединения, в ней необходимо выполнить настройку, то есть определить IP-адреса и маршруты.	Настройку требуется выполнять только для применения некоторых функций. Например, с помощью Навигатора iSeries для IPv6 можно определить интерфейс Ethernet или интерфейс туннеля. После этого настройка интерфейсов IPv6 будет выполнена автоматически. В результате система сможет подключаться к другим локальным или удаленным системам IPv6, в зависимости от типа сети и наличия маршрутизатора IPv6.
Система имен доменов (DNS)	Приложения применяют DNS для преобразования имен хостов в IP-адреса с помощью API сокетов `gethostbyname()`. Кроме того, с помощью DNS приложения могут преобразовать IP-адреса в имена хостов. Для этого применяется API `gethostbyaddr()`. В IPv4 для обратного преобразования применяется домен in-addr.arpa.	То же самое в IPv6. Для поддержки IPv6 применяется тип записи AAAA (четыре буквы A) и функция обратного преобразования (преобразование IP-адреса в имя). Приложение может выбрать, следует ли принимать адреса IPv6 от DNS и устанавливать соединения с помощью этих адресов. API сокетов `gethostbyname()` не был изменен в протоколе IPv6. API `getaddrinfo()` позволяет принимать только адреса IPv6, либо адреса IPv6 и IPv4. Для обратного преобразования в IPv6 применяется домен ip6.arpa. Если с его помощью преобразование выполнить не удается, то применяется домен ip6.int (см. описание API `getnameinfo()`).
Протокол динамической настройки хостов (DHCP)	Применяется для динамического получения IP-адреса и другой информации о конфигурации.	В настоящее время протокол DHCP не поддерживает IPv6.
Протокол передачи файлов (FTP)	Протокол передачи файлов служит для приема и отправки файлов по сети.	В настоящее время FTP не поддерживает протокол IPv6.
фрагменты	Если пакет слишком велик для его передачи по каналу связи, отправитель (хост или маршрутизатор) может разбить его на несколько фрагментов.	В IPv6 пакет можно разбить на пакеты только на узле отправителя. Сборка пакета может выполняться только на узле получателя. В настоящее время дополнительный заголовок фрагментации не поддерживается.
таблица хостов	В Навигаторе iSeries - настраиваемая таблица, связывающая IP-адреса с именами хостов; например, `127.0.0.1`, loopback. Эта таблица применяется программой преобразования имен сокетов. Эта программа вызывается перед обращением к DNS, либо после обращения к DNS, если преобразование выполнить не удалось (порядок обращения зависит от приоритета поиска имени хоста).	В настоящий момент эта таблица не поддерживается в IPv6. Для преобразования имен IPv6 заказчики должны задать запись AAAA на сервере DNS. Сервер DNS можно запустить в той же системе, что и программу преобразования имен, либо в другой системе.
интерфейс	Логический объект, применяемый в TCP/IP для передачи пакетов. В IPv4 это понятие всегда тесно связано с адресом, а иногда эквивалентно ему. Иногда интерфейс называется логическим интерфейсом. Интерфейсы запускаются и завершают работу независимо друг от друга и от TCP/IP. Для запуска и завершения работы интерфейса можно воспользоваться командами STRTCPIFC и ENDTCPIFC, либо Навигатором iSeries.	Тот же самый смысл, что и в IPv4. Интерфейсы могут запускаться и завершаться независимо друг от друга и от TCP/IP. Для этого применяется Навигатор iSeries.
Протокол управляющих сообщений Internet (ICMP)	ICMP применяется в протоколе IPv4 для обмена информацией о сети.	В протоколе IPv6 применяется для тех же целей. Однако Протокол управляющих сообщений Internet версии 6 (ICMPv6) поддерживает ряд новых атрибутов. Основные типы сообщений остались прежними, например, целевой узел недостижим, эхо-запрос и ответ. Новые типы и коды были добавлены для поддержки функции поиска соседей и других связанных с ней функций.
Протокол Internet для управления группами (IGMP)	IGMP применяется маршрутизаторами IPv4 для поиска хостов, которым должны доставляться данные многоцелевой рассылки. Кроме того, он применяется хостами IPv4 для извещения маршрутизаторов IPv4 о наличии на хосте получателей многоцелевой рассылки.	Заменен на протокол MLD. Этот протокол выполняет те же функции, что и протокол IGMP в IPv4. Он применяет протокол ICMPv6, в котором предусмотрено несколько новых типов, предназначенных для MLD.
Заголовок IP	Длина составляет от 20 до 60 байт в зависимости от числа дополнительных параметров IP.	Длина составляет ровно 40 байт. В заголовке IP никакие дополнительные параметры не указываются. Как правило, структура заголовка IPv6 проще, чем в IPv4.

	IPv4	IPv6
Дополнительные параметры заголовка IP	Различные дополнительные параметры, которые можно указать в заголовке IP (перед заголовком транспортного уровня).	В заголовке IPv6 дополнительные параметры не указываются. Вместо них IPv6 добавляет дополнительные заголовки. Такие заголовки могут содержать информацию AH и ESP (как и в IPv4), а также информацию о прохождении транзитных участков, маршруте, фрагменте и получателе. В настоящее время протокол IPv6 не поддерживает дополнительные заголовки.
Байт протокола в заголовке IP	Код протокола транспортного уровня. Примером значения может служить ICMP.	Заголовок, который указывается сразу после заголовка IPv6. В нем задаются те же значения, что и в поле протокола заголовка IPv4. После этого заголовка может быть указан еще ряд дополнительных заголовков, формат которых может быть расширен. Следующим может быть указан заголовок транспортного протокола, один из дополнительных заголовков или заголовок ICMPv6.
Байт Тип сервиса (TOS) в заголовке IP	Применяется протоколом QoS и дифференцированными службами для определения класса потока данных.	Как и в IPv4, задает класс потока данных IPv6. Для обозначения класса используются другие значения. В настоящее время протокол IPv6 не поддерживает поле TOS.
Функции Навигатора iSeries	Навигатор iSeries позволяет настроить все параметры TCP/IP.	Навигатор iSeries предоставляет все необходимые функции для настройки необязательных параметров IPv6, в том числе мастер **Настройка IPv6**.
Соединение LAN	Применяется интерфейсом IP для подключения к физической сети. Существует несколько типов соединений, в том числе Token Ring, Ethernet и PPP. Иногда называется физическим интерфейсом, каналом связи или линией связи.	В IPv6 также используется этот термин. В настоящее время поддерживаются только линии связи адаптеров Ethernet 2838 и 2849 и линии связи туннелей.
Протокол L2TP	Протокол L2TP можно рассматривать как виртуальный протокол PPP. Он может применяться при работе с любой поддерживаемой линией связи.	В настоящее время протокол L2TP не поддерживает IPv6.
циклический адрес	Интерфейс с адресом `127.*.*.*` (обычно - `127.0.0.1`), который может применяться узлом для отправки пакетов самому себе. Соответствующий физический интерфейс (описание линии) называется *LOOPBACK.	То же самое значение в IPv6. Предусмотрен единственный циклический адрес, равный `0000:0000:0000:0000:0000:0000:0000:0001` или `::1` (сокращенный вариант). Соответствующий виртуальный физический интерфейс называется *LOOPBACK6.
Максимальный блок передачи (MTU)	Максимальный блок передачи - это максимальное число байт, которое можно передать по линии связи определенного типа, например, линии связи Ethernet или модемной линии. Обычно в IPv4 максимальный блок передачи равен 576.	В IPv6 минимальный размер MTU составляет 1280 байт. Следовательно, пакеты IPv6, размер которых меньше этого ограничения, не будут разбиваться на фрагменты. Для передачи пакетов IPv6 по линии связи с размером MTU меньше 1280 эти пакеты должны разбиваться и собираться на уровне канала связи.
netstat	Утилита, предоставляющая информацию о состоянии соединений, интерфейсов и маршрутов TCP/IP. Ее можно вызвать из Навигатора iSeries или в сеансе 5250.	То же самое значение в IPv6. Для работы с IPv6 эту функцию можно вызвать из сеанса 5250 или Навигатора iSeries.
Преобразование сетевых адресов (NAT)	Одна из основных функций брандмауэра, встроенная в стек протоколов TCP/IP. Для ее настройки применяется Навигатор iSeries.	В настоящий момент функция NAT не поддерживает протокол IPv6. Точнее, в IPv6 функция NAT не нужна. В связи со значительным расширением пространства адресов в IPv6 не возникает проблема нехватки адресов. Кроме того, в этом протоколе предусмотрены более простые средства изменения адреса.
таблица сетей	В Навигаторе iSeries - таблица, содержащая информацию об именах и IP-адресах сетей. Маска сети не указывается. Например, запись таблицы может содержать имя сети Network14 и IP-адрес 1.2.3.4.	Эта таблица не изменилась в IPv6.
запрос на получение информации об узле	Не поддерживается.	Удобная сетевая утилита, похожая на утилиту ping. Она позволяет запросит у другого узла IPv6 его имя хоста, обычный адрес IPv6 или адрес IPv4. В настоящее время эта утилита не поддерживается.
фильтрация пакетов	Одна из основных функций брандмауэра, встроенная в стек протоколов TCP/IP. Для ее настройки применяется Навигатор iSeries.	В настоящее функция фильтрации пакетов не поддерживает протокол IPv6. Однако для туннеля, по которому передаются пакеты IPv6, можно настроить функцию фильтрации IPv4.
пересылка пакетов	Сервер iSeries можно настроить таким образом, чтобы он пересылал пакеты IP, предназначенные для удаленных узлов сети. Обычно входящий и исходящий интерфейсы подключены к разным локальным сетям.	В настоящее время пересылка пакетов IPv6 не поддерживается.

	IPv4	IPv6
инкапсуляция пакетов	В IPv4 инкапсуляция пакетов выполняется при передаче данных по соединениям VPN, работающим в режиме туннеля (пакеты IPv4 инкапсулируются в пакеты IPv4), а также при передаче данных по соединениям L2TP.	В IPv6 инкапсуляция данных в пакеты IPv4 рассматривается как основной механизм перехода от одного протокола к другому. В настоящее время организацией IETF определено минимум 5 различных режимов инкапсуляции пакетов IPv6 в пакеты IPv4, каждый из которых обладает своими особенностями и преимуществами. В настоящее время поддерживается базовый способ инкапсуляции пакетов IPv6 в пакеты IPv4, позволяющий узлам IPv6 обмениваться данными по сети Internet, в которой поддерживается протокол IPv4. Этот способ предполагает **настройку туннеля**, то есть виртуального двухточечного канала связи между двумя узлами IPv6. Для такого туннеля был добавлен новый тип линии связи, который называется *TNLCFG64.
PING	Основное средство TCP/IP для проверки достижимости хоста. Эту функцию можно вызвать из Навигатора iSeries или сеанса 5250.	То же самое значение в IPv6. Состояние соединений IPv6 можно проверять как в сеансе 5250, так и с помощью программы Навигатор iSeries.
Двухточечный протокол (PPP)	PPP позволяет устанавливать коммутируемые соединения с помощью различных модемов и линий связи.	В настоящее время протокол PPP не поддерживает IPv6.
ограничения на использование портов	В этих меню iSeries пользователь может выбрать номера портов или диапазоны номеров портов TCP или UDP, которые разрешено использовать только определенному профайлу.	Не поддерживается для IPv6. Настроенные ограничения относятся только к IPv4.
порты	В TCP и UDP применяются разные наборы портов, номера которых находятся в диапазоне от 1 до 65535.	В IPv6 применяются аналогичные порты. Поскольку в этом протоколе предусмотрено новое семейство адресов, число наборов портов увеличилось до четырех. Например, предусмотрено два порта TCP с номером 80, к которым могут подключаться приложения: один из них находится в AF_INET, а второй - в AF_INET6.
внутренние и внешние адреса	Все адреса IPv4 являются внешними. Исключение составляют три диапазона внутренних адресов, определенных организацией IETF в документе RFC 1918: `10.*.*.* (10/8)`, `172.16.0.0 - 172.31.255.255 (172.16/12)` и `192.168.*.* (192.168/16)`. Внутренние адреса обычно применяются в различных организациях. Такие адреса не распознаются в Internet.	В IPv6 применяется аналогичная структура адресов, но с некоторыми существенными различиями. Адреса делятся на внешние и временные (временные адреса ранее назывались анонимными). Дополнительная информация приведена в RFC 3041. В отличие от внутренних адресов IPv4, временные адреса распознаются в глобальной сети. Они применяются для другой цели. Временный адрес скрывает идентификатор клиента, устанавливающего соединение (по соображениям защиты). Срок действия временного адреса ограничен. Такой адрес не содержит идентификатор интерфейса, то есть адрес канала связи (MAC). Как правило, временный адрес нельзя отличить от обычного внешнего адреса. В IPv6 также есть понятие ограниченного адресного пространства, связанное с предусмотренным распределением адресов (см. “пространство адресов” на стр. 20).
таблица протоколов	В Навигаторе iSeries - таблица, содержащая имена протоколов и связанные с ними номера портов. Например: UDP, 17. По умолчанию в таблице есть записи для следующих протоколов: IP, TCP, UDP, ICMP.	Эта таблица может применяться в IPv6 без каких-либо изменений.
Quality of service (QoS)	Quality of service позволяет задать приоритет пакетов и пропускную способность для приложений TCP/IP.	В настоящее время QoS не поддерживает протокол IPv6. Однако при передаче пакетов IPv6 по туннелю, проходящему через сеть IPv4, поток данных IPv4 может обрабатываться существующими службами QoS системы iSeries. В этом случае данные пакетов IPv6 будут обрабатываться правильно.
изменение адреса	Выполняется вручную или с помощью DHCP. Изменение адресов компьютеров в сети организации представляет собой весьма трудоемкий процесс, который рекомендуется выполнять лишь в случае крайней необходимости.	Встроенная функция протокола IPv6. Процедура изменения адресов выполняется в значительной мере автоматически, особенно для адресов с префиксом `/48`.

	IPv4	IPv6
маршрут	Один или несколько IP-адресов, связанных с парой значений, которая включает в себя имя физического интерфейса и IP-адрес следующего транзитного узла. Если адрес получателя пакета IP входит в указанную группу адресов, то этот пакет пересылается указанному транзитному узлу по заданной линии связи. Маршруты IPv4 связаны с интерфейсом IPv4, а значит, и с адресом IPv4. Маршрут по умолчанию называется *DFTROUTE.	То же самое значение, что и в IPv4. Есть одно существенное отличие: маршруты IPv6 связаны с физическим интерфейсом (каналом связи, например, *TNLCFG64 или ETH03), а не с логическим интерфейсом. Такое изменение было внесено по ряду причин. Одна из причин заключается в том, что в IPv6 и в IPv4 применяются разные алгоритмы выбора адреса отправителя. Дополнительная информация приведена в разделе “выбор адреса отправителя”. Для повышения надежности разрешено создавать одинаковые маршруты. Дубликаты маршрута игнорируются во время выбора маршрута.
Протокол информации о маршрутизации (RIP)	RIP - протокол маршрутизации, который поддерживается демоном routed.	В настоящее время протокол RIP не поддерживает IPv6. В IPv6 применяются статические маршруты.
таблица служб	На сервере iSeries - таблица, содержащая имена служб и связанные с ними номера портов и имена протоколов. Например, для службы с именем FTP-control задан порт 21 и протоколы TCP и UDP. В таблице служб указано большое число стандартных служб. Эта таблица применяется многими приложениями для определения порта службы.	В IPv6 эта таблица применяется без изменений.
Простой протокол управления сетью (SNMP)	Протокол SNMP служит для управления системами.	В настоящее время протокол SNMP не поддерживает IPv6. В IPv6 применяются статические маршруты.
API сокетов	Эти API могут применяться в приложениях для работы с TCP/IP. Изменения, внесенные в сокеты в протоколе IPv6, не влияют на работу приложений, которые не планируют применять IPv6.	В IPv6 приложения с использованием сокетов могут применять новое семейство адресов: AF_INET6. Изменения, внесенные в API в протоколе IPv6, не влияют на работу существующих приложений, использующих протокол IPv4. Приложения, которые должны поддерживать потоки данных IPv4 и IPv6, либо только поток данных IPv6, можно легко адаптировать путем преобразования адресов IPv4 в адреса IPv6 формата `::ffff:a.b.c.d`, где `a.b.c.d` - исходный адрес IPv4 клиента. Новые API поддерживают преобразование адресов IPv6 из текстового формата в двоичный, и наоборот. Дополнительная информация о поддержке сокетов в протоколе IPv6 приведена в разделе Применение семейства адресов AF_INET6.
выбор адреса отправителя	Приложение может назначить IP-адрес отправителя (обычно для этого применяется API сокетов `bind()`). Если связывание будет установлено с INADDR_ANY, то адрес отправителя выбирается исходя из маршрута.	Как и при работе с IPv4, приложение может назначить адрес отправителя в формате IPv6 с помощью функции `bind()`. Кроме того, оно может позволить системе выбрать адрес IPv6 отправителя с помощью in6addr_any. Однако поскольку с линией связи IPv6 может быть связано несколько адресов IPv6, будет применяться другой внутренний алгоритм выбора IP-адреса отправителя.
запуск и завершение работы	Для запуска и завершения работы TCP/IP служат команды STRTCP и ENDTCP.	Применяются те же команды. Протоколы IPv4 и IPv6 нельзя запустить или завершить независимо друг от друга, либо независимо от TCP/IP. Это означает, что запускаются и завершаются сразу все функции TCP/IP, а не только протоколы IPv4 и IPv6. Все интерфейсы IPv6 запускаются автоматически, если параметр AUTOSTART равен `*YES` (это значение установлено по умолчанию). Протокол IPv6 нельзя применять, если не установлен протокол IPv4. Кроме того, обязательно нужно задать циклический адрес IPv6 (`::1`).
Telnet	Telnet позволяет работать с удаленной системой так же, как с системой, с которой установлено прямое соединение.	В настоящее время Telnet не поддерживает протокол IPv6.
трассировка маршрута	Одна из основных функций TCP/IP, которая применяется для определения маршрута. Эту функцию можно вызвать из Навигатора iSeries или сеанса 5250.	То же самое значение в IPv6. Для работы с IPv6 эту функцию можно вызвать из сеанса 5250 или Навигатора iSeries.
транспортные уровни	TCP, UDP, RAW. Новый транспортный протокол, SCTP, объединяет лучшие качества протоколов TCP и UDP, то есть обеспечивает гарантированную доставку данных без установления соединения. Протокол SCTP разработан сравнительно недавно и еще не поддерживается в системе iSeries.	Для IPv6 поддерживаются те же транспортные протоколы.

	IPv4	IPv6
неопределенный адрес	Такой тип адреса отсутствует. В приложениях с API сокетов в качестве INADDR_ANY используется адрес `0.0.0.0`.	Равен `::/128` (128 нулевых битов). Указывается в качестве IP-адреса отправителя в некоторых пакетах при поиске соседей, а также в других случаях, например, при работе с сокетами. В приложениях с API сокетов адрес `::/128` используется в качестве `in6addr_any`.
виртуальная частная сеть (VPN)	Виртуальная частная сеть совместно с функцией IPsec позволяет расширить защищенную внутреннюю сеть за счет внешней сети.	В настоящее время VPN не поддерживает протокол IPv6. Однако при передаче пакетов IPv6 по туннелю, проходящему через сеть IPv4, поток данных IPv4 может обрабатываться существующими функциями VPN системы iSeries. Эти функции будут правильно обрабатывать данные, содержащиеся в пакетах IPv6.

Устранение неполадок IPv6

Если на сервере настроен протокол IPv6, то для устранения ошибок в его работе можно воспользоваться некоторыми из тех средств устранения неполадок, которые применяются при работе с IPv4. Например, функция трассировки маршрута и утилита PING разрешают указывать адреса в форматах IPv4 и IPv6, поэтому они могут применяться для проверки соединений и маршрутов в сетях обоих типов. Кроме того, вы можете воспользоваться функцией трассировки соединений для сбора информации о пакетах, передаваемых по линиям связи IPv4 и IPv6.

Общие рекомендации по устранению неполадок IPv4 и IPv6 приведены в разделе Устранение неполадок TCP/IP.

Дополнительная информация о протоколе IPv6

Дополнительную информацию о протоколе IPv6 можно найти в следующих источниках:

Рабочая группа Internet (IETF) (http://www.ietf.cnri.reston.va.us/)
На этом Web-сайте приведена информация о Рабочей группе Internet, которая занимается разработкой протокола Internet (в том числе, IPv6).

IP версии 6 (IPv6) (http://playground.sun.com/pub/ipng/html/ipng-main.html)
На этом Web-сайте приведены спецификации протокола IPv6 и ссылки на другие источники информации об IPv6.

Форум IPv6 (http://www.ipv6forum.com/)
На этом Web-сайте можно найти самую свежую информацию об изменениях и дополнениях, внесенных в протокол IPv6.

Глава 4. Планирование настройки TCP/IP

Перед тем как приступить к установке и настройке сервера iSeries, необходимо составить план предстоящей операции. Ниже перечислены разделы, содержащие инструкции и рекомендации по выполнению соответствующих процедур. В частности, в них можно найти рекомендации по настройке основных параметров TCP/IP. В этих рекомендациях предполагается, что в системе будет применяться протокол IPv4. Соответствующие инструкции и рекомендации по настройке протокола IPv6 приведены в разделе Настройка протокола IPv6.

Требования к настройке TCP/IP
Соберите и запишите основную информацию о конфигурации, необходимую для настройки TCP/IP.

Меры безопасности в сети TCP/IP
Определите, какие меры по защите необходимо принять при подключении системы к сети.

Требования к настройке TCP/IP

Напечатайте этот раздел и запишите параметры конфигурации системы iSeries, а также сети TCP/IP, к которой она подключена. Эта информация потребуется при настройке TCP/IP. Инструкции по определению значений параметров в первых двух строках приведены сразу после таблицы. Если вы встретите незнакомые термины, откройте руководство IBM TCP/IP for AS/400: More Cool Things Than Ever  и ознакомьтесь с главой 2, ″TCP/IP: Basic Installation and Configuration″.

Необходимая информация	В системе	Пример
Тип адаптера связи, подключенного к системе (см. приведенные ниже инструкции)		Ethernet
Имя ресурса		CMN01
IP-адрес сервера iSeries		199.5.83.158
Маска подсети сервера iSeries		255.255.255.0
Адрес шлюза		199.5.83.129
Полное имя системы		sys400.xyz.company.com
IP-адрес сервера DNS		199.4.191.76

Для того чтобы узнать параметры адаптера связи, выполните следующие действия:

1. Введите в командной строке сервера `go hardware` и нажмите клавишу **Enter**.
2. Введите 1, чтобы выбрать опцию Работа с ресурсами связи, и нажмите **Enter**.

   Появится список имен ресурсов связи. Для просмотра дополнительной информации или выполнения операции выполните инструкции, показанные на экране.

Дальнейшие действия:
Установка TCP/IP

Меры безопасности в сети TCP/IP

При планировании конфигурации TCP/IP нужно оценить необходимый уровень защиты. Ниже приведены рекомендации, которые помогут вам обеспечить безопасность при работе с TCP/IP:

- **Запускайте только те приложения TCP/IP, с которыми вы планируете работать.**
  С каждым приложением TCP/IP связана потенциальная возможность внешней атаки. Система должна самостоятельно отклонять запросы на запуск нежелательных приложений, не полагаясь на маршрутизатор. В качестве дополнительной меры безопасности запретите автоматический запуск всех ненужных приложений.
- **Ограничьте длительность работы приложений TCP/IP.**
  Ограничив время работы серверов, вы уменьшите вероятность внешнего нападения. Рекомендуется выключать серверы TCP/IP, например, FTP и Telnet, в нерабочие часы.
- **Ограничьте доступ к приложениям TCP/IP.**
  По умолчанию для изменения параметров TCP/IP необходимы права доступа *IOSYSCFG. Пользователь без прав доступа *IOSYSCFG может запускать приложения TCP/IP только при наличии прав доступа *ALLOBJ или явных прав на запуск приложения. Будьте внимательны, предоставляя специальные права доступа пользователям. Оцените, какие права доступа нужны пользователю, и предоставьте ему только минимальный набор прав. Создайте список пользователей, у которых есть специальные права доступа, и периодически его пересматривайте. Это также позволяет сократить доступ к серверу в нерабочее время.
- **Тщательно проверьте маршруты TCP/IP:**
  - Запретите пересылку IP-пакетов, чтобы хакеры не могли взломать через Web-сервер другие защищенные системы.
  - Определите только один маршрут к внешнему Web-серверу: маршрут по умолчанию к провайдеру Internet.
  - Не задавайте имена и IP-адреса внутренних защищенных систем в таблице хостов Web-сервера. Укажите в ней имена других внешних серверов, к которым вы планируете обращаться.
- **Защитите серверы TCP/IP, обеспечивающие возможность входа в систему для удаленных пользователей**
  Приложения FTP и Telnet чаще всего являются источником внешних атак. Информация о методах защиты от подобных нападений и советы по настройке меню входа в систему приведены в книге Советы по организации защиты iSeries  .

Дополнительная информация о средствах и способах защиты приведена в разделе Защита iSeries при работе в Internet.

Глава 5. Установка TCP/IP

Основные функции TCP/IP, позволяющие подключить сервер iSeries к сети, поставляются вместе с продуктом OS/400. Однако для работы с такими приложениями TCP/IP, как Telnet, FTP и SMTP, вам потребуется установить программу TCP/IP Connectivity Utilities. Этот лицензионный продукт поставляется вместе с операционной системой, но устанавливается независимо от нее.

Для установки программы TCP/IP Connectivity Utilities на сервере iSeries выполните следующие действия:

1. Вставьте дистрибутивный носитель TCP/IP в систему. Если это компакт-диск, вставьте его в оптический дисковод. Если это магнитная лента, вставьте ее в лентопротяжное устройство.
2. Введите `GO LICPGM` в командной строке и нажмите **Enter** для перехода к меню Работа с лицензионными программами.
3. В меню Работа с лицензионными программами выберите опцию **11** (Установить лицензионные программы) для просмотра списка лицензионных программ и их компонентов.
4. Введите **1** (Установить) в поле Опция напротив 57*xx*TC1 (TCP/IP Connectivity Utilities for iSeries). Нажмите **Enter**. Имя выбранной лицензионной программы появится в меню Подтвердить установку лицензионных программ. Нажмите **Enter** для подтверждения.
5. В меню Опции установки укажите следующие значения:

Установочное устройство	При установке с компакт-диска введите `QOPT`. При установке с магнитной ленты введите `TAP01`.
Устанавливаемые объекты	Данная опция позволяет выбрать для установки программы, языковые объекты или и то, и другое.
Автоматический перезапуск	Эта опция позволяет выполнить автоматическую перезагрузку системы после установки.

   После установки программы TCP/IP Connectivity Utilities появится меню Работа с лицензионными программами или меню Вход в систему.
6. Выберите опцию **50** (Показать протокол сообщений), чтобы убедиться, что программа установлена правильно.

   Если во время установки произошла ошибка, в нижней части меню Работа с лицензионными программами будет показано сообщение `Работа с лицензионными программами прервана`. В этом случае установите программу TCP/IP Connectivity Utilities еще раз. Если ошибку устранить не удалось, обратитесь в службу поддержки.

Примечание:

Рекомендуется установить также следующие лицензионные программы:

- Программу iSeries Access for Windows 95/NT (5769–XD1 выпуска V3R1M3 или выше), в состав которой входит Навигатор iSeries, применяемый для настройки некоторых функций TCP/IP.
- Программу IBM HTTP Server for iSeries (57*xx*–DG1), которая предоставляет поддержку Web-сервера.
- Для работы некоторых приложений TCP/IP требуется установить и другие лицензионные программы. Список этих программ приведен в инструкции по установке приложения.

Глава 6. Настройка TCP/IP

Процедура настройки TCP/IP делится на два независимых этапа: начальная настройка и изменение существующей конфигурации для применения протокола IPv6. В этом разделе приведены инструкции по выполнению обеих задач. Для того чтобы ознакомиться с инструкциями по настройке TCP/IP на сервере, щелкните на одной из следующих ссылок:

Начальная настройка TCP/IP
Содержит инструкции по настройке TCP/IP на новом сервере. В ходе описанной процедуры вы настроите параметры TCP/IP и установите соединение.

Настройка протокола IPv6
Содержит инструкции по настройке сервера для работы с IPv6. Этот протокол отличается надежностью и предоставляет расширенное пространство адресов. Если вы никогда не работали с протоколом IPv6, ознакомьтесь с разделом Протокол Internet версии 6 (IPv6), в котором описаны его основные характеристики. Перед настройкой протокола IPv6 на сервере необходимо настроить TCP/IP.

Настройка TCP/IP в состоянии с ограничениями
Этим способом можно воспользоваться для настройки TCP/IP в системе, которая находится в состоянии с ограничениями.

Начальная настройка TCP/IP

Выберите один из следующих способов настройки TCP/IP на новом сервере:

Настройка TCP/IP с помощью мастера EZ-Setup
Этот способ рекомендуется выбрать в том случае, если персональный компьютер настроен для применения мастера EZ-Setup. Мастер EZ-Setup поставляется вместе с сервером iSeries.

Настройка TCP/IP с помощью текстового интерфейса
Этот способ настройки можно выбрать в том случае, если мастер EZ-Setup недоступен. Например, этим способом можно воспользоваться в том случае, если для применения программы Навигатор iSeries на персональном компьютере требуется настроить TCP/IP.

Настройка TCP/IP с помощью мастера EZ-Setup

Удобный графический интерфейс Навигатора iSeries позволяет быстро настроить TCP/IP. Для настройки основных параметров запустите мастер EZ-Setup Навигатора iSeries, который поможет вам создать первое соединение и задать параметры TCP/IP. Это наиболее простой способ настройки TCP/IP на сервере, поэтому рекомендуется использовать именно его. Компакт-диск с мастером EZ-Setup входит в комплект поставки сервера iSeries.

Для настройки сервера выполните следующие действия:

1. Запустите мастер EZ-Setup. Для этого загрузите компакт-диск, поставляемый вместе с сервером. Выполните инструкции мастера по настройке TCP/IP.
2. Запустите TCP/IP
   a. В окне программы Навигатор iSeries разверните **значок сервера –> Сеть**.
   b. Щелкните правой кнопкой мыши на пункте **Настройка TCP/IP** и выберите опцию **Запустить**. Вместе с TCP/IP будут автоматически запущены все интерфейсы и серверы, настроенные на одновременный запуск с TCP/IP.

Настройка TCP/IP на сервере выполнена. Если в дальнейшем вам потребуется изменить конфигурацию TCP/IP, воспользуйтесь для этого Навигатором iSeries. Инструкции по добавлению маршрутов и интерфейсов приведены в разделе Изменение конфигурации TCP/IP с помощью Навигатора iSeries. Инструкции по настройке протокола IP версии 6 приведены в разделе Настройка протокола IPv6.

Настройка TCP/IP с помощью текстового интерфейса

Если мастер EZ-Setup программы Навигатор iSeries недоступен, воспользуйтесь текстовым интерфейсом. Например, этим способом можно воспользоваться на персональном компьютере, если перед применением программы Навигатор iSeries требуется выполнить начальную настройку TCP/IP.

Для выполнения действий по настройке, описанных в этом разделе, вашему пользовательскому профайлу необходимы специальные права доступа *IOSYSCFG. Дополнительная информация об этих правах доступа приведена в разделе, посвященном пользовательским профайлам, руководства iSeries Security Reference


.

Для настройки TCP/IP с помощью текстового интерфейса выполните следующие действия:

1. Введите в командной строке GO TCPADM и нажмите Enter. Появится меню Администрирование TCP/IP.
2. Укажите опцию 1 (Настроить TCP/IP) и нажмите Enter. Появится меню Настроить TCP/IP (CFGTCP). Выберите в этом меню необходимую задачу настройки. Перед тем как приступить к настройке сервера, внимательно ознакомьтесь с пунктами этого меню.

Для настройки TCP/IP на сервере выполните следующие действия.

1. Настройте описание линии связи
2. Включить пересылку IP-дейтаграмм
3. Настройте интерфейс
4. Настройте маршрут
5. Определите локальный домен и имена хостов
6. Определите таблицу хостов
7. Запустите TCP/IP

Настройка описания линии связи (Ethernet)

Ниже приведены инструкции по настройке TCP/IP для адаптера связи Ethernet. Если в вашей системе установлен другой адаптер, например, адаптер Token Ring, обратитесь к *Приложению A* книги Справочник по настройке TCP/IP.

Для настройки описания линии связи выполните следующие действия:

1. Введите в командной строке CRTLINETH и нажмите Enter. Появится меню Создать описание линии (Ethernet) (CRTLINETH).
2. Укажите имя линии связи и нажмите Enter. (Можно задать любое имя.)
3. Укажите имя ресурса и нажмите Enter.

Дальнейшие действия:
Включение пересылки IP-дейтаграмм

Включение пересылки IP-дейтаграмм

Для передачи пакетов между подсетями включите пересылку IP-дейтаграмм.

Для того чтобы включить пересылку IP-дейтаграмм, выполните следующие действия:

1. В командной строке введите CHGTCPA и нажмите F4.
2. Когда на экране появится вопрос о *пересылке IP-дейтаграмм*, введите ответ *YES.

Дальнейшие действия:
Настройте интерфейс

Настройка интерфейса

Для настройки интерфейса выполните следующие действия:

1. Введите в командной строке CFGTCP и нажмите Enter. Появится меню Настроить TCP/IP.
2. В меню Настроить TCP/IP выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
3. Укажите опцию 1 (Добавить) и нажмите Enter. Появится меню Добавить интерфейс TCP/IP.
4. Укажите адрес сервера iSeries, маску подсети и ранее настроенное имя описания линии. Нажмите Enter.

Для запуска интерфейса введите опцию 9 (Запустить) напротив настроенного интерфейса и нажмите Enter.

Дальнейшие действия:
Настройте маршрут

Настройка маршрута

Для доступа к удаленным сетям нужна, по крайней мере, одна запись маршрутизации. Если записей маршрутизации нет, то сервер не сможет обращаться к системам, расположенным вне локальной сети. Кроме того, записи маршрутизации нужны для обеспечения доступа клиентов TCP/IP из удаленных сетей к серверу.

Рекомендуется, чтобы в таблице маршрутизации был определен хотя бы один маршрут по умолчанию (*DFTROUTE). Если в таблице не будет найден подходящий маршрут, то данные будут отправлены IP-маршрутизатору, указанному в первой записи маршрута по умолчанию.

Для настройки маршрута по умолчанию выполните следующие действия:

1. Выберите опцию 2 (Работа с маршрутами TCP/IP) в меню Настроить TCP/IP и нажмите Enter.
2. Укажите опцию 1 (Добавить) и нажмите Enter. Появится меню Добавить маршрут TCP/IP (ADDTCPRTE).
3. Укажите в качестве целевого адреса маршрута значение *DFTROUTE, укажите в качестве маски подсети значение *NONE, задайте IP-адрес следующего транзитного узла и нажмите Enter.

Дальнейшие действия:
Определите локальный домен и имена хостов

Определение локального домена и имен хостов

Для определения локального домена и имен хостов выполните следующие действия:

1. Выберите опцию 12 (Изменить домен TCP/IP) в меню Настроить TCP/IP и нажмите Enter.
2. Укажите имена локального хоста и локального домена. В остальных полях оставьте значения по умолчанию. Нажмите Enter.

Дальнейшие действия:
Определите таблицу хостов

Определение таблицы хостов

Для того чтобы определить таблицу хостов, выполните следующие действия:

1. Выберите опцию 10 (Работа с записями таблицы хостов TCP/IP) в меню Настройка TCP/IP и нажмите Enter.
2. Укажите опцию 1 (Добавить) и нажмите Enter. Появится меню Добавить запись в таблицу хостов TCP/IP.
3. Укажите IP-адрес, связанное с ним имя локального хоста и полное имя хоста, а затем нажмите Enter.
4. Для того чтобы задать несколько имен хостов, укажите знак плюс (+).
5. Повторите эти действия для всех хостов сети, к которым вы планируете обращаться по имени. Добавьте в таблицу запись для каждого из таких хостов.

Дальнейшие действия:
Запустите TCP/IP

Запуск TCP/IP
Службы TCP/IP становятся доступными только после запуска TCP/IP.

Для запуска TCP/IP введите в командной строке `STRTCP`.

Команда Запустить TCP/IP (STRTCP) инициализирует и активизирует функции TCP/IP, а также запускает интерфейсы и задания серверов. Эта команда запускает только те интерфейсы и серверы TCP/IP, для которых задан параметр AUTOSTART *YES.

Настройка TCP/IP на сервере выполнена. Если в дальнейшем вам потребуется изменить конфигурацию TCP/IP, воспользуйтесь для этого Навигатором iSeries. Инструкции по добавлению маршрутов и интерфейсов приведены в разделе Изменение конфигурации TCP/IP с помощью Навигатора iSeries. Инструкции по настройке протокола IP версии 6 приведены в разделе Настройка протокола IPv6.

Настройка протокола IPv6

Для того чтобы приступить к работе со следующим поколением протокола IP, настройте протокол IPv6 в сети. Перед применением функций IPv6 необходимо добавить в конфигурацию TCP/IP линию связи для IPv6. Настройте линию связи адаптера Ethernet 2838 или 2849, либо линию связи туннеля (виртуальную линию). Инструкции по настройке IPv6 приведены в следующих разделах:

Требования к настройке
В этом разделе перечислены аппаратные и программные ресурсы, необходимые для настройки протокола IPv6 на сервере.

Настройка протокола IPv6 с помощью мастера
В этом разделе приведены инструкции по работе с мастером **Настройка IPv6**, который поможет вам задать параметры IPv6 на сервере.

Требования к настройке
Выберите один из двух вариантов конфигурации протокола IPv6. Если вы не знаете, какой вариант нужно выбрать, ознакомьтесь со сценариями применения IPv6.

Для применения функций IPv6 на сервере должны быть выполнены следующие требования:

Для настройки линии связи Ethernet протокола IPv6:
- OS/400 версии 5, выпуска 2 или более поздней версии
- Программы iSeries Access for Windows и Навигатор iSeries
  - Сетевой компонент Навигатора iSeries
- Адаптер Ethernet 2838 или 2849, специально предназначенный для работы с IPv6.
- Если вы планируете передавать пакеты IPv6 за пределы локальной сети, вам потребуется маршрутизатор, поддерживающий протокол IPv6.
- На сервере необходимо настроить и запустить TCP/IP (с использованием протокола IPv4). Для этого протокола должен быть выделен отдельный физический адаптер. Если протокол IPv4 еще не настроен на сервере, то перед настройкой линии связи Ipv4 обратитесь к разделу Начальная настройка TCP/IP.

Для создания и настройки линии связи туннеля (TNLCFG64):
- OS/400 версии 5, выпуска 2 или более поздней версии
- Программы iSeries Access for Windows и Навигатор iSeries
  - Сетевой компонент Навигатора iSeries

- Перед настройкой линии связи туннеля для IPv6 на сервере необходимо настроить TCP/IP (с использованием протокола IPv4). Если протокол IPv4 еще не настроен на сервере, обратитесь к разделу Начальная настройка TCP/IP.

Инструкции по запуску мастера приведены в разделе Настройка IPv6 с помощью мастера.

Настройка IPv6 с помощью мастера

Для настройки протокола IPv6 на сервере вам потребуется изменить конфигурацию сервера с помощью мастера **Настройка IPv6**, предусмотренного в программе Навигатор iSeries. Протокол IPv6 можно настроить только с помощью Навигатора iSeries. Для этого нельзя использовать текстовый интерфейс.

Примечание: С помощью команды Создать описание линии Ethernet (CRTLINETH) в текстовом интерфейсе можно создать описание линии связи Ethernet для IPv6. Однако при этом вам потребуется указать шестнадцатеричный адрес группы 333300000001. Для завершения настройки IPv6 необходимо запустить мастер **Настройка IPv6**.

При работе с мастером вам потребуется задать следующие значения:

Для настройки линии связи Ethernet протокола IPv6:
Такая линия связи позволяет передавать пакеты IPv6 по локальной сети IPv6. При работе с мастером вам потребуется указать имя аппаратного ресурса связи сервера iSeries, на котором планируется настроить протокол IPv6, например, CMN01. В качестве такого ресурса можно указать адаптер Ethernet 2838 или 2849, который еще не настроен для протокола IPv4. Примеры с описанием различных ситуаций, в которых для IPv6 можно настроить линию связи Ethernet, приведены в разделе Создание локальной сети (LAN) IPv6.

Для создания и настройки линии связи туннеля (TNLCFG64):
Такая линия связи позволяет передавать пакеты IPv6 по сетям IPv4. При работе с мастером вам потребуется задать адрес IPv4 локальной конечной точки и адрес IPv6 локального интерфейса, связанного с туннелем. Примеры двух ситуаций, в которых для IPv6 можно настроить линию связи туннеля, приведены в разделах Отправка пакетов IPv6 по локальной сети (LAN) IPv4 и Отправка пакетов IPv6 по глобальной сети (WAN) IPv4.

Для запуска мастера **Настройка IPv6** выполните следующие действия:

1. В окне программы Навигатор iSeries выберите **свой сервер —> Сеть —> Настройка TCP/IP**.
2. Щелкните правой кнопкой мыши на пункте **IPv6** и выберите опцию **Настройка IPv6**.
3. Для настройки IPv6 на сервере выполните инструкции мастера.

Настройка TCP/IP в состоянии с ограничениями

Задача

Вам, как сетевому администратору, необходимо получить отчеты о состоянии резервного копирования сервера. При запуске процедур резервного копирования операционная система должна находиться в состоянии с ограничениями, что позволит предотвратить изменение конфигурации пользователем. Поскольку управление системой выполняется удаленно, то вы просматриваете отчеты о состоянии можно с помощью устройства PDA (или другого устройства, поддерживающего работу в сетях TCP/IP). В устройстве PDA используется приложение, работающее с сокетами, поэтому для его применения необходим активный интерфейс TCP/IP, позволяющий обмениваться данными с сервером. Для обмена данными в таком режиме необходимо сначала запустить протокол TCP/IP со специальными параметрами. После этого необходимо запустить отдельный интерфейс TCP/IP, который позволит создавать соединения с системой. Ниже приведена более подробная информация.

Предварительные требования

На сервере iSeries должна быть запущена операционная система OS/400(R) V5R2 или более позднего выпуска.

Ограничения

Ниже перечислены возможности, отсутствующие, когда система находится в состоянии с ограничениями:

- В системе нельзя запустить серверы TCP/IP (команда STRTCPSRV), поскольку для этого необходимы активные подсистемы.
- Для каждого типа линии (Ethernet, Roken-Ring или DDI) можно запустить только один интерфейс, не подключенный к описанию сетевого сервера (NWSD) или описанию сетевого интерфейса (NWID).

Этапы настройки

1. Запустите протокол TCP/IP со специальными параметрами

   В системе iSeries, находящейся в состоянии с ограничениями, введите следующую команду: STRTCP STRSVR(*NO) STRIFC(*NO). В состоянии с ограничениями данную команду можно запустить только с такими параметрами. Команда запустит протокол TCP/IP; тем не менее, при этом не будут запущены серверы приложений TCP/IP и интерфейсы IP (их нельзя запустить в состоянии с ограничениями).
2. Запустите отдельный интерфейс TCP/IP

   После запуска протокола TCP/IP в состоянии с ограничениями система позволяет запустить отдельный интерфейс, который необходим для работы с приложением, применяющим сокеты.

   a. Убедитесь в том, что в интерфейсе, который необходимо запустить, используется описание линии *ELAN, *TRLAN или *DDI.

      Для просмотра типа линии интерфейса введите в командной строке команду CFGTCP и выберите опцию 1 - Работа с интерфейсами TCP/IP.

   b. Убедитесь в том, что интерфейс не подключен к описанию сетевого сервера или сетевого интерфейса. Во всех остальных случаях на экране появится сообщение об ошибке.

      Для того чтобы проверить, подключен ли интерфейс к описанию сетевого интерфейса (NWID) или сетевого сервера (NWSD), введите команду DSPLIND abc (где abc - это имя описания линии). В качестве имени ресурса не должно быть указано значение *NWID или *NWSD.

      Примечание: Если интерфейс подключен к NWID или NWSD, рекомендуется выбрать другой интерфейс.

   c. Теперь можно запустить интерфейс. Для этого введите в командной строке следующую команду: STRTCPIFC INTNETADR('a.b.c.d'). Вместо a.b.c.d необходимо указать IP-адрес интерфейса.

      Примечание: Не указывайте параметр STRTCPIFC INTNETADR(*AUTOSTART).
3. Проверьте, активен ли интерфейс.

   С помощью команды Ping отправьте пробный пакет интерфейсу, созданному для работы с приложением. В состоянии с ограничениями можно воспользоваться лишь несколькими служебными возможностями TCP/IP. Тем не менее, команды Ping и Netstat использовать можно. Дополнительная информация о работе с командами ping и netstat приведена в публикации Инструменты для проверки структуры сети, в разделе Устранение неполадок TCP/IP.

Глава 7. Изменение конфигурации TCP/IP с помощью Навигатора iSeries

В некоторых случаях может потребоваться внести изменения в конфигурацию уже настроенного протокола TCP/IP. По мере роста сети может возникнуть необходимость изменить какие-либо параметры или добавить интерфейсы и маршруты в конфигурацию сервера. Кроме того, вам может потребоваться настроить протокол IPv6 (Протокол Internet версии 6) для применения приложений IPv6. Для выполнения большинства таких задач в программе Навигатор iSeries предусмотрены специальные мастеры.

В перечисленных ниже разделах приведены инструкции по изменению конфигурации TCP/IP с помощью Навигатора iSeries. Выберите один из этих разделов в качестве начальной точки для поиска информации об изменении конфигурации TCP/IP с помощью Навигатора iSeries.

Изменение параметров TCP/IP

Настройка протокола IPv6

Добавление интерфейсов IPv4

Добавление интерфейсов IPv6

Добавление маршрутов IPv4

Добавление маршрутов IPv6

Изменение параметров TCP/IP

С помощью программы Навигатор iSeries можно просмотреть и изменить параметры TCP/IP. Например, вы можете изменить параметры, относящиеся к именам хостов и доменов, серверу имен, записям в таблице хостов, системным атрибутам, запретам на порты, серверам и соединениям клиентов. Кроме того, можно изменить общие свойства протоколов IPv4 и IPv6 или свойства одного из них, например, транспортный протокол.

Для перехода к окну свойств TCP/IP выполните следующие действия:

1. В окне программы Навигатор iSeries выберите **значок сервера —> Сеть**.
2. Щелкните правой кнопкой мыши на пункте **Настройка TCP/IP** в правой области окна и выберите **Свойства**. Появится окно диалога **Свойства TCP/IP**.
3. Щелкните на одной из вкладок, расположенных в верхней области окна диалога, для просмотра и изменения информации о TCP/IP.

Для добавления или изменения записей таблицы хостов выполните следующие действия:

1. В окне программы Навигатор iSeries выберите **значок сервера —> Сеть**.
2. Щелкните правой кнопкой мыши на пункте **Настройка TCP/IP** и выберите опцию **Таблица хостов**. Появится окно диалога **Таблица хостов**.
3. С помощью окна диалога **Таблица хостов** добавьте, измените или удалите записи таблицы хостов.

Для перехода к окну свойств протокола IPv4 выполните следующие действия:

1. В окне программы Навигатор iSeries выберите **значок сервера —> Сеть**.
2. Щелкните правой кнопкой мыши на пункте **IPv4** и выберите опцию **Свойства**. Появится окно диалога **Свойства IPv4**.
3. Измените параметры протокола IPv4 на соответствующих страницах окна свойств.

Для перехода к окну свойств протокола IPv6 выполните следующие действия:

1. В окне программы Навигатор iSeries выберите **значок сервера —> Сеть**.

2. Щелкните правой кнопкой мыши на пункте **IPv6** и выберите опцию **Свойства**. Появится окно диалога **Свойства IPv6**.
3. Измените параметры протокола IPv6 на соответствующих страницах окна свойств.

Настройка протокола IPv6

Если вы никогда не работали с протоколом IPv6, ознакомьтесь с разделом Протокол Internet версии 6 (IPv6), в котором описаны его основные характеристики.

Для настройки протокола IPv6 необходимо изменить конфигурацию сервера с помощью мастера **Настройка IPv6**. Перед запуском этого мастера ознакомьтесь с разделом Настройка протокола IPv6, в котором приведены инструкции по настройке и перечислены предварительные требования.

Добавление интерфейсов IPv4

Для создания интерфейса IPv4 выполните следующие действия:
1. В окне программы Навигатор iSeries выберите **значок сервера —> Сеть —> Настройка TCP/IP —> IPv4**.
2. Щелкните правой кнопкой мыши на пункте **Интерфейсы**, выберите опцию **Создать интерфейс**, а затем - опцию **Локальная сеть**, **Глобальная сеть** или **Виртуальный IP** для создания интерфейса IPv4 соответствующего типа.
3. Выполните инструкции мастера по созданию интерфейса IPv4.

Добавление интерфейсов IPv6

Для создания интерфейса IPv6 выполните следующие действия:
1. В окне программы Навигатор iSeries выберите **значок сервера —> Сеть —> Настройка TCP/IP —> IPv6**.
2. Щелкните правой кнопкой мыши на **Интерфейсы** и выберите **Создать интерфейс**.
3. Выполните инструкции мастера по созданию интерфейса IPv6.

Добавление маршрутов IPv4

Изменения, вносимые в параметры маршрутизации, вступают в силу немедленно.

Для настройки нового маршрута IPv4 выполните следующие действия:
1. В окне программы Навигатор iSeries выберите **значок сервера —> Сеть —> Настройка TCP/IP —> IPv4**.
2. Щелкните правой кнопкой мыши на пункте **Маршруты** и выберите **Создать маршрут**.
3. Выполните инструкции мастера по созданию маршрута IPv4.

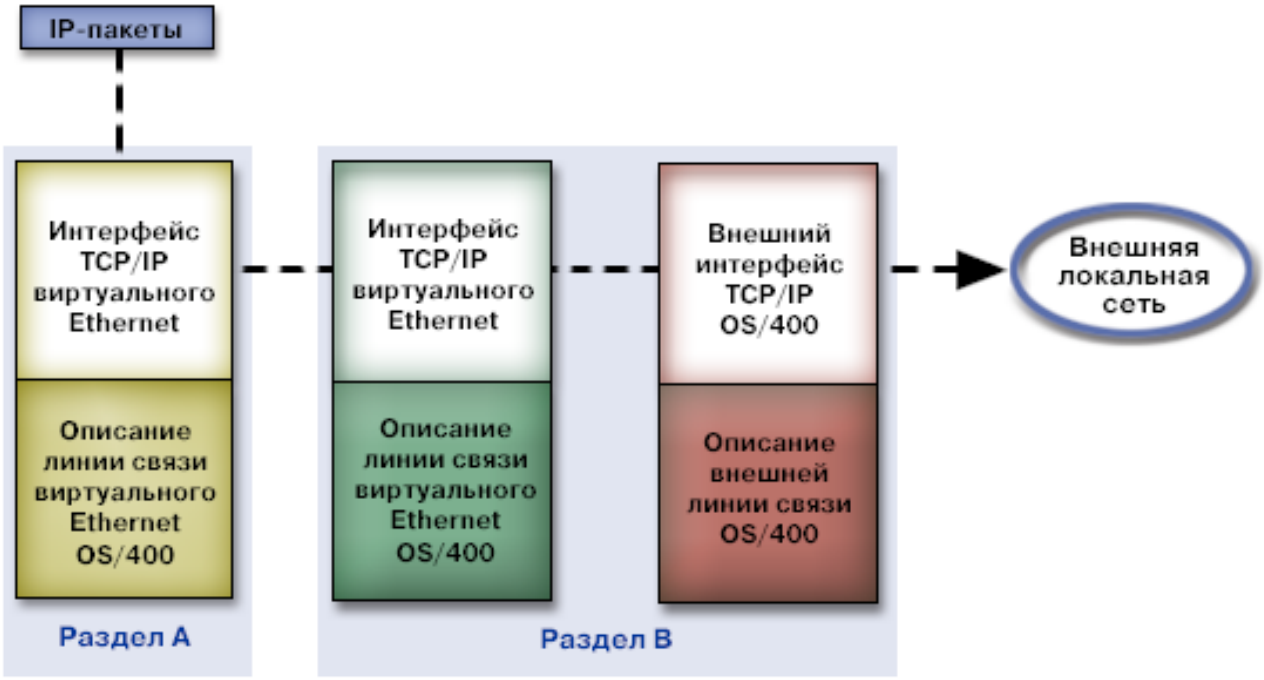
Добавление маршрутов IPv6

Изменения, вносимые в параметры маршрутизации, вступают в силу немедленно.

Для настройки нового маршрута IPv6 выполните следующие действия:
1. В окне программы Навигатор iSeries выберите **значок сервера —> Сеть —> Настройка TCP/IP —> IPv6**.
2. Щелкните правой кнопкой мыши на пункте **Маршруты** и выберите **Создать маршрут**.
3. Выполните инструкции мастера по созданию маршрута IPv6.

Глава 8. Подключение виртуальной сети Ethernet к внешним локальным сетям с помощью TCP/IP

Если разделы системы обмениваются данными с помощью виртуальной сети Ethernet, то может возникнуть необходимость и в передаче информации между разделами и внешней сетью. Существует несколько различных способов подключения виртуальной сети Ethernet к внешним сетям с помощью разных функций TCP/IP. Вы должны разрешить обмен данными TCP/IP между виртуальной сетью Ethernet и внешними локальными сетями. На следующем рисунке приведена логическая схема передачи пакетов IP.



Данные IP, отправленные из раздела A, передаются через виртуальный интерфейс Ethernet этого раздела на виртуальный интерфейс Ethernet раздела B. С помощью любой из описанных ниже трех функций TCP/IP можно обеспечить передачу пакетов IP на внешний интерфейс и далее получателю.

Подключить виртуальную сеть Ethernet к внешней локальной сети можно одним из трех способов. Каждый способ имеет свои особенности, которые делают его более или менее предпочтительным в зависимости от ваших навыков настройки TCP/IP и параметров среды. Вы можете воспользоваться любым из следующих трех способов:

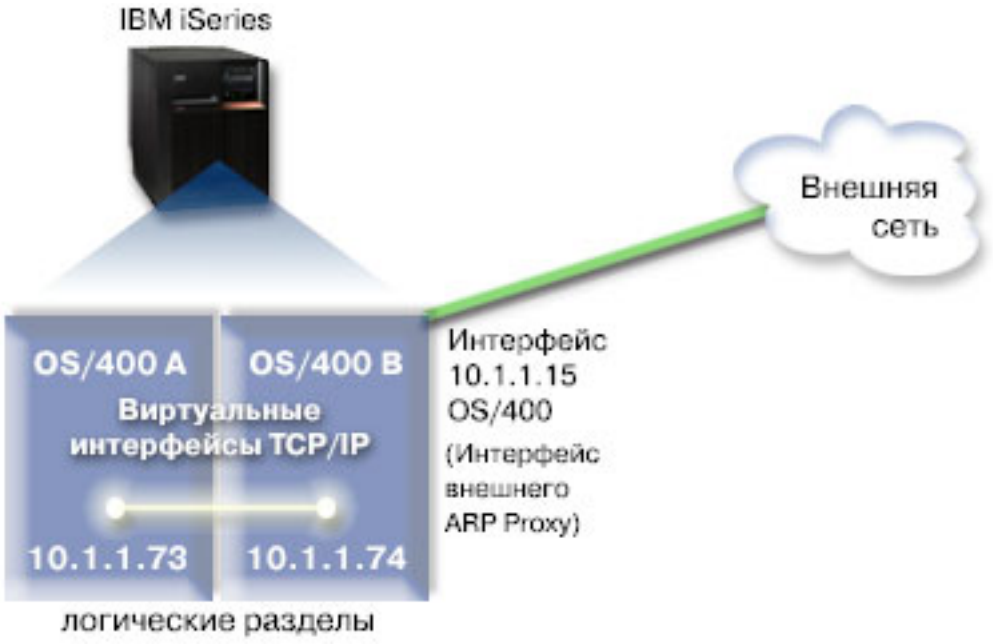
- **Подключение с помощью Proxy ARP**
  Этот способ основан на подключении виртуального интерфейса раздела к внешнему интерфейсу с помощью прозрачного доступа к подсетям. Функция Proxy ARP встроена в стек TCP/IP. Если в системе есть необходимый для этого IP-адрес, рекомендуется использовать данный способ.
- **Преобразование сетевых адресов**
  Для маршрутизации пакетов между разделом и внешней сетью может применяться функция фильтрации пакетов OS/400.
- **Маршрутизация TCP/IP**
  Маршрутизация пакетов в виртуальной сети Ethernet может выполняться с помощью стандартных средств маршрутизации TCP/IP, как и в любой другой локальной сети. Для этого необходимо обновить информацию о маршрутизации в сети.

Подключение с помощью Proxy ARP

Данный метод подключения основан на технологии, известной как *прозрачный доступ к подсетям*. Дополнительная информация об этой технологии приведена в следующих публикациях:

- V4 TCP/IP for AS/400: More Cool Things Than Ever
  В этом справочнике приведены примеры сценариев, иллюстрирующих стандартные решения, а также примеры конфигураций. Он поможет вам составить план, установить и настроить TCP/IP на сервере iSeries, а также устранить возникающие неполадки.
- Маршрутизация TCP/IP и распределение нагрузки
  Данный раздел содержит сведения о настройке маршрутизации и распределении нагрузки.

Для подключения виртуальной сети Ethernet к внешней локальной сети с помощью Proxy ARP необходимы глубокие знания протокола TCP/IP и технологии прозрачного доступа к подсетям. Кроме того, необходимо выделить блок последовательных IP-адресов, используемых в сети. Этот блок адресов объединяется в подсеть. В данном примере блок состоит из четырех IP-адресов (от 10.1.1.72 до 10.1.1.75). Поскольку адресов четыре, маской подсети для них будет значение 255.255.255.252. Каждый адрес присваивается одному виртуальному интерфейсу TCP/IP в каждом разделе системы, как показано на схеме.



В данном примере пакеты TCP/IP передаются из раздела A по виртуальной сети Ethernet на интерфейс с адресом 10.1.1.74 в разделе B. Поскольку адрес 10.1.1.74 связан с внешним интерфейсом Proxy ARP с адресом 10.1.1.15, то пакеты из виртуальной сети Ethernet передаются дальше с помощью интерфейса Proxy ARP.

Для того чтобы настроить передачу данных в виртуальной сети Ethernet с помощью Proxy ARP, необходимо выполнить следующие действия.

1. Включение обмена данными между логическими разделами на основе виртуальной сети Ethernet
2. Создание описаний линий Ethernet
3. Включение пересылки IP-дейтаграмм
4. Создание интерфейса для включения Proxy ARP
5. Создание виртуального интерфейса TCP/IP в разделе A
6. Создание виртуального интерфейса TCP/IP в разделе B
7. Создание маршрута
8. Проверка работы сетевых соединений

Этап 1: Включение обмена данными между логическими разделами на основе виртуальной сети Ethernet

Примечание: В том случае, если применяются не только серверы моделей 270 и 8*xx*, необходимо выполнить эти действия с помощью Консоли аппаратного обеспечения сервера eServer (HMC), а не основного раздела. Дополнительная информация приведена в разделе Виртуальная сеть Ethernet.

Для включения виртуальной сети Ethernet необходимо:

1. В командной строке основного раздела (раздела A) ввести `STRSST` и нажать Enter.
2. Ввести ИД пользователя и пароль сервисных средств.
3. В меню системного инструментария (SST) выбрать опцию 5 (Работа с разделами системы).
4. В меню Работа с разделами системы выбрать опцию 3(Работа с конфигурацией разделов).
5. Нажать F10 (Работа с виртуальными сетями Ethernet).
6. Ввести 1 в соответствующем столбце для раздела A и раздела B, чтобы включить обмен данными между разделами на основе виртуальной сети Ethernet.
7. Выйти из меню Системного инструментария (SST) и вернуться в командную строку.

Дальнейшие действия:

Создание описаний линий Ethernet

Этап 2: Создание описаний линий Ethernet

Создать описания можно одним из двух способов, в зависимости от модели сервера. Выберите способ, соответствующий применяемой модели сервера.

- Создание описаний линий Ethernet на серверах моделей 270 и 8*xx*
- Создание описаний линий Ethernet на серверах других моделей (отличных от 270 и 8xx)

Создание описаний линий Ethernet на серверах моделей 270 и 8*xx*

Для настройки новых описаний линий Ethernet, поддерживающих виртуальные сети Ethernet, выполните следующие действия:

1. В командной строке раздела A введите команду `WRKHDWRSC *CMN` и нажмите Enter.
2. В меню Работа с ресурсами связи выберите опцию 7 (Показать сведения о ресурсах) для нужного виртуального порта Ethernet.

   Виртуальный ресурс Ethernet - это порт Ethernet с обозначением 268C. У каждой виртуальной линии Ethernet, подключенной к логическому разделу, есть один виртуальный ресурс.
3. Пролистайте меню Показать сведения о ресурсах и найдите адрес порта. Адрес порта соответствует виртуальной линии Ethernet, выбранной во время настройки логического раздела.
4. В меню Работа с ресурсами связи выберите опцию 5 (Работа с описаниями конфигураций) для нужного виртуального порта Ethernet и нажмите Enter.
5. В меню Работа с описаниями конфигураций выберите опцию 1 (Создать) и нажмите Enter для перехода к меню Создать описание линии Ethernet (CRTLINETH).
   a. В поле *Описание линии* введите `VETH0`. Несмотря на то, что имя VETH0 выбрано произвольно, оно соответствует пронумерованному столбцу на странице Виртуальная линия Ethernet, на которой вы включили обмен данными между логическими разделами. Указав VETH0 также в качестве имени описания линий и имени связанной виртуальной сети Ethernet, вы сможете легко отслеживать конфигурации виртуальных линий Ethernet.
   b. В поле *Быстродействие линии* введите `1G`.
   c. В поле *Дуплекс* укажите `*FULL` и нажмите Enter.

d. В поле *Максимальный размер кадра* укажите 8996 и нажмите Enter. Применение этого значения позволяет повысить скорость передачи данных в виртуальной сети Ethernet.

   На экране будет показано сообщение о создании описания линии.

6. Включите описание линии. Для этого введите команду WRKCFGSTS *LIN и выберите опцию 1 (Включить) для описания VETH0.
7. Для того чтобы создать описание линии Ethernet раздела B, повторите действия 1 - 6 в командной строке раздела B.

   Имена всех описаний линий можно выбирать произвольно; тем не менее, рекомендуется использовать одно и то же имя для всех описаний линий, связанных с виртуальной сетью Ethernet. В данном сценарии все описания линий имеют имя VETH0.

Дальнейшие действия:

Включение пересылки IP-дейтаграмм

Создание описаний линий Ethernet на серверах других моделей (отличных от 270 и 8xx)

Для настройки новых описаний линий Ethernet, поддерживающих виртуальные сети Ethernet, выполните следующие действия:

1. В командной строке раздела A введите команду WRKHDWRSC *CMN и нажмите Enter.
2. В меню Работа с ресурсами связи выберите опцию 7 (Показать сведения о ресурсах) для нужного виртуального порта Ethernet.

   Виртуальные ресурсы Ethernet - это порты Ethernet с обозначением 268C. У каждой виртуального адаптера Ethernet есть один виртуальный ресурс. С каждым портом 268C связан код расположения, который создается при создании виртуального адаптера Ethernet с помощью HMC (этап 1).
3. Пролистайте меню Показать сведения о ресурсах и найдите ресурс 268C, связанный с кодом расположения, созданным для данного описания виртуальной линии Ethernet.
4. В меню Работа с ресурсами связи выберите опцию 5 (Работа с описаниями конфигураций) для нужного виртуального ресурса Ethernet и нажмите Enter.
5. В меню Работа с описаниями конфигураций выберите опцию 1 (Создать) и нажмите Enter для перехода к меню Создать описание линии Ethernet (CRTLINETH).
   a. В поле *Описание линии* введите VETH0. Указав VETHO также в качестве имени описания линий и имени связанной виртуальной сети Ethernet, вы сможете легко отслеживать конфигурации виртуальных линий Ethernet.
   b. В поле *Быстродействие линии* введите 1G.
   c. В поле *Дуплекс* укажите *FULL и нажмите Enter.
   d. В поле *Максимальный размер кадра* укажите 8996 и нажмите Enter. Применение этого значения позволяет повысить скорость передачи данных в виртуальной сети Ethernet.

      На экране будет показано сообщение о создании описания линии.
6. Включите описание линии. Для этого введите команду WRKCFGSTS *LIN и выберите опцию 1 (Включить) для описания VETH0.
7. Для того чтобы создать описание линии Ethernet раздела B, повторите действия 1 - 6 в командной строке раздела B.

   Имена всех описаний линий можно выбирать произвольно; тем не менее, рекомендуется использовать одно и то же имя для всех описаний линий, связанных с виртуальной сетью Ethernet. В данном сценарии все описания линий имеют имя VETH0.

Дальнейшие действия:

Включение пересылки IP-дейтаграмм

Этап 3: Включение пересылки IP-дейтаграмм

Для передачи пакетов между подсетями включите пересылку IP-дейтаграмм.

Для того чтобы включить пересылку IP-дейтаграмм, выполните следующие действия:

1. В командной строке раздела A введите `CHGTCPA` и нажмите F4.
2. Когда на экране появится вопрос о *пересылке IP-дейтаграмм*, введите ответ `*YES`.

Дальнейшие действия:

Создание интерфейса для включения Proxy ARP

Этап 4: Создание интерфейса для включения Proxy ARP

Для того чтобы создать интерфейс TCP/IP для включения Proxy ARP, выполните следующие действия:

1. Выделите блок последовательных IP-адресов в сети.

   Поскольку данная виртуальная сеть Ethernet состоит из двух разделов, необходим блок из четырех адресов. Последний сегмент первого IP-адреса блока должен делиться на четыре. Первый и последний IP-адреса - это широковещательный адрес и адрес подсети, которые не используются. Второй и третий IP-адреса можно использовать для интерфейсов TCP/IP виртуальной сети Ethernet в разделах A и B. В данном примере применяется блок IP-адресов с 10.1.1.72 по 10.1.1.75 с маской подсети 255.255.255.252.

   Кроме того, необходимо выделить отдельный IP-адрес для внешнего интерфейса TCP/IP. Этот адрес может не принадлежать блоку последовательных адресов, но должен соответствовать исходной маске подсети 255.255.255.0. В данном примере выбран внешний IP-адрес 10.1.1.15.
2. Создайте интерфейс TCP/IP OS/400 для раздела B. Этот интерфейс называют внешним интерфейсом IP Proxy ARP. Для создания интерфейса выполните следующие действия:
   a. В командной строке раздела B введите `CFGTCP` и нажмите Enter для перехода к меню Настройка TCP/IP.
   b. Выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
   c. Выберите опцию 1 (добавить) и нажмите Enter для перехода к меню Добавить интерфейс TCP/IP (ADDTCPIFC).
   d. В поле *IP-адрес* укажите `'10.1.1.15'`.
   e. В поле *Описание линии* укажите имя описания линии, например, ETHLINE.
   f. В поле *Маска подсети* укажите `'255.255.255.0'`.
3. Запустите интерфейс. Для этого в меню Работа с интерфейсами TCP/IP выберите опцию 9 (Запустить) для данного интерфейса.

Дальнейшие действия:

Создание виртуального интерфейса TCP/IP в разделе A

Этап 5: Создание виртуального интерфейса TCP/IP в разделе A

Для создания виртуального интерфейса выполните следующие действия:

1. В командной строке раздела A введите `CFGTCP` и нажмите Enter для перехода к меню Настройка TCP/IP.
2. Выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
3. Выберите опцию 1 (добавить) и нажмите Enter для перехода к меню Добавить интерфейс TCP/IP (ADDTCPIFC).
4. В поле *IP-адрес* укажите `'10.1.1.73'`.
5. В поле *Описание линии* укажите имя описания линии, например, ETHLINE.
6. В поле *Маска подсети* укажите `'255.255.255.252'`.

7. Запустите интерфейс. Для этого в меню Работа с интерфейсами TCP/IP выберите опцию 9 (Запустить) для данного интерфейса.

Дальнейшие действия:

Создание виртуального интерфейса TCP/IP в разделе B

Этап 6: Создание виртуального интерфейса TCP/IP в разделе B

Для создания виртуального интерфейса выполните следующие действия:

1. В командной строке раздела B введите `CFGTCP` и нажмите Enter для перехода к меню Настройка TCP/IP.
2. Выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
3. Выберите опцию 1 (добавить) и нажмите Enter для перехода к меню Добавить интерфейс TCP/IP (ADDTCPIFC).
4. В поле *IP-адрес* укажите `'10.1.1.74'`.
5. В поле *Описание линии* укажите имя описания линии, например, ETHLINE.
6. В поле *Маска подсети* укажите `'255.255.255.252'`.
7. В поле *Связанный локальный интерфейс* укажите `'10.1.1.15'`. Это необходимо для того, чтобы связать виртуальный интерфейс с внешним интерфейсом и включить пересылку пакетов с помощью Proxy ARP между виртуальным интерфейсом 10.1.1.74 и внешним интерфейсом 10.1.1.15.
8. Запустите интерфейс. Для этого в меню Работа с интерфейсами TCP/IP выберите опцию 9 (Запустить) для данного интерфейса.

Дальнейшие действия:

Создание маршрута

Этап 7: Создание маршрута

Для того чтобы создать маршрут по умолчанию, по которому пакеты будут отправляться за пределы виртуальной сети Ethernet, выполните следующие действия:

1. В командной строке раздела A введите `CFGTCP`.
2. Выберите опцию 2 (Работа с маршрутами TCP/IP) и нажмите Enter.
3. Выберите опцию 1 (Добавить) и нажмите Enter.
4. В поле *Целевой адрес маршрута* укажите `*DFTROUTE` .
5. В поле *Маска подсети* укажите `*NONE`.
6. В поле *Следующий узел* укажите `'10.1.1.74'`.

   Пакеты будут по умолчанию передаваться из раздела A на интерфейс 10.1.1.74 в виртуальной сети Ethernet по этому маршруту. Поскольку адрес 10.1.1.74 связан с внешним интерфейсом Proxy ARP 10.1.1.15, пакеты будут передаваться за пределы виртуальной сети Ethernet с помощью интерфейса Proxy ARP.

Дальнейшие действия:

Проверка работы сетевых соединений

Этап 8: Проверка работы сетевых соединений

Проверьте работу сетевых соединений с помощью команды ping:

- В командной строке раздела A дважды введите команду ping, указав в ней сначала адрес виртуального интерфейса Ethernet 10.1.1.74, а затем - адрес внешнего узла.
- В командной строке внешнего узла OS/400 введите команду ping, указав адреса виртуальных интерфейсов Ethernet 10.1.1.73 и 10.1.1.74.

Подключение с помощью функции преобразования сетевых адресов

Служба преобразования сетевых адресов (NAT) позволяет пересылать пакеты между виртуальной сетью Ethernet и внешней сетью. Такой тип NAT называется статическим, и поддерживает обработку как входящих, так и исходящих пакетов в виртуальной сети Ethernet. Если виртуальная сеть Ethernet не получает пакетов от внешних отправителей, то можно применять и другие типы NAT, например, маскирующий NAT. Помимо функций маршрутизации TCP/IP и Proxy ARP, вы можете воспользоваться возможностями существующих сетевых соединений OS/400. Поскольку при этом применяются правила обработки пакетов IP, необходимо создать и активировать эти правила с помощью Навигатора iSeries.

На следующем рисунке приведен пример подключения виртуальной сети Ethernet к внешней сети с помощью NAT. Адреса 10.1.1.*x* соответствуют внешней сети, а адреса 192.168.1.*x* - виртуальной сети Ethernet.

В данном примере все пакеты TCP/IP, отправляемые с сервера, передаются с помощью интерфейса 10.1.1.2. Поскольку в сценарии используется статичное преобразование, то для входящих пакетов адрес 10.1.1.3 заменяется на 192.168.1.5. Для исходящих пакетов адрес 192.168.1.5 заменяется на 10.1.1.3. Разделы A и B обмениваются пакетами с помощью адресов 192.168.1.1 и 192.168.1.5 соответственно.

Для применения статического NAT необходимо настроить систему OS/400 и параметры TCP/IP. После этого необходимо создать и применить правила обработки пакетов IP. Для того чтобы настроить передачу данных в виртуальной сети Ethernet на основе NAT, необходимо выполнить следующие действия:

1. Включение обмена данными между логическими разделами на основе виртуальной сети Ethernet
2. Создание описаний линий Ethernet
3. Включение пересылки IP-дейтаграмм
4. Создание интерфейсов
5. Проверка работы сетевых соединений
6. Создание правил обработки пакетов
7. Проверка работы сетевых соединений

Этап 1: Включение обмена данными между логическими разделами на основе виртуальной сети Ethernet

Примечание: В том случае, если применяются не только серверы моделей 270 и 8*xx*, необходимо выполнить эти действия с помощью Консоли аппаратного обеспечения сервера eServer (HMC), а не основного раздела. Дополнительная информация приведена в разделе Виртуальная сеть Ethernet.

Для включения виртуальной сети Ethernet необходимо:

1. В командной строке основного раздела (раздела A) ввести `STRSST` и нажать Enter.
2. Ввести ИД пользователя и пароль сервисных средств.
3. В меню системного инструментария (SST) выбрать опцию 5 (Работа с разделами системы).
4. В меню Работа с разделами системы выбрать опцию 3(Работа с конфигурацией разделов).
5. Нажать F10 (Работа с виртуальными сетями Ethernet).
6. Ввести 1 в соответствующем столбце для раздела A и раздела B, чтобы включить обмен данными между разделами на основе виртуальной сети Ethernet.
7. Выйти из меню Системного инструментария (SST) и вернуться в командную строку.

Дальнейшие действия:

Создание описаний линий Ethernet

Этап 2: Создание описаний линий Ethernet

Создать описания можно одним из двух способов, в зависимости от модели сервера. Выберите способ, соответствующий применяемой модели сервера.

- Создание описаний линий Ethernet на серверах моделей 270 и 8*xx*
- Создание описаний линий Ethernet на серверах других моделей (отличных от 270 и 8xx)

Создание описаний линий Ethernet на серверах моделей 270 и 8*xx*

Для настройки новых описаний линий Ethernet, поддерживающих виртуальные сети Ethernet, выполните следующие действия:

1. В командной строке раздела A введите команду `WRKHDWRSC *CMN` и нажмите Enter.
2. В меню Работа с ресурсами связи выберите опцию 7 (Показать сведения о ресурсах) для нужного виртуального порта Ethernet.

   Виртуальный ресурс Ethernet - это порт Ethernet с обозначением 268C. У каждой виртуальной линии Ethernet, подключенной к логическому разделу, есть один виртуальный ресурс.
3. Пролистайте меню Показать сведения о ресурсах и найдите адрес порта. Адрес порта соответствует виртуальной линии Ethernet, выбранной во время настройки логического раздела.
4. В меню Работа с ресурсами связи выберите опцию 5 (Работа с описаниями конфигураций) для нужного виртуального порта Ethernet и нажмите Enter.
5. В меню Работа с описаниями конфигураций выберите опцию 1 (Создать) и нажмите Enter для перехода к меню Создать описание линии Ethernet (CRTLINETH).
   a. В поле *Описание линии* введите `VETH0`. Несмотря на то, что имя VETH0 выбрано произвольно, оно соответствует пронумерованному столбцу на странице Виртуальная линия Ethernet, на которой вы включили обмен данными между логическими разделами. Указав VETH0 также в качестве имени описания линий и имени связанной виртуальной сети Ethernet, вы сможете легко отслеживать конфигурации виртуальных линий Ethernet.
   b. В поле *Быстродействие линии* введите `1G`.
   c. В поле *Дуплекс* укажите `*FULL` и нажмите Enter.

d. В поле *Максимальный размер кадра* укажите 8996 и нажмите Enter. Применение этого значения позволяет повысить скорость передачи данных в виртуальной сети Ethernet.

   На экране будет показано сообщение о создании описания линии.

6. Включите описание линии. Для этого введите команду WRKCFGSTS *LIN и выберите опцию 1 (Включить) для описания VETH0.
7. Для того чтобы создать описание линии Ethernet раздела B, повторите действия 1 - 6 в командной строке раздела B.

   Имена всех описаний линий можно выбирать произвольно; тем не менее, рекомендуется использовать одно и то же имя для всех описаний линий, связанных с виртуальной сетью Ethernet. В данном сценарии все описания линий имеют имя VETH0.

Дальнейшие действия:

Включение пересылки IP-дейтаграмм

Создание описаний линий Ethernet на серверах других моделей (отличных от 270 и 8xx)

Для настройки новых описаний линий Ethernet, поддерживающих виртуальные сети Ethernet, выполните следующие действия:

1. В командной строке раздела A введите команду WRKHDWRSC *CMN и нажмите Enter.
2. В меню Работа с ресурсами связи выберите опцию 7 (Показать сведения о ресурсах) для нужного виртуального порта Ethernet.

   Виртуальные ресурсы Ethernet - это порты Ethernet с обозначением 268C. У каждой виртуального адаптера Ethernet есть один виртуальный ресурс. С каждым портом 268C связан код расположения, который создается при создании виртуального адаптера Ethernet с помощью HMC (этап 1).
3. Пролистайте меню Показать сведения о ресурсах и найдите ресурс 268C, связанный с кодом расположения, созданным для данного описания виртуальной линии Ethernet.
4. В меню Работа с ресурсами связи выберите опцию 5 (Работа с описаниями конфигураций) для нужного виртуального ресурса Ethernet и нажмите Enter.
5. В меню Работа с описаниями конфигураций выберите опцию 1 (Создать) и нажмите Enter для перехода к меню Создать описание линии Ethernet (CRTLINETH).
   a. В поле *Описание линии* введите VETH0. Указав VETHO также в качестве имени описания линий и имени связанной виртуальной сети Ethernet, вы сможете легко отслеживать конфигурации виртуальных линий Ethernet.
   b. В поле *Быстродействие линии* введите 1G.
   c. В поле *Дуплекс* укажите *FULL и нажмите Enter.
   d. В поле *Максимальный размер кадра* укажите 8996 и нажмите Enter. Применение этого значения позволяет повысить скорость передачи данных в виртуальной сети Ethernet.

      На экране будет показано сообщение о создании описания линии.
6. Включите описание линии. Для этого введите команду WRKCFGSTS *LIN и выберите опцию 1 (Включить) для описания VETH0.
7. Для того чтобы создать описание линии Ethernet раздела B, повторите действия 1 - 6 в командной строке раздела B.

   Имена всех описаний линий можно выбирать произвольно; тем не менее, рекомендуется использовать одно и то же имя для всех описаний линий, связанных с виртуальной сетью Ethernet. В данном сценарии все описания линий имеют имя VETH0.

Дальнейшие действия:

Включение пересылки IP-дейтаграмм

Этап 3: Включение пересылки IP-дейтаграмм

Для передачи пакетов между подсетями включите пересылку IP-дейтаграмм.

Для того чтобы включить пересылку IP-дейтаграмм, выполните следующие действия:

1. В командной строке раздела A введите `CHGTCPA` и нажмите F4.
2. Когда на экране появится вопрос о *пересылке IP-дейтаграмм*, введите ответ `*YES`.

Дальнейшие действия:

Создание интерфейсов

Этап 4: Создание интерфейсов

Для создания интерфейсов TCP/IP выполните следующие действия:

1. Для обмена данными с сервером создайте и запустите интерфейс TCP/IP OS/400 в разделе B. Для создания интерфейса выполните следующие действия:
   a. В командной строке раздела B введите `CFGTCP` и нажмите Enter для перехода к меню Настройка TCP/IP.
   b. Выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
   c. Выберите опцию 1 (добавить) и нажмите Enter для перехода к меню Добавить интерфейс TCP/IP (ADDTCPIFC).
   d. В поле *IP-адрес* укажите `'10.1.1.2'`.
   e. В поле *Описание линии* укажите `ETHLINE`.
   f. В поле *Маска подсети* укажите `'255.255.255.0'`.
   g. Запустите интерфейс. Для этого в меню Работа с интерфейсами TCP/IP выберите опцию 9 (Запустить) для данного интерфейса.
2. Создайте и запустите еще один интерфейс TCP/IP для подключения к внешней сети. Он должен работать с тем же описанием линии, что и существующий внешний интерфейс TCP/IP. Этот интерфейс будет преобразовывать IP-адреса для данного раздела. Для создания интерфейса выполните следующие действия:
   a. В командной строке раздела B введите `CFGTCP` и нажмите Enter для перехода к меню Настройка TCP/IP.
   b. Выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
   c. Выберите опцию 1 (добавить) и нажмите Enter для перехода к меню Добавить интерфейс TCP/IP (ADDTCPIFC).
   d. В поле *IP-адрес* укажите `'10.1.1.3'`.
   e. В поле *Описание линии* укажите `ETHLINE`.
   f. В поле *Маска подсети* укажите `'255.255.255.0'`.
   g. Запустите интерфейс. Для этого в меню Работа с интерфейсами TCP/IP выберите опцию 9 (Запустить) для данного интерфейса.
3. Создайте и запустите интерфейс TCP/IP OS/400 для виртуальной сети Ethernet в разделе A. Для создания интерфейса выполните следующие действия:
   a. В командной строке раздела A введите `CFGTCP` и нажмите Enter для перехода к меню Настройка TCP/IP.
   b. Выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
   c. Выберите опцию 1 (добавить) и нажмите Enter для перехода к меню Добавить интерфейс TCP/IP (ADDTCPIFC).
   d. В поле *IP-адрес* укажите `'192.168.1.1'`.
   e. В поле *Описание линии* введите `VETH0`.
   f. В поле *Маска подсети* укажите `'255.255.255.0'`.

g. Запустите интерфейс. Для этого в меню Работа с интерфейсами TCP/IP выберите опцию 9 (Запустить) для данного интерфейса.

4. Создайте и запустите интерфейс TCP/IP OS/400 для виртуальной сети Ethernet в разделе B. Для создания интерфейса выполните следующие действия:
   a. В командной строке раздела B введите `CFGTCP` и нажмите Enter для перехода к меню Настройка TCP/IP.
   b. Выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
   c. Выберите опцию 1 (добавить) и нажмите Enter для перехода к меню Добавить интерфейс TCP/IP (ADDTCPIFC).
   d. В поле *IP-адрес* укажите `'192.168.1.5'`.
   e. В поле *Описание линии* введите `VETH0`.
   f. В поле *Маска подсети* укажите `'255.255.255.0'`.
   g. Запустите интерфейс. Для этого в меню Работа с интерфейсами TCP/IP выберите опцию 9 (Запустить) для данного интерфейса.

Дальнейшие действия:

Проверка работы сетевых соединений

Этап 8: Проверка работы сетевых соединений

Проверьте работу сетевых соединений с помощью команды ping:

- В командной строке раздела A дважды введите команду ping, указав в ней сначала адрес виртуального интерфейса Ethernet 192.168.1.5, а затем - адрес внешнего узла.
- В командной строке внешнего узла OS/400 введите команду ping, указав в ней адреса виртуальных интерфейсов Ethernet 192.168.1.1 и 192.168.1.5.

Дальнейшие действия:

Создание правил обработки пакетов

Этап 6: Создание правил обработки пакетов

С помощью мастера преобразования адресов Навигатора iSeries создайте правила обработки пакетов, на основе которых внутренние адреса раздела A будут преобразовываться во внешние адреса раздела B.

Для создания правил обработки пакетов выполните следующие действия:

1. В окне Навигатора iSeries выберите свой сервер **iSeries –> Сеть –>Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Правила обработки пакетов** и выберите опцию **Редактор правил**.
3. В меню **Мастер** выберите **Преобразование адресов**.
4. Выполните указания мастера по созданию правил обработки пакетов. Выполните следующие действия:
   - Выберите пункт **Таблица преобразования адресов**
   - Укажите внутренний IP-адрес `192.168.1.1`
   - Укажите внешний IP-адрес `10.1.1.3`
   - Выберите линию, для которой выполняется настройка интерфейсов, например, ETHLINE
5. В меню **Файл** выберите пункт **Активировать правила**.

Дальнейшие действия:

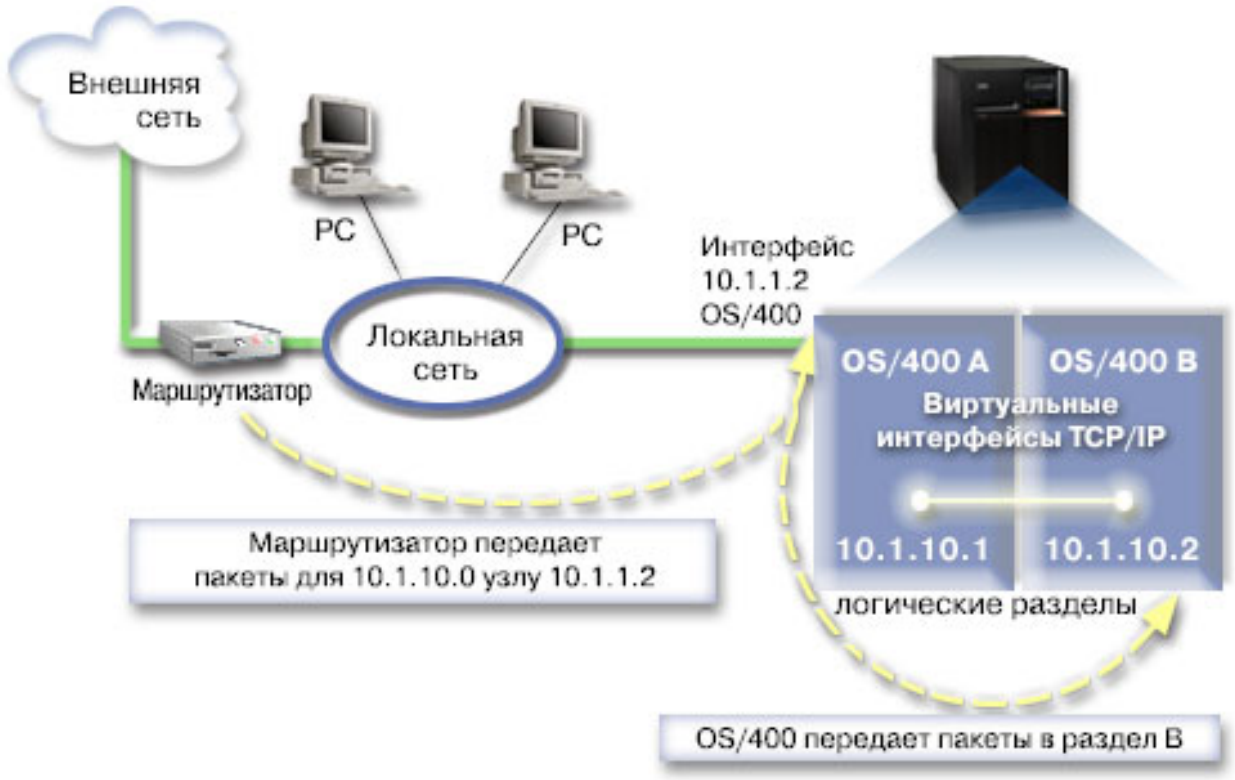
Проверка работы сетевых соединений

Этап 7: Проверка работы сетевых соединений

После создания правил обработки пакетов необходимо проверить работу сетевых соединений. Для проверки исходящих соединений воспользуйтесь командой ping в разделе A, указав в ней адрес внешнего узла. После этого для проверки входящих соединений на удаленном узле также введите команду ping, указав в ней адрес раздела A.

Способ маршрутизации TCP/IP

Существует несколько способов маршрутизации пакетов для разделов сервера iSeries. Это несложная задача, но, в зависимости от топологии сети, такое решение может быть непрактичным. Обратите внимание на следующую схему.



Существующий интерфейс TCP/IP (10.1.1.2) подключен к локальной сети. Сеть подключена к удаленным сетям с помощью маршрутизатора. Адрес виртуального интерфейса TCP/IP в разделе B - 10.1.10.2, а виртуального интерфейса TCP/IP в разделе A - 10.1.10.1. Если включить в системе OS/400 пересылку IP-дейтаграмм, то OS/400 будет обрабатывать все входящие и исходящие пакеты IP для раздела B. При создании определения соединения TCP/IP для раздела B в качестве адреса маршрутизатора необходимо указать 10.1.10.1.

Сложность данного способа маршрутизации заключается в пересылке пакетов IP на сервер iSeries. В данном сценарии можно определить на маршрутизаторе такой маршрут, при котором пакеты, адресованные сети 10.1.10.0, будут передаваться интерфейсу 10.1.1.2. Этот маршрут будет работать при обмене пакетами с удаленными клиентскими системами. Он также подходит для локальных клиентских систем (подключенных к той же сети, что и сервер iSeries), если в качестве следующего узла на них указан тот же маршрутизатор. В том случае, если указан другой маршрутизатор, в каждой клиентской системе должен быть определен маршрут, по которому пакеты для адреса 10.1.10.0 будут передаваться на интерфейс системы OS/400 10.1.1.2; это определяет непрактичность данного способа. Если в локальной сети находится много клиентских систем, необходимо задать большое число маршрутов.

Для того чтобы настроить передачу данных в виртуальной сети Ethernet на основе маршрутизации TCP/IP, необходимо выполнить следующие действия:

1. Включение обмена данными между логическими разделами на основе виртуальной сети Ethernet
2. Создание описаний линий Ethernet
3. Включение пересылки IP-дейтаграмм
4. Создание интерфейсов

Этап 1: Включение обмена данными между логическими разделами на основе виртуальной сети Ethernet

Примечание: В том случае, если применяются не только серверы моделей 270 и 8*xx*, необходимо выполнить эти действия с помощью Консоли аппаратного обеспечения сервера eServer (HMC), а не основного раздела. Дополнительная информация приведена в разделе Виртуальная сеть Ethernet.

Для включения виртуальной сети Ethernet необходимо:

1. В командной строке основного раздела (раздела A) ввести `STRSST` и нажать Enter.
2. Ввести ИД пользователя и пароль сервисных средств.
3. В меню системного инструментария (SST) выбрать опцию 5 (Работа с разделами системы).
4. В меню Работа с разделами системы выбрать опцию 3(Работа с конфигурацией разделов).
5. Нажать F10 (Работа с виртуальными сетями Ethernet).
6. Ввести 1 в соответствующем столбце для раздела A и раздела B, чтобы включить обмен данными между разделами на основе виртуальной сети Ethernet.
7. Выйти из меню Системного инструментария (SST) и вернуться в командную строку.

Дальнейшие действия:

Создание описаний линий Ethernet

Этап 2: Создание описаний линий Ethernet

Создать описания можно одним из двух способов, в зависимости от модели сервера. Выберите способ, соответствующий применяемой модели сервера.

- Создание описаний линий Ethernet на серверах моделей 270 и 8*xx*
- Создание описаний линий Ethernet на серверах других моделей (отличных от 270 и 8xx)

Создание описаний линий Ethernet на серверах моделей 270 и 8*xx*

Для настройки новых описаний линий Ethernet, поддерживающих виртуальные сети Ethernet, выполните следующие действия:

1. В командной строке раздела A введите команду `WRKHDWRSC *CMN` и нажмите Enter.
2. В меню Работа с ресурсами связи выберите опцию 7 (Показать сведения о ресурсах) для нужного виртуального порта Ethernet.

   Виртуальный ресурс Ethernet - это порт Ethernet с обозначением 268C. У каждой виртуальной линии Ethernet, подключенной к логическому разделу, есть один виртуальный ресурс.
3. Пролистайте меню Показать сведения о ресурсах и найдите адрес порта. Адрес порта соответствует виртуальной линии Ethernet, выбранной во время настройки логического раздела.
4. В меню Работа с ресурсами связи выберите опцию 5 (Работа с описаниями конфигураций) для нужного виртуального порта Ethernet и нажмите Enter.
5. В меню Работа с описаниями конфигураций выберите опцию 1 (Создать) и нажмите Enter для перехода к меню Создать описание линии Ethernet (CRTLINETH).

a. В поле *Описание линии* введите VETH0. Несмотря на то, что имя VETH0 выбрано произвольно, оно соответствует пронумерованному столбцу на странице Виртуальная линия Ethernet, на которой вы включили обмен данными между логическими разделами. Указав VETHO также в качестве имени описания линий и имени связанной виртуальной сети Ethernet, вы сможете легко отслеживать конфигурации виртуальных линий Ethernet.

b. В поле *Быстродействие линии* введите 1G.

c. В поле *Дуплекс* укажите *FULL и нажмите Enter.

d. В поле *Максимальный размер кадра* укажите 8996 и нажмите Enter. Применение этого значения позволяет повысить скорость передачи данных в виртуальной сети Ethernet.

На экране будет показано сообщение о создании описания линии.

6. Включите описание линии. Для этого введите команду WRKCFGSTS *LIN и выберите опцию 1 (Включить) для описания VETH0.
7. Для того чтобы создать описание линии Ethernet раздела B, повторите действия 1 - 6 в командной строке раздела B.

Имена всех описаний линий можно выбирать произвольно; тем не менее, рекомендуется использовать одно и то же имя для всех описаний линий, связанных с виртуальной сетью Ethernet. В данном сценарии все описания линий имеют имя VETH0.

Дальнейшие действия:

Включение пересылки IP-дейтаграмм

Создание описаний линий Ethernet на серверах других моделей (отличных от 270 и 8xx)

Для настройки новых описаний линий Ethernet, поддерживающих виртуальные сети Ethernet, выполните следующие действия:

1. В командной строке раздела A введите команду WRKHDWRSC *CMN и нажмите Enter.
2. В меню Работа с ресурсами связи выберите опцию 7 (Показать сведения о ресурсах) для нужного виртуального порта Ethernet.

Виртуальные ресурсы Ethernet - это порты Ethernet с обозначением 268C. У каждой виртуального адаптера Ethernet есть один виртуальный ресурс. С каждым портом 268C связан код расположения, который создается при создании виртуального адаптера Ethernet с помощью HMC (этап 1).

3. Пролистайте меню Показать сведения о ресурсах и найдите ресурс 268C, связанный с кодом расположения, созданным для данного описания виртуальной линии Ethernet.
4. В меню Работа с ресурсами связи выберите опцию 5 (Работа с описаниями конфигураций) для нужного виртуального ресурса Ethernet и нажмите Enter.
5. В меню Работа с описаниями конфигураций выберите опцию 1 (Создать) и нажмите Enter для перехода к меню Создать описание линии Ethernet (CRTLINETH).

a. В поле *Описание линии* введите VETH0. Указав VETHO также в качестве имени описания линий и имени связанной виртуальной сети Ethernet, вы сможете легко отслеживать конфигурации виртуальных линий Ethernet.

b. В поле *Быстродействие линии* введите 1G.

c. В поле *Дуплекс* укажите *FULL и нажмите Enter.

d. В поле *Максимальный размер кадра* укажите 8996 и нажмите Enter. Применение этого значения позволяет повысить скорость передачи данных в виртуальной сети Ethernet.

На экране будет показано сообщение о создании описания линии.

6. Включите описание линии. Для этого введите команду WRKCFGSTS *LIN и выберите опцию 1 (Включить) для описания VETH0.
7. Для того чтобы создать описание линии Ethernet раздела B, повторите действия 1 - 6 в командной строке раздела B.

Имена всех описаний линий можно выбирать произвольно; тем не менее, рекомендуется использовать одно и то же имя для всех описаний линий, связанных с виртуальной сетью Ethernet. В данном сценарии все описания линий имеют имя VETH0.

Дальнейшие действия:

Включение пересылки IP-дейтаграмм

Этап 3: Включение пересылки IP-дейтаграмм

Для передачи пакетов между подсетями включите пересылку IP-дейтаграмм.

Для того чтобы включить пересылку IP-дейтаграмм, выполните следующие действия:

1. В командной строке раздела A введите `CHGTCPA` и нажмите F4.
2. Когда на экране появится вопрос о *пересылке IP-дейтаграмм*, введите ответ `*YES`.

Дальнейшие действия:

Создание интерфейсов

Этап 4: Создание интерфейсов

Для создания интерфейсов TCP/IP выполните следующие действия:

1. Создайте интерфейс TCP/IP OS/400 в разделе A:
   a. В командной строке раздела A введите `CFGTCP` и нажмите Enter для перехода к меню Настройка TCP/IP.
   b. Выберите опцию 1 (Работа с интерфейсами TCP/IP) и нажмите Enter.
   c. Выберите опцию 1 (добавить) и нажмите Enter для перехода к меню Добавить интерфейс TCP/IP (ADDTCPIFC).
   d. В поле *IP-адрес* укажите `'10.1.1.2'`.
   e. В поле *Описание линии* укажите имя описания линии, например, ETHLINE.
   f. В поле *Маска подсети* укажите `'255.255.255.0'`.
2. Запустите интерфейс. Для этого в меню Работа с интерфейсами TCP/IP выберите опцию 9 (Запустить) для данного интерфейса.
3. Для того чтобы создать и запустить интерфейсы TCP/IP в разделах A и B, выполните инструкции, приведенные для этапов 2 и 3.

   Эти интерфейсы применяются в виртуальной сети Ethernet. Присвойте данным интерфейсам IP-адреса 10.1.10.1 и 10.1.10.2 с маской подсети 255.255.255.0.

Особенности виртуальных сетей Ethernet

Виртуальные сети Ethernet могут применяться в качестве альтернативного способа обмена данными между разделами, позволяя не соединять их с помощью сетевых адаптеров. Благодаря этому можно создавать высокоскоростные соединения между логическими разделами без покупки дополнительного аппаратного обеспечения. Для каждого из 16 включенных портов в системе создается виртуальный порт связи Ethernet, например, CMN*xx*, с типом ресурса 268C. При этом логические разделы, подключенные к общей локальной сети (LAN), могут обмениваться данными с помощью этого соединения. Физическая система позволяет настроить до 16 различных виртуальных локальных сетей. Виртуальная сеть Ethernet поддерживает те же функциональные возможности, что и сетевой адаптер Ethernet с пропускной способностью 1 Гбит/с. Виртуальная сеть Ethernet не поддерживает сети Token-Ring, а также сети Ethernet с пропускной способностью 10 и 100 Мбит/с.

Виртуальная сеть Ethernet - это экономичное сетевое решение, обладающее следующими преимуществами:

- Экономичность: Для его реализации не требуется почти никакого дополнительного сетевого оборудования. Создавать на сервере дополнительные разделы и подключать их к внешней локальной сети можно без установки дополнительных физических сетевых адаптеров. Если число свободных разъемов на сервере, в которые можно установить дополнительные адаптеры LAN, ограничено, то виртуальная сеть Ethernet позволяет управлять подключенными к сети разделами без модернизации сервера.
- Гибкость: Данная технология позволяет настроить до 16 отдельных соединений, с помощью которых можно создавать различные маршруты обмена данными между разделами. В логических разделах могут быть реализованы как виртуальная сеть Ethernet, так и физическое соединение с локальной сетью, что обеспечивает высокую гибкость конфигурации. Эта функция часто применяется при размещении в разделе с Linux приложения-брандмауэра.
- Высокое быстродействие: Виртуальная сеть Ethernet эмулирует соединение Ethernet с пропускной способностью 1 Гбит/с и обеспечивает быстрый и надежный обмен данными между разделами. Благодаря этому возникают дополнительные возможности интеграции отдельных приложений, работающих в разных логических разделах.
- Универсальность: В виртуальную сеть Ethernet можно объединять разделы, работающие под управлением как OS/400, так и Linux.
- Снижение нагрузки на сеть: Если обмен данными между разделами осуществляется с помощью виртуальной сети Ethernet, то значительно снижаются объемы данных, передаваемых по внешней локальной сети. Если внешняя сеть также является сетью Ethernet, в работе которой могут возникать конфликты, то применение виртуальной сети Ethernet позволит избежать падения качества обслуживания других пользователей сети.

Глава 9. Дополнительная информация о настройке TCP/IP

После того как вы настроите и запустите систему, у вас может возникнуть вопрос о дальнейших действиях. Ниже перечислены ссылки на книги и руководства фирмы IBM (в формате PDF), а также на разделы Information Center, содержащие дополнительную информацию о настройке TCP/IP. Вы можете просмотреть или напечатать документы в формате PDF. Для правильной настройки TCP/IP на сервере iSeries ознакомьтесь с информацией из следующих источников:

Книги

- **Справочник по настройке TCP/IP** (592 Кб)
  Эта книга содержит информацию о настройке протокола TCP/IP, а также о работе в сети и об управлении сетью.

- **Советы по организации защиты iSeries** (1 Мб)
  Данное руководство содержит рекомендации по защите сервера iSeries.

Руководства

- **TCP/IP Tutorial and Technical Overview** (7 Мб)
  Это руководство содержит основную информацию о стеке протоколов TCP/IP.

- **TCP/IP for AS/400: More Cool Things Than Ever** (9 Мб)
  Это руководство содержит расширенный список стандартных приложений и служб TCP/IP.

IPv6

- **Рабочая группа Internet (IETF)** (http://www.ietf.cnri.reston.va.us/)
  На этом Web-сайте приведена информация о Рабочей группе Internet, которая занимается разработкой протокола Internet (в том числе, IPv6).

- **IP версии 6 (IPv6)** (http://playground.sun.com/pub/ipng/html/ipng-main.html)
  На этом Web-сайте приведены спецификации протокола IPv6 и ссылки на другие источники информации об IPv6.

- **Форум IPv6**(http://www.ipv6forum.com/)
  На этом Web-сайте можно найти самую свежую информацию об изменениях и дополнениях, внесенных в протокол IPv6.

Прочая информация

- **TCP/IP**
  Этот раздел содержит сведения о приложениях и службах TCP/IP, не связанных с настройкой.

Для сохранения документа в формате PDF на рабочей станции:

1. В окне браузера щелкните правой кнопкой мыши на имени документа PDF (на приведенной выше ссылке).
2. Выберите пункт **Сохранить как...**.
3. Перейдите в каталог, выбранный для хранения документа PDF.
4. Нажмите кнопку **Сохранить**.

Если вам необходима программа Adobe Acrobat Reader для просмотра или печати документов PDF, вы можете загрузить экземпляр этой программы с Web-сайта фирмы Adobe

(www.adobe.com/prodindex/acrobat/readstep.html)  .

Часть 2. Приложения

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
| North Castle Drive
| Armonk, NY 10504-1785
| 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 106-0032, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: ФИРМА 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, Лицензионного соглашения на машинный код IBM или любого
| другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в управляемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления, касающиеся намерений и планов IBM, могут изменяться и отзываться без предварительного уведомления, и отражают только текущие цели и задачи.

Данный документ содержит примеры данных и отчетов, применяемых в повседневных бизнес-операциях. Для более наглядной демонстрации примеры содержат имена людей, названия компаний, товарных знаков и продуктов. Все имена и названия вымышлены и любое совпадение или аналогии с реальными именами и адресами является случайным.

При просмотре данного документа в электронном виде фотографии и цветные иллюстрации могут не отображаться.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:

AS/400
e(эмблема)server
eServer
IBM
iSeries
OS/400
Redbooks

Microsoft, Windows, Windows NT и логотип Windows являются товарными знаками корпорации Microsoft 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 выбранной для загрузки информации предоставляется в соответствии с следующими условиями и при подтверждении вашего с ними согласия.

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

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

На эту информацию, а также на содержащиеся в ней 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 случае, если, по мнению IBM, использование этой информации может нанести 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 этой информации. Информация предоставляется на условиях ″как есть″, без каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности, соблюдения авторских прав или пригодности для каких-либо конкретных целей.

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

Напечатано в Дании