IBM

eserver

iSeries

Оптимизация маршрутизации TCP/IP и распределение нагрузки

Версия 5, выпуск 3

IBM

@server

iSeries

Оптимизация маршрутизации TCP/IP и распределение нагрузки

Версия 5, выпуск 3

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 29.

Пятое издание (август 2005 года)

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

Содержание

Оптимизация маршрутизации TCP/IP и распределение нагрузки

Существует несколько способов оптимизировать маршрутизацию данных TCP/IP и распределить нагрузку на сервер iSeries. Встроенные функции маршрутизации сервера iSeries позволяют не использовать внешний маршрутизатор при работе с сетями TCP/IP.

Ознакомившись с описанием способов оптимизации маршрутизации и распределения нагрузки, вы узнаете о некоторых новых возможностях сервера iSeries. В описании каждого способа приведен рисунок, наглядно демонстрирующий, каким образом устанавливаются соединения. Однако эти описания не содержат инструкций по настройке указанных способов маршрутизации. Основное внимание уделено принципам, которыми необходимо руководствоваться при настройке маршрутизации для оптимизации работы сервера iSeries.

Для чего нужна оптимизация маршрутизации?

Описанные способы позволяют уменьшить общие затраты на установление соединений за счет сокращения числа внешних маршрутизаторов и серверов. Реализация этих способов маршрутизации позволяет освободить часть имеющихся IP-адресов за счет более эффективного использования оставшихся. Ознакомившись со способами распределения нагрузки, связанной с передачей данных по сети, вы можете повысить производительность сервера iSeries.

Как напечатать этот раздел?

Для того чтобы вам было удобнее читать, напечатайте этот раздел. Для этого выполните инструкции, приведенные под заголовком “Как напечатать этот раздел” на стр. 2.

Предварительные действия

Если вы не знакомы с принципами настройки маршрутизации и распределения нагрузки в системе iSeries, то предварительно ознакомьтесь со следующими разделами:

Раздел “Функции маршрутизации TCP/IP в различных выпусках” на стр. 2 содержит информацию о функциях маршрутизации, предусмотренных в различных выпусках сервера iSeries. С его помощью вы можете узнать, какие функции доступны на вашем сервере.

Раздел “**Обработка пакетов**” на стр. 2 содержит информацию о том, каким образом сервер iSeries обрабатывает пакеты данных.

Раздел “Общие правила маршрутизации” на стр. 4 позволяет получить представление об основных правилах маршрутизации пакетов в системе iSeries. Знание этих правил потребуется вам при знакомстве с различными способами маршрутизации.

Выбор способа маршрутизации?

Вам на выбор предоставлено несколько способов маршрутизации. Решите, какой из этих способов лучше всего подойдет для вашей сети, и реализуйте его с учетом особенностей этой сети:

Раздел “**Способы маршрутизации**” на стр. 4 рассказывает о том, каким образом сервер iSeries выполняет маршрутизацию данных.

Раздел “**Способы распределения нагрузки TCP/IP**” на стр. 22 содержит информацию о функциях TCP/IP, которые могут быть использованы для распределения нагрузки, связанной с передачей данных через сервер iSeries.

Дополнительная информация о маршрутизации данных TCP/IP на сервере iSeries

Более подробные сведения по этой теме приведены в разделе “Дополнительная информация об оптимизации маршрутизации TCP/IP и распределении нагрузки” на стр. 27.

Как напечатать этот раздел

Вы можете просмотреть версию этого документа в формате PDF или загрузить ее для печати. Для просмотра файлов в формате необходима программа Adobe(R) Acrobat(R) Reader. Копию этой программы можно бесплатно загрузить с Web-сайта Adobe(R) Acrobat(R). 

Для просмотра или загрузки документа в формате PDF, щелкните на ссылке Оптимизация маршрутизации и распределение нагрузки (приблизительно 719 KB).

Для того чтобы сохранить документ PDF для последующего просмотра или печати, выполните следующие действия:

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

Функции маршрутизации TCP/IP в различных выпусках

Ниже перечислены функции, поддерживаемые серверами iSeries(TM) с различными выпусками операционной системы. Перед тем как вы окончательно определитесь с выбором функции маршрутизации, которую вы решите реализовать в своей системе, убедитесь, что эта функция поддерживается в текущем выпуске операционной системы. В некоторых случаях требуемого результата можно добиться другими способами.

V3R1: Пересылка пакетов, основанная на статических маршрутах.

V3R7/V3R2: Протокол SLIP, маршрутизация с помощью Протокола преобразования адресов Proxy (ARP), а также поддержка ненумерованных сетевых соединений.

V4R1: Протокол динамической информации о маршрутизации версии 1 (RIPv1).

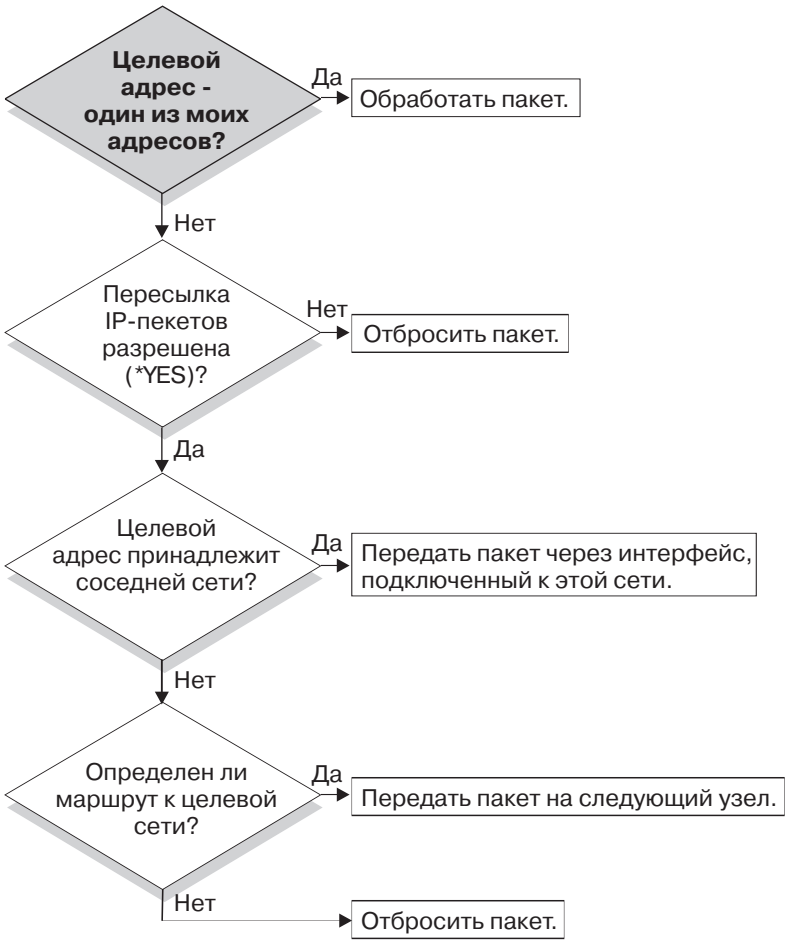
V4R2: Протокол динамической информации о маршрутизации версии 2 (RIPv2), прозрачный доступ к подсетям, распределение нагрузки по нескольким маршрутам.

V4R3: Виртуальные IP-адреса, сокрытие IP-адресов, преобразование сетевых адресов (NAT), бесклассовая междоменная маршрутизация (CIDR).

V4R4: Создание соединений IP с помощью OptiConnect.

Обработка пакетов

Получив представление о том, каким образом сервер обрабатывает пакеты, вам будет проще настроить маршрутизацию в системе. Ниже показана упрощенная схема обработки пакета IP (дейтаграммы) на сервере iSeries(TM). Некоторые действия могут выполняться сервером в другом порядке, однако результат обработки пакета будет таким же. В этом разделе описана процедура обработки пакетов, которая применяется по умолчанию. Если в системе настроены дополнительные средства маршрутизации, то процедура обработки пакетов может несколько отличаться от указанной.



RZAJW523-0

Сначала адрес получателя из заголовка IP сравнивается со всеми адресами, определенными в системе. Если пакет предназначен для данной системы, он передается протоколу более высокого уровня, например, TCP, а затем - приложению, которое работает с целевым портом.

Если пакет не предназначен для данной системы, то проверяется значение атрибута пересылки пакетов IP. Если он равен *YES, то данная система настроена для пересылки пакетов в качестве маршрутизатора. Если в атрибутах TCP/IP или в профайле PPP значение этого параметра равно *NO, то пакет удаляется.

Выполняется поиск адреса получателя в записях о маршрутах типа *DIRECT, определенных в системе. Для этого адрес получателя пакета добавляется к маске подсети, указанной в записях о маршрутизации *DIRECT, связанных с интерфейсами системы. Если адрес будет найден, то пакет должен быть передан в одну из сетей, к которым данная система подключена напрямую. Вначале просматриваются те записи о маршрутах, в которых маршрут описан наиболее точно.

Если сервер iSeries не подключен к удаленному хосту напрямую, то выполняется поиск в таблице маршрутизации. Записи просматриваются в порядке увеличения размера сети, к которой относится маршрут (начиная с маски подсети 255.255.255.255, и заканчивая маской подсети 0.0.0.0). Если маршрут найден, то пакет пересылается шлюзу следующего транзитного узла.

Последняя точка на схеме указывает, что если маршрут для пересылки пакета не найден, то пакет удаляется.

Общие правила маршрутизации

Существует несколько основных правил, применяемых к протоколу TCP/IP в целом, и, в частности, к TCP/IP на сервере iSeries(TM). Эти правила следует учитывать при работе с функциями маршрутизации сервера iSeries. Они помогут вам определить, что происходит с пакетами в вашей системе и там, куда они направляются. Как и из большинства правил, из них существуют исключения.

1. У вашей системы нет IP-адреса; IP-адреса существуют только у интерфейсов.

   Исключением из этого правила являются виртуальные IP-адреса (без установки соединения), присвоенные системе. Запуск виртуального IP возможен в системе V4R3.

2. В общем, если целевой IP-адрес определен в вашей системе, системе обработает его вне зависимости от того, от какого интерфейса пришел данный пакет.

   В данном случае исключением является случай, когда адрес связан с ненумерованным интерфейсом, или же если активны IP NAT или фильтрация; в этом случае пакет может быть переслан или аннулирован.

3. IP-адрес и маска определяют адрес подключенной сети.

4. Маршрут вне системы выбирается на основе связанного с интерфейсом сетевого адреса. Выбор маршрута основывается на следующих элементах:

- Порядок поиска группы маршрутов: прямые маршруты, маршруты в подсети, а затем маршруты по умолчанию.
- Внутри группы выбирается маршрут с наиболее подходящей маской подсети.
- Одинаково подходящие маршруты выбираются в зависимости от порядка их следования в списке или метода распределения загрузки.
- Маршруты могут быть добавлены вручную или динамически системой.

Способы маршрутизации

Маршрут определяет путь, по которому может быть установлено соединение для передачи данных от отправителя получателю, а также способ создания этого соединения. В этом разделе перечислены ссылки на информацию о различных способах маршрутизации, которые могут применяться на сервере iSeries(TM).

- “Маршрутизация двухточечных соединений” на стр. 5
  Двухточечное соединение устанавливается между локальной и удаленной системой, либо между локальной и удаленной сетью. В данном разделе описаны два способа настройки IP-адресов при создании двухточечного соединения.
- “Маршрутизация с помощью Протокола преобразования адресов Proxy” на стр. 8
  Протокол преобразования адресов (ARP) Proxy обеспечивает возможность передачи данных между физическими сетями, не требуя создания логической сети или обновления таблиц маршрутизации. Дополнительно в этом разделе приведено описание прозрачных подсетей, которые являются расширением протокола ARP Proxy.
- “Динамическая маршрутизация” на стр. 10
  Динамическая маршрутизация обеспечивает автоматическое обновление таблиц маршрутизации при изменении конфигурации сети.
- “Связывание маршрутов” на стр. 11
  Связывание маршрутов позволяет задать интерфейс для отправки пакетов, содержащих ответ на сообщение.
- “Бесклассовая междоменная маршрутизация” на стр. 12
  Бесклассовая междоменная маршрутизация позволяет сократить размер таблиц маршрутизации и увеличить число свободных IP-адресов.

- “Маршрутизация с помощью виртуальных IP-адресов” на стр. 13
  Системе можно присвоить один или несколько виртуальных IP-адресов, не связанных с физическим интерфейсом. За счет этого, в частности, можно запустить несколько экземпляров Web-сервера Domino(TM), связанных с различными адресами, или другой службы, которая работает с портом по умолчанию.
- “Устойчивость к сбоям” на стр. 14
  В этом разделе описано несколько способов восстановления маршрута после сбоя маршрутизатора.
- “**Маршрутизация с преобразованием сетевых адресов**” на стр. 15
  Такой способ маршрутизации может применяться для защиты внутренней сети при подключении к внешним сетям, например, Internet. Функция NAT позволяет скрыть IP-адреса локальных компьютеров. В этом разделе описаны различные типы NAT, поддерживаемые сервером iSeries, и сферы их использования.
- “Маршрутизация в системе несколькими разделами с помощью OptiConnect” на стр. 19
  Продукт OptiConnect позволяет подключить несколько серверов iSeries к высокоскоростной оптоволоконной шине передачи данных. В этом разделе приведена информация о работе с OptiConnect в системе с несколькими логическими разделами.

Маршрутизация двухточечных соединений

Двухточечные соединения обычно используются для соединения двух систем в глобальной сети (WAN). Такое соединение может быть установлено между локальной и удаленной системой, либо между локальной и удаленной сетью. Не стоит смешивать понятия Двухточечный протокол и двухточечное соединение. Двухточечный протокол (PPP) определяет один из типов двухточечных соединений, которые обычно применяются для подключения компьютера к Internet. Дополнительная информация о настройке соединений PPP и работе с ними приведена в разделе Соединения PPP.

Двухточечные соединения могут устанавливаться по телефонным линиям, выделенным линиям или в сетях другого типа, например, Frame Relay. Существует два способа настройки IP-адресов для двухточечного соединения: нумерованное соединение и ненумерованное соединение. Как следует из названия, при установлении нумерованных соединений для каждого интерфейса определяется уникальный IP-адрес. Для установления ненумерованного соединения дополнительный IP-адрес не требуется.

Нумерованные сетевые соединения:

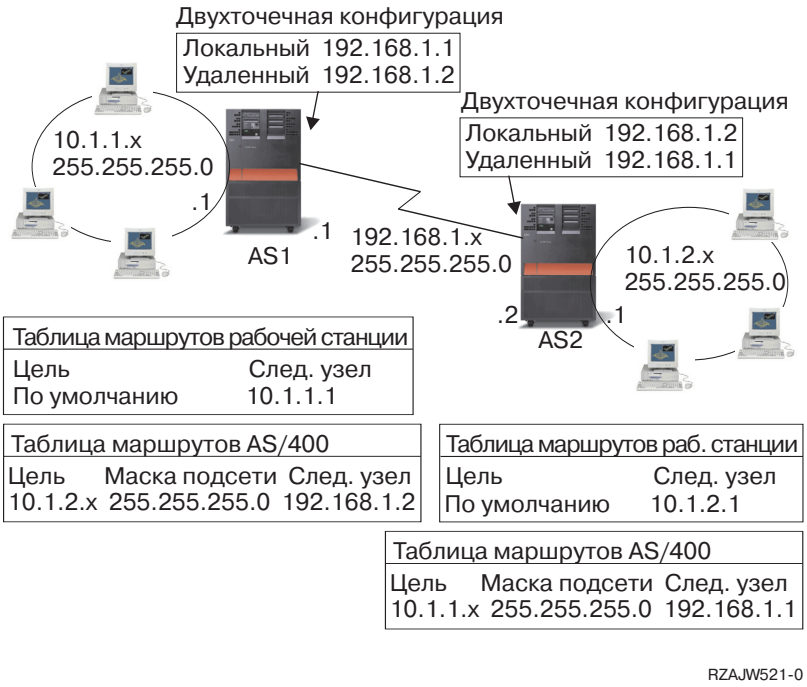
На первый взгляд, самый простой способ настройки двухточечного соединения - это создание нумерованного соединения. В определении нумерованного соединения для каждого конечного узла определен уникальный IP-адрес.

Ниже перечислены некоторые особенности, которые следует учитывать при работе с нумерованными двухточечными соединениями:

- Компьютерам, между которыми устанавливается соединение, назначены уникальные IP-адреса.
- В систему должны быть добавлены операторы маршрутизации, перенаправляющие поток данных в удаленную систему.
- Адреса в двухточечном соединении должен задавать администратор сети.
- Адреса могут применяться только для соединения двух систем.

После того как двухточечное соединение будет определено на сервере iSeries(TM), на одном из конечных узлов соединения необходимо создать запись маршрутизации, описывающую маршруты ко всем сетям, к которым подключен другой конечный узел. Процесс выбора маршрута зависит от того, присвоены ли интерфейсам сервера iSeries уникальные IP-адреса. Все адреса и маршруты должен задать администратор сети. В сети небольшого размера несложно вручную настроить все адреса, так как их число обычно невелико. Однако в большой сети для определения интерфейса конечной системы может потребоваться создать отдельную подсеть.

На следующем рисунке изображено нумерованное сетевое соединение между двумя серверами iSeries. Если вам необходимо просто установить соединение между системами AS1 и AS2, то запись маршрутизации создавать не нужно. Если же планируете подключаться к системам удаленной сети (10.1.2.x), то в обеих конечных системах нужно добавить запись маршрутизации, указанную на рисунке. Это связано с тем, что соединение с сетью 192.168.1.x проходит через удаленную сеть 10.1.2.x.



RZAJW521-0

Ненумерованные сетевые соединения:

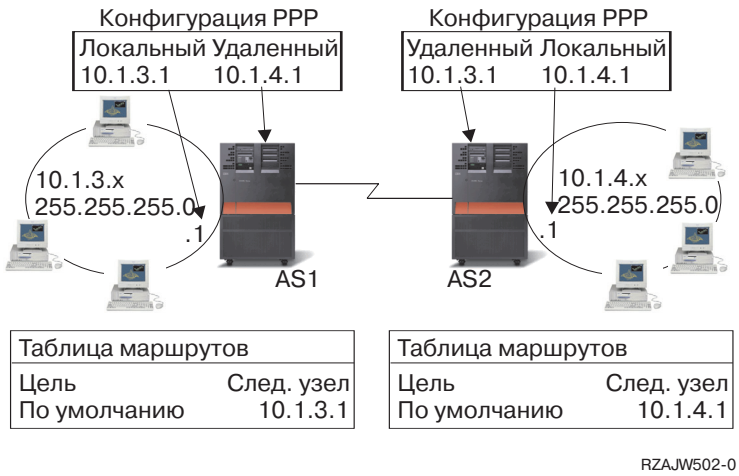
Для настройки ненумерованного соединения требуется выполнить более сложную процедуру, чем в случае с нумерованным соединением. Однако в дальнейшем вы сэкономите время на обслуживании такого соединения.

Процесс выбора маршрута зависит от того, назначен ли IP-адрес интерфейсу сервера iSeries. При настройке ненумерованного соединения двухточечному интерфейсу не присваивается уникальный адрес. Фактически интерфейсу сервера iSeries, через который устанавливается ненумерованное соединение, присваивается IP-адрес удаленной системы.

При работе с ненумерованным соединением следует учитывать следующие особенности:

- Двухточечному интерфейсу присваивается адрес, относящийся к удаленной сети.
- В системе не нужно добавлять записи маршрутизации.
- Поскольку администратору не нужно задавать IP-адрес соединения, процедура управления сетью становится значительно проще.

В следующем примере интерфейс системы AS1 логически относится к сети 10.1.4.x, а интерфейс системы AS2 - к сети 10.1.3.x. В локальной сети 10.1.3.x системе AS1 присвоен адрес 10.1.3.1. Следовательно, система AS1 может напрямую подключаться к любой системе в сети 10.1.3.x.

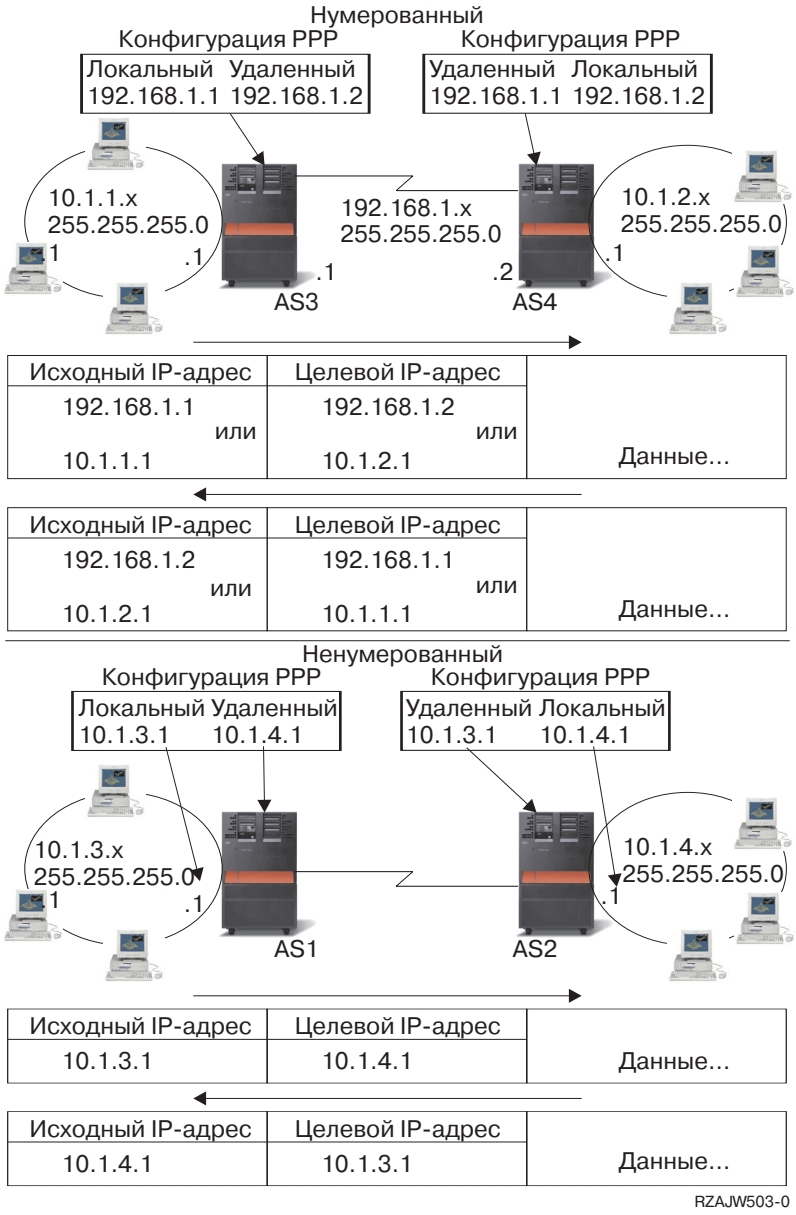


Требуется настроить соединение системы AS1 с системой AS2. В локальной сети 10.1.4.x системе AS2 присвоен адрес 10.1.4.1. Следовательно, система AS2 может напрямую подключаться к любой системе в сети 10.1.4.x. В системах AS1 и AS2 удаленный адрес должен быть добавлен в таблицу маршрутизации в качестве локального интерфейса. Пакеты, отправленные по этому адресу, не будут обрабатываться локальной системой. Они будут передаваться через интерфейс удаленной системе. Процедура обработки пакетов будет выполняться удаленной системой.

Теперь нужно настроить соединения системы AS1 с сетью 10.1.4.x и системы AS2 с сетью 10.1.3.x. Если бы эти две системы были расположены в одном помещении, можно было бы просто добавить к каждой системе сетевой адаптер и подключить новый интерфейс к локальной сети. В этом случае в системах AS1 и AS2 не требовалось бы добавлять записи маршрутизации. Однако в данном примере системы находятся в разных городах, поэтому необходимо настроить двухточечное соединение. Но даже в этом случае хотелось бы избежать создания записей маршрутизации. Этого можно достичь, создав определение ненумерованного двухточечного соединения (PPP). В этом случае для определения маршрута будет применяться IP-адрес удаленной системы.

Передача данных по нумерованному и ненумерованному соединению:

На следующем рисунке показаны адреса, применяемые при работе с нумерованным и ненумерованным соединением. В верхней области рисунка показано, что для подключения к удаленной системе по нумерованному соединению могут применяться адреса 192.168.1.2 и 10.1.2.1. Это связано с тем, что в системе AS3 существует запись маршрутизации, в которой в качестве следующего транзитного узла для пакетов, отправленных системе 10.1.2.1, указана система 192.168.1.2. В пакете, содержащем ответ, указываются адреса, взятые из исходного пакета. В нижней области рисунка указаны адреса, которые применяются для установления ненумерованного соединения. Пакет отправляется от системы 10.1.3.1 системе 10.1.4.1. Для передачи пакета не требуются записи маршрутизации, так как двухточечное соединение устанавливается через интерфейс, которому назначен адрес удаленной системы.



RZAJW503-0

Маршрутизация с помощью Протокола преобразования адресов Proxy

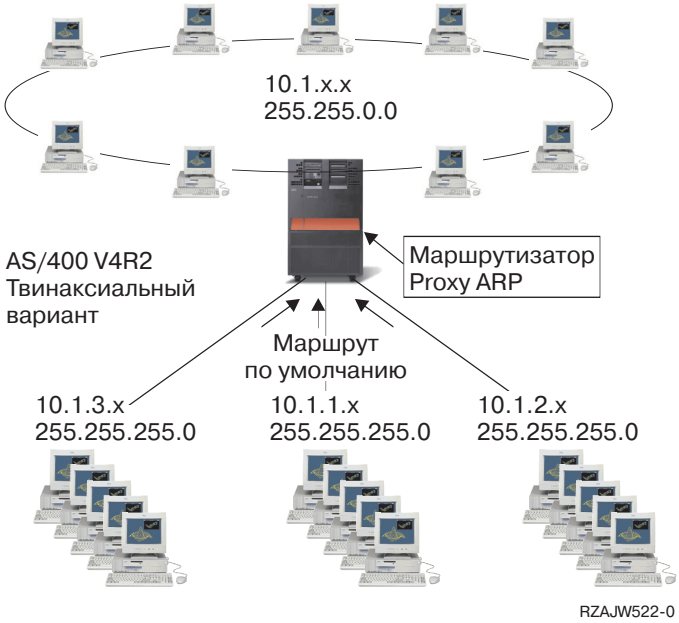
Маршрутизация с помощью протокола преобразования адресов (ARP) Proxy позволяет представить несколько физических сетей в виде одной логической сети. Такая маршрутизация позволяет обеспечить возможность передачи данных между физическими сетями, не создавая новую логическую сеть и не обновляя таблицы маршрутизации. Протокол ARP Proxy позволяет локальным системам работать с внешними системами так, как будто они подключены к локальной сети. Это свойство позволяет предоставить всей сети возможность подключения к внешним системам через коммутируемое соединение. На следующем рисунке показан возможный сценарий работы. Сеть 10.1.1.x - это локальная сеть, а компьютеры 10.1.1.65 по 10.1.1.68 - ваши удаленные системы.

Когда локальной системе (10.1.1.x) потребуется отправить данные одной из удаленных систем, она отправит запрос ARP. В результате всем системам, подключенным к сегменту локальной сети, будет разослано оповещающее сообщение, запрашивающее адрес целевой системы. Удаленные системы не получат данное сообщение. В этот момент в действие вступает ARP Proxy. На сервере iSeries(TM) хранится список удаленных систем. Когда сервер iSeries получает запрос ARP на получение адреса одной из удаленных систем, он отправляет в ответ на этот запрос адрес требуемой системы. После этого сервер iSeries получает данные и пересылает их удаленной системе. Для пересылка необходимо, чтобы в параметре Пересылка пакетов IP было указано значение *yes. Если соединение с удаленной системой не установлено, то сервер iSeries не отвечает на запрос ARP, поэтому локальная система не отправляет данные.

Роль Proxy для всей подсети или диапазона хостов может играть “Прозрачный доступ к подсетям”.Функция прозрачного доступа к подсетям позволяет создать фиктивную сеть, которой будут присвоены адреса, не лежащие в адресном пространстве основной сети.

Прозрачный доступ к подсетям

Прозрачные подсети представляют собой расширение протокола ARP Proxy. Прозрачная подсеть работает как отдельный хост. За счет этого появляется возможность подключиться ко всей подсети или группе хостов с адресами из заданного диапазона. На следующем рисунке показано, что внутренним сетям (с 10.1.1.x по 10.1.3.x) присвоены адреса, не входящие в адресное пространство основной сети (10.1.x.x).



Твинаксиальным локальным сетям выделены диапазоны адресов, входящие в диапазон адресов физической локальной сети. В версиях младше V4R2 функции Добавить маршрут TCP/IP и Добавить интерфейс TCP/IP не поддерживали такую возможность. Начиная с версии V4R2 эти ограничения были сняты. Теперь двум интерфейсам из разных сегментов можно присвоить адреса, которые относятся к одному сегменту. Когда сервер iSeries(TM) обнаруживает такие адреса, он автоматически включает функцию ARP Proxy для всех систем, подключенных с помощью твинаксиального контроллера. За счет этого все системы, подключенные к сети 10.1.x.x, могут обмениваться данными с любыми системами подсетей без внесения каких-либо изменений в конфигурацию.

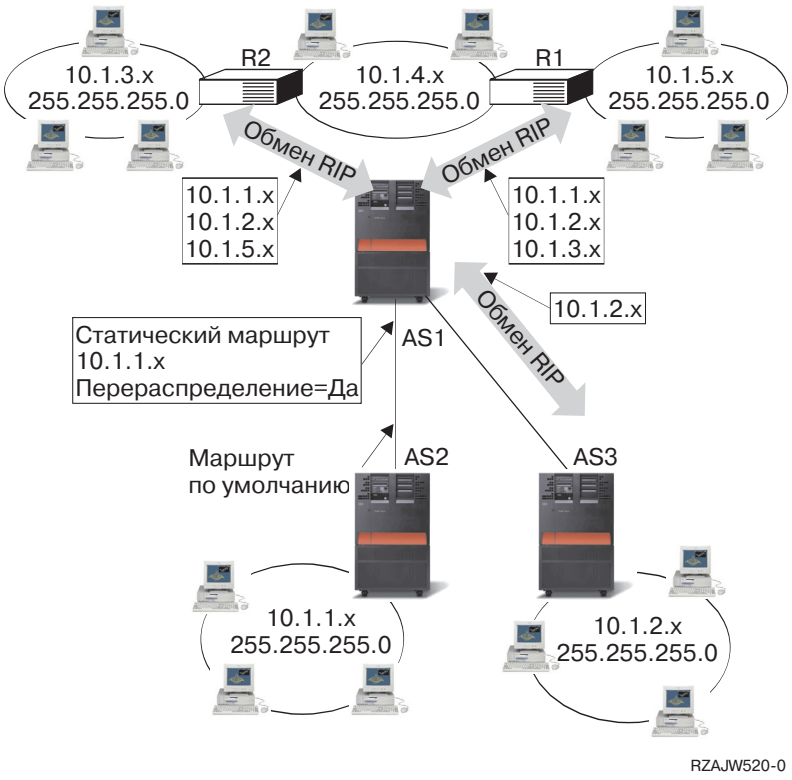
Прозрачный доступ к подсетям через глобальную сеть:

Функция прозрачного доступа к подсетям может быть расширена для управления удаленными локальными сетями. Прозрачный доступ к подсетям через глобальную сеть позволяет логически подключить удаленные сети к локальной подсети. На приведенном выше рисунке три сети подключены к локальной сети 10.1.x.x через сервер iSeries. Все эти сети определены с помощью маски подсети, которая делает их прозрачными для домашней сети. Функция ARP Proxy отвечает на все запросы ARP, отправленные локальными системами, в которых спрашивается адрес системы, расположенной в подсети 10.1.1.x, 10.1.2.x или 10.1.3.x. Все данные, отправляемые локальным компьютерам, автоматически отправляются серверу iSeries, расположенному в локальной сети. Сервер iSeries, в свою очередь, пересылает данные, отправленные локальным компьютером, соответствующему удаленному серверу iSeries. Удаленный сервер iSeries либо обрабатывает данные, либо пересылает их одной из систем в удаленной сети. На удаленных рабочих станциях должен быть задан маршрут по умолчанию, в котором в качестве следующего транзитного узла указан удаленный сервер iSeries. На локальных рабочих станциях не нужно обновлять записи маршрутизации, так как никакие логические сети не создаются.

Динамическая маршрутизация

Функция динамической маршрутизации предоставляется Протоколами внутренних шлюзов (IGP), такими как Протокол информации о маршрутизации (RIP). RIP позволяет настраивать хосты в качестве узлов сети RIP. Процедура настройки такого способа маршрутизации достаточно проста. Кроме того, он обеспечивает автоматическое обновление таблиц маршрутизации при изменении или сбое сети. На сервере iSeries(TM) применяется протокол RIPv2, позволяющий обновлять настроенные в сети маршруты путем обмена пакетами RIP.

На приведенном ниже рисунке в центральной системе (AS1) добавляется статический маршрут, описывающий соединение с сетью 10.1.1.x через систему AS2. Для этого статического маршрута включена опция Рассылка данных о маршрутах. В результате информация об этом маршруте будет добавлена в таблицы других маршрутизаторов и систем. Когда одному из этих маршрутизаторов потребуется передать данные хосту сети 10.1.1.x, он отправит их центральному серверу iSeries (AS1). В системе AS2 запущен сервер маршрутизации, поддерживающий обмен информацией RIP. В этом примере система AS1 отправляет сообщение о том, что система AS2 напрямую подключена к сети 10.1.2.x.



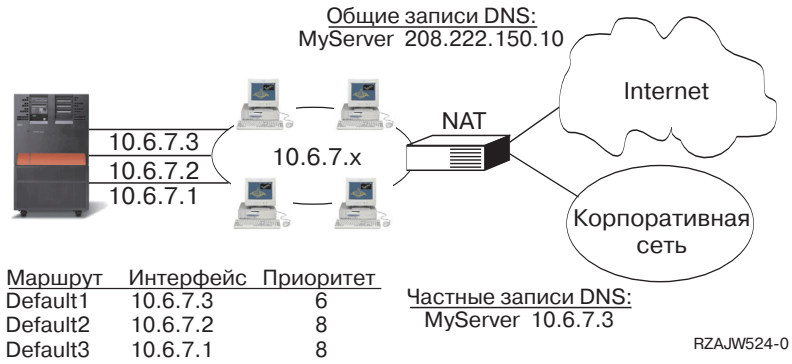
Описание примера

- Система AS1 получает пакет RIP от AS2 и обрабатывает его. Если в системе AS1 не определен маршрут к сети 10.1.2.x, то система сохранит полученный маршрут. Если же в системе определен маршрут к сети 10.1.2.x с таким же или меньшим числом транзитных участков, то информация о новом маршруте не будет сохранена. В этом примере система AS1 сохраняет информацию о маршруте.
- Система AS1 получает от R1 пакет с информацией о маршруте к сети 10.1.5.x. Она сохраняет этот маршрут.
- Система AS1 получает от R2 пакет с информацией о маршруте к сети 10.1.3.x. Она сохраняет этот маршрут.
- В следующий раз система AS1 отправит маршрутизатору R1 сообщение RIP с информацией о тех маршрутах, которые не известны R1. В их число входят маршруты к сетям 10.1.1.x, 10.1.2.x, и 10.1.3.x. Система AS1 не отправляет информацию о маршруте к сети 10.1.4.x, так как ей известно, что хост маршрутизатора R1 напрямую подключен к сети 10.1.4.x. Аналогичная информация будет отправлена маршрутизатору R2 и системе AS3.

Связывание маршрутов

Выбор предпочитаемого интерфейса для связывания позволяет указать, какой интерфейс будет применяться для отправки ответных сообщений. Этот интерфейс задается в параметре Предпочитаемый интерфейс для связывания при добавлении маршрута.

На следующем рисунке приведен пример системы, в которой три интерфейса связаны с одной сетью. Для того чтобы запросы могли приниматься через все интерфейсы, ответные сообщения должны отправляться обратно через тот же интерфейс. Для этого необходимо создать дополнительные маршруты для каждого интерфейса. В данном примере добавляется три маршрута по умолчанию, каждый из которых явно связан с соответствующим интерфейсом. Связи между интерфейсами и маршрутами не зависят от порядка включения и выключения интерфейсов.

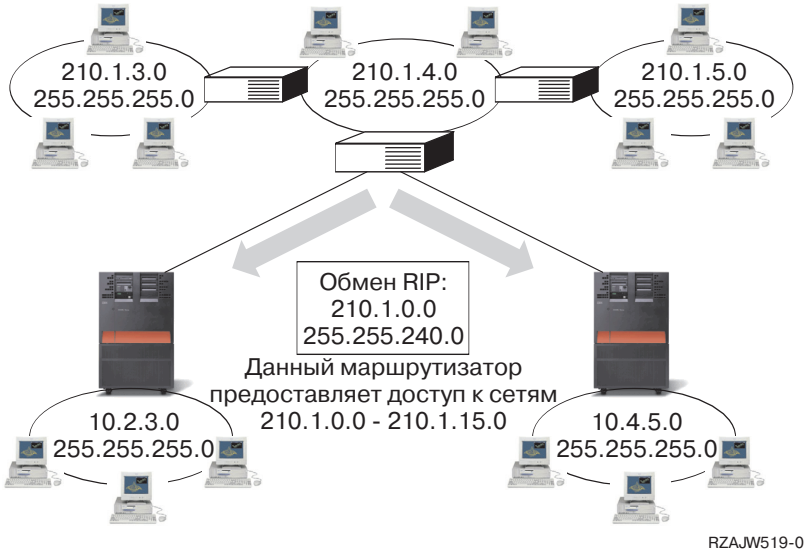


Бесклассовая междоменная маршрутизация

Бесклассовая междоменная маршрутизация (CIDR или supernetting) предоставляет способ для объединения нескольких диапазонов адресов класса C в одну сеть, или маршрут. Такой способ маршрутизации позволяет увеличить число IP-адресов класса C. Эти адреса предоставляются клиентам провайдерами Internet. Адреса CIDR позволяют сократить размер таблиц маршрутизации и увеличить число свободных IP-адресов.

В прошлом требовалось указывать маску подсети, которая равнялась или была больше маски, необходимой для данного класса сетей. Для адресов класса C это значило, что максимальной по размеру была подсеть 255.255.255.0 (253 хоста). Если в какой-то момент в организации становилось больше 253 хостов, то ей выделялись дополнительные адреса класса C. При этом задача настройки маршрутов значительно усложнялась.

Теперь CIDR позволяет объединять смежные адреса класса C в один диапазон сетевых адресов с помощью маски подсети. Например, если у вас есть четыре сетевых адреса класса C (208.222.148.0, 208.222.149.0, 208.222.150.0, и 208.222.151.0 с маской подсети 255.255.255.0), вы можете попросить своего провайдера Internet создать на их основе общую сеть с маской 255.255.252.0. При этом на уровне маршрутизатора четыре сети будут объединены в одну. CIDR позволяет сократить число занятых, но неиспользуемых IP-адресов.

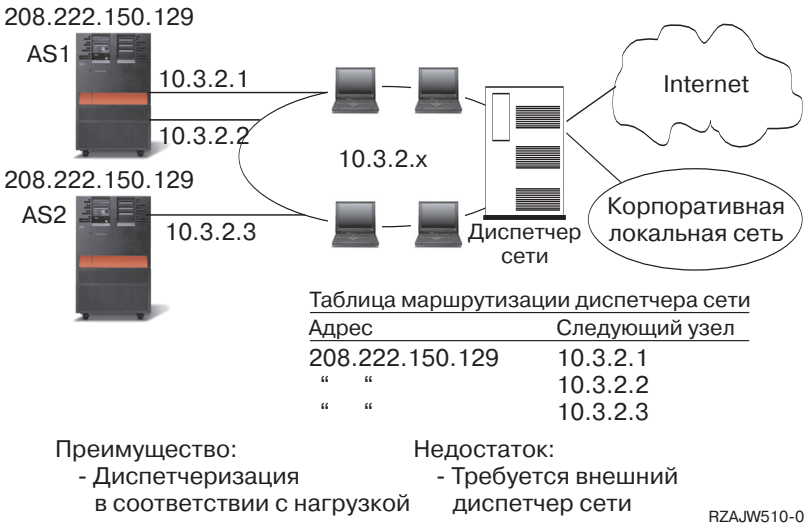


В этом примере маршрутизатор отправляет одно сообщение RIP с адресом сети 210.1.0.0 и маской подсети 255.255.240.0. Таким образом, система будет получать сообщения RIP для сетей с 210.1.0.0 по 210.1.15.0, отправленные через этот маршрутизатор. В данном случае с помощью CIDR вместо шестнадцати сообщений отправляется одно.

Маршрутизация с помощью виртуальных IP-адресов

Виртуальные интерфейсы IP, или циклические интерфейсы, - это мощное средство, которое применяется для решения различных задач. Системе можно присвоить один или несколько виртуальных IP-адресов, не связанных с физическим интерфейсом. За счет этого, в частности, можно запустить несколько экземпляров Web-сервера Domino(TM), связанных с различными адресами, или другой службы, которая работает с портом по умолчанию.

Чаще всего виртуальные IP-адреса применяются в случаях, когда необходимо создать несколько логических каналов для передачи данных между шлюзом и сервером iSeries(TM), например, с целью распределения нагрузки или обеспечения устойчивости к сбоям. Для этого на сервере iSeries необходимо создать несколько дополнительных интерфейсов и приобрести дополнительные IP-адреса. О наличии нескольких интерфейсов должно быть известно только в локальной сети. Удаленным клиентам не должны быть известны все IP-адреса сервера iSeries. В идеальном случае клиентам должен быть известен только один IP-адрес. Удаленный клиент не должен знать, каким образом отправленный им пакет передается через шлюз, локальную сеть и попадает на сервер iSeries. Для того чтобы скрыть эту информацию, применяются виртуальные IP-адреса. Локальные клиенты подключаются к серверу iSeries с помощью любого из физических IP-адресов, в то время как удаленные клиенты подключаются через виртуальный интерфейс IP.



Поддержка виртуальных IP-адресов в основном предназначена для тех серверов iSeries, которые обслуживают удаленных клиентов. Немаловажно, что виртуальный IP-адрес и физические интерфейсы расположены в разных подсетях. Виртуальный IP-адрес позволяет представить сервер во внешней сети в виде отдельного хоста, который не подключен к какой-либо сети или подсети. Для этого маска подсети, связанная с виртуальным интерфейсом IP, должна быть равна 255.255.255.255.

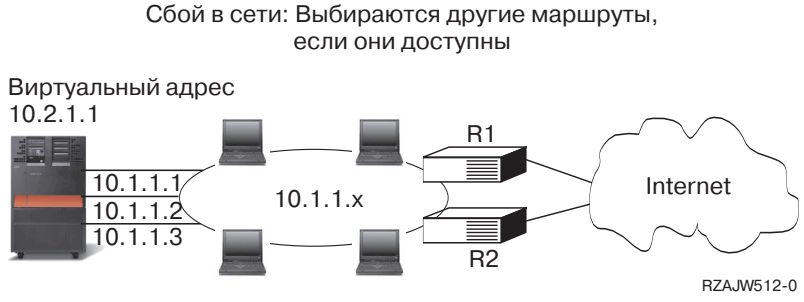
Так как виртуальный IP-адрес не связан с физическим интерфейсом, сервер iSeries никогда не отвечает на запросы Протокола преобразования адресов (ARP) на получение виртуального IP-адреса. Другими словами, невозможно отправить данные по виртуальному IP-адресу. Для того чтобы другие системы могли подключаться с помощью виртуального IP-адреса, в них должен быть определен маршрут к системе с таким адресом. Именно поэтому виртуальные IP-адреса в основном предназначены для работы с удаленными клиентами. В приведенном ниже примере на всех рабочих станциях в качестве следующего промежуточного шлюза задан один из интерфейсов 10.3.2 сервера iSeries. Сервер iSeries обрабатывает все получаемые пакеты. Если адрес получателя совпадает с одним из адресов, определенных в системе (включая виртуальные IP-адреса), то система принимает пакет.

Серверы DNS сообщают клиентам адреса запрошенных серверов. В данном случае все адреса представляют одну и ту же систему. Функция виртуальных IP-адресов может быть использована для объединения нескольких систем в одну систему большего размера.

Устойчивость к сбоям

Виртуальные IP-адреса применяются и для защиты от сбоя маршрутизатора.

В данном примере описано несколько способов восстановления маршрута после сбоя маршрутизатора. Соединение будет максимально надежным, когда в системе определен виртуальный IP-адрес. В этом случае сеанс не будет прерван даже при сбое интерфейса, так как данные смогут передаваться через другие интерфейсы.



Что происходит при сбое маршрутизатора R1?

- Соединения, проходящие через маршрутизатор R1, перенаправляются через маршрутизатор R2.
- После того как работа маршрутизатора R1 будет восстановлена, все данные, направляемые по активным соединениям, продолжат передаваться через маршрутизатор R2.

Что происходит при сбое интерфейса 10.1.1.1?

- Активные соединения с 10.1.1.1 разрываются, однако соединения, установленные через интерфейсы 10.1.1.2, 10.1.1.3, и 10.2.1.1, остаются.
- Повторное связывание маршрута:
  - В версиях младше V4R2: Маршруты с несколькими транзитными участками повторно связываются с интерфейсом 10.1.1.2 или 10.1.1.3.
  - V4R2: Маршруты повторно связываются только в случае, если параметр Предпочитаемый интерфейс связывания равен NONE.
  - В версиях V4R3 и старше: Вам необходимо настроить интерфейс 10.2.1.1 в качестве виртуального IP-адреса и основного адреса системы.
    - Основной IP-адрес системы остается активным.
    - Другие компьютеры могут работать с данной системой до тех пор, пока активен хотя бы один физический интерфейс.

Маршрутизация с преобразованием сетевых адресов

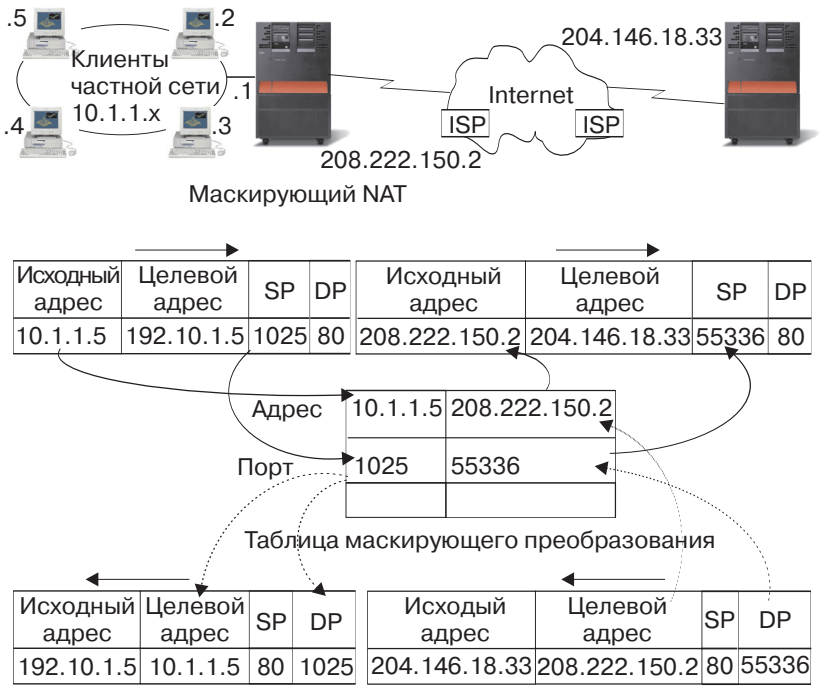
Функция преобразования сетевых адресов (NAT) применяется при подключении ко внешним сетям, в частности, Internet, для защиты внутренней сети. Она позволяет скрыть IP-адреса локальных компьютеров, расположенных за брандмауэром. В целях маршрутизации на сервере iSeries(TM) могут применяться следующие типы NAT:

- “Маскирующий NAT”
  Маскирующий NAT позволяет скрыть внутреннюю сеть, представив ее во внешней сети в виде одной системы, которой присвоен IP-адрес, связанный с внешним интерфейсом сервера.
- “Динамический NAT” на стр. 17
  Динамический NAT применяется при подключении локального компьютера к внешней сети. Основное отличие состоит в том, что для обслуживания таких соединений применяется пул внешних IP-адресов.
- “Статический NAT” на стр. 18
  Статический NAT применяется при подключении внешних хостов к внутренней сети.

Маскирующий NAT

Маскирующий NAT позволяет скрыть частную сеть, присвоив ей только один адрес внешней сети, который будет представлять всю частную сеть. Чаще всего этот адрес назначается провайдером Internet (ISP). Если для подключения к сети применяется двухточечный протокол (PPP), то этот адрес может быть динамическим. Такой способ преобразования адресов может применяться только при подключении компьютера частной сети к компьютеру общей сети. Все исходящие соединения устанавливаются с помощью разных номеров портов IP.

Маскирующий NAT позволяет рабочим станциям с внутренними IP-адресами подключаться к хостам в Internet с помощью сервера iSeries(TM). Провайдер Internet передает серверу iSeries IP-адрес шлюза в Internet. Термин локальный компьютер используется для обозначения всех компьютеров внутренней сети, независимо от способа их подключения (LAN или WAN) и удаленности расположения. Термин внешний компьютер используется для обозначения всех компьютеров, подключенных к Internet. На следующем рисунке показана схема преобразования адресов с помощью маскирующего NAT.



RZAJW507-0

С точки зрения хостов Internet все соединения, устанавливаемые локальными рабочими станциями, устанавливаются сервером iSeries. Это вызвано тем, что с сервером iSeries и рабочими станциями связан общий IP-адрес. Когда маршрутизатор получает пакет, предназначенный для локальной рабочей станции, он определяет внутренний адрес этой рабочей станции и отправляет пакет по этому адресу.

На всех рабочих станциях в качестве шлюза и целевой системы по умолчанию должен быть настроен сервер iSeries. В тот момент, когда рабочая станция отправляет серверу iSeries пакет данных для передачи в Internet, ей назначается номер порта связи. Функция маскирующего NAT сохраняет номер порта, и при получении ответа на пакет данных по этому соединению она отправляет ответ нужной рабочей станции.

Маскирующий NAT хранит список активных соединений, а также время передачи последнего пакета по этому соединению. Периодически из списка удаляются записи о соединениях, простаивающих в течение заданного интервала времени. Считается, что такие соединения больше не используются.

Все соединения с Internet должны устанавливаться локальными рабочими станциями. Это очень эффективный брандмауэр зашиты. Поскольку в Internet не передается никакая информация о наличии рабочих станций, их адреса остаются скрытыми от внешних хостов.

Основой для реализации маскирующего NAT является использование логических портов, создаваемых маскирующим NAT для того, чтобы различать различные потоки данных, передаваемых по соединению. При установлении соединения TCP указываются номера исходного и целевого портов. К этим значениям NAT добавляет номер логического порта.

Обработка исходящих сообщений маскирующим NAT:

Исходящим сообщением на предыдущей иллюстрации называется пакет, который отправляется из частной частной локальной сети в Internet. Исходящее сообщение содержит номер исходного порта рабочей станции. NAT сохраняет этот номер и заменяет его в заголовке протокола передачи данных на уникальный номер логического порта. Для исходящих дейтаграмм номером исходного порта является номер локального порта.

1. При обработке исходящих сообщений маскирующий NAT предполагает, что все получаемые им пакеты IP адресованы внешним хостам. Он не проверят, что пакет действительно должен быть отправлен во внешнюю сеть, а не локальной рабочей станции.

2. В наборе номеров логических портов выполняется поиск записи с указанным в сообщении протоколом передачи данных, IP-адресом отправителя и номером исходного порта. Если такая запись найдена, то вместо номера исходного порта подставляется соответствующий номер логического порта. В противном случае создается новый порт, и вместо номера исходного порта подставляется номер нового логического порта.

3. Преобразуется IP-адрес отправителя.

4. Пакет обычным образом обрабатывается протоколом IP и передается указанному внешнему хосту.

Обработка входящих сообщений маскирующим NAT (ответов и прочих сообщений):

Входящим сообщением на предыдущей иллюстрации называется пакет, отправленный из Internet в частную локальную сеть. Для входящих дейтаграмм номером целевого порта является номер локального порта. (Для входящих сообщений номером исходного порта является номер внешнего порта. Для исходящих сообщений номером целевого порта является номер внешнего порта.)

В ответных сообщениях, которые отправляются хостами Internet локальным компьютерам, в заголовке уровня передачи данных в качестве номера целевого порта указан номер логического порта, присвоенный маскирующим NAT. Ниже описана процедура обработки входящих сообщений маскирующим NAT:

1. Маскирующий NAT выполняет поиск номера логического порта (исходного порта) в базе данных. Если такой номер не найден, то считается, что запрос на получение такого пакета не поступал, и пакет возвращается отправителю без изменений. После этого выполняется обычная процедура обработки пакета, получатель которого неизвестен.

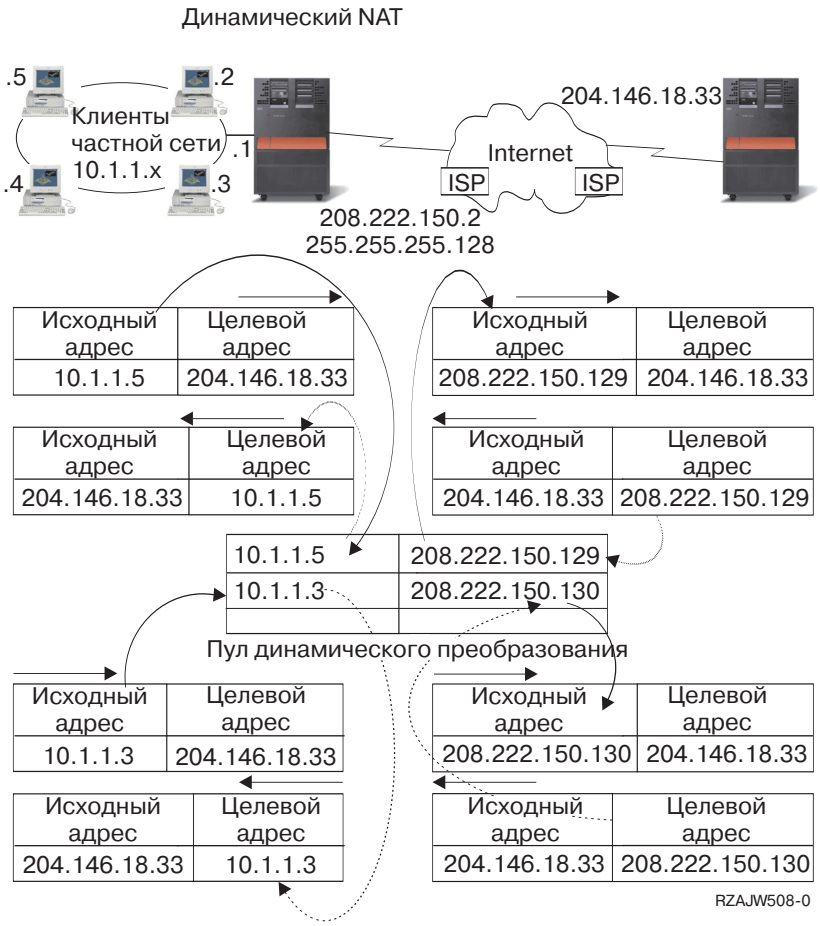
2. Если номер логического порта найден в базе данных, проверяется, совпадает ли IP-адрес отправителя пакета с IP-адресом получателя, указанным в соответствующей записи таблицы номеров логических портов. При совпадении номер исходного порта в заголовке IP заменяется на номер порта локальной рабочей станции. В противном случае пакет возвращается без изменений.

3. Вместо IP-адреса получателя в заголовке пакета указывается соответствующий адрес локальной рабочей станции.

4. После этого пакет обычным образом обрабатывается протоколом IP или TCP и передается локальной рабочей станции. Поскольку для определения порта и адреса локальной рабочей станции маскирующему NAT требуется номер логического порта, он поддерживает обработку только тех дейтаграмм, которые поступают от внешних хостов в ответ на какое-то сообщение.

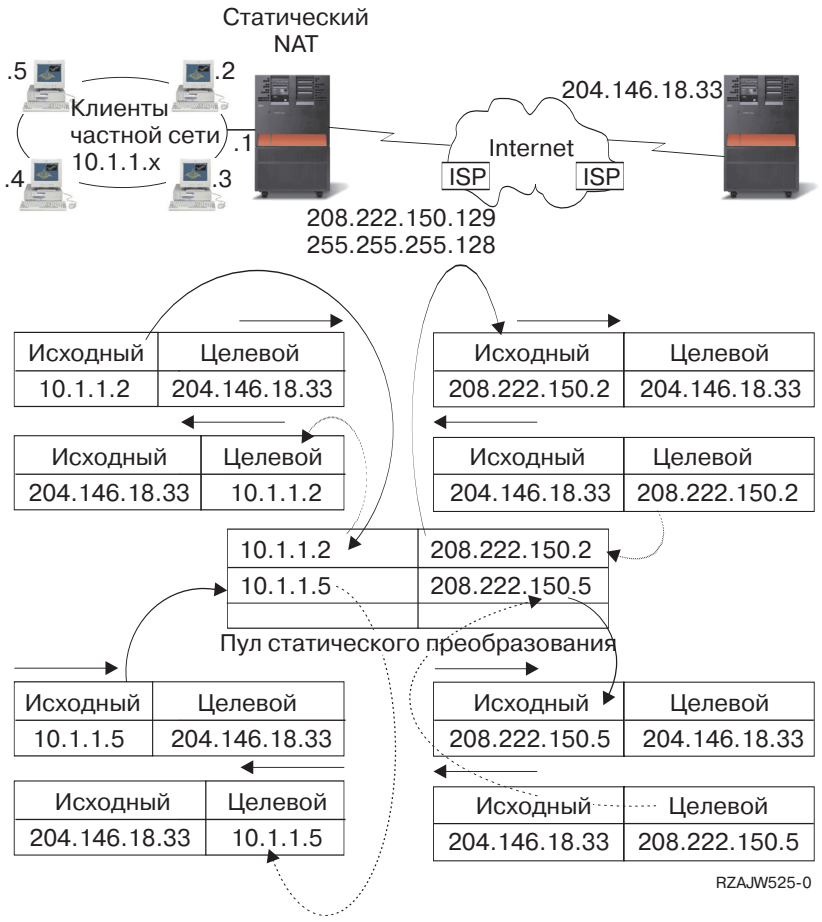
Динамический NAT

Динамический NAT применяется при подключении компьютеров внутренней сети к хостам внешней сети. При таком способе преобразования адресов создается пул сетевых адресов, применяемый для установления соединений с внешней сетью. Каждому соединению присваивается уникальный внешний адрес. Максимальное число активных соединений ограничено числом внешних адресов в пуле. Другими словами, между соединениями и адресами устанавливается взаимно-однозначное соответствие. Динамический NAT позволяет подключаться к Internet с помощью IP-адреса, выделенного из пула. На приведенном ниже рисунке проиллюстрировано динамическое преобразование адресов.



Статический NAT

Статический NAT обеспечивает однозначное преобразование внутренних адресов во внешние. Он применяется для обслуживания соединений, которые устанавливаются хостами внешней сети с внутренней сетью. Для каждого локального адреса должен быть задан уникальный глобальный адрес.



Маршрутизация в системе несколькими разделами с помощью OptiConnect

В системе с несколькими разделами и шиной OptiConnect также могут применяться основные функции маршрутизации - протокол ARP Proxy, двухточечный протокол и виртуальные интерфейсы IP. Ниже перечислено несколько способов применения этих функций.

- “TCP/IP и OptiConnect”
  Функция OptiConnect предоставляет возможность определять соединения TCP/IP, устанавливаемые через шину OptiConnect. В этом разделе приведено подробное описание этой функции.
- “Маршрутизация виртуальных соединений OptiConnect в системе с несколькими логическими разделами” на стр. 20
  Виртуальные интерфейсы TCP/IP, создаваемые с помощью OptiConnect, применяются для установления соединений между логическими разделами. Сервер iSeries(TM) логически разделен на несколько виртуальных систем. У каждой виртуальной системы, которая называется разделом, есть свое адресное пространство. С точки зрения протокола TCP/IP каждый раздел является отдельным сервером. В данном разделе приведена подробная информация о работе с этой функцией.

TCP/IP и OptiConnect

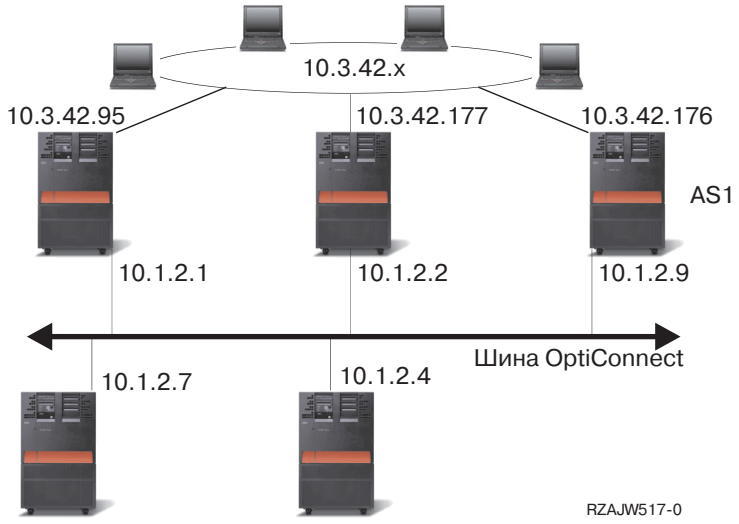
Функция OptiConnect предоставляет возможность определять соединения TCP/IP, устанавливаемые через шину OptiConnect. Для маршрутизации таких соединений TCP/IP могут применяться другие способы маршрутизации, основанные на ARP Proxy, ненумерованных двухточечных соединениях и виртуальных интерфейсах IP. Для настройки этих способов маршрутизации необходимо настроить локальную сеть, эмулированную с помощью OptiConnect, либо двухточечное соединение OptiConnect.

В **локальной сети, эмулированной с помощью OptiConnect**, шина OptiConnect представляется протоколу TCP/IP в виде локальной сети.Локальную сеть OptiConnect достаточно легко настроить, однако соединения в такой сети не устанавливаются автоматически, так как для этого необходим Протокол информации о маршрутизации (RIP) или статические маршруты.

При **настройка двухточечного соединений OptiConnect** для каждой пары хостов OptiConnect настраивается ненумерованный двухточечный интерфейс.При этом новая сеть не создается, поэтому все соединения в локальной сети OptiConnect устанавливаются автоматически. Главным преимуществом этого способа является то, что не требуется создавать описания маршрутов. Соединение между хостами из разных сетей устанавливается автоматически. Другим преимуществом является то, что если обе сети активны, то данные, которыми обмениваются серверы iSeries(TM), передаются через шину OptiConnect, так как маска подсети такого маршрута задана наиболее точно. При сбое шины OptiConnect поток данных автоматически перенаправляется для передачи через локальную сеть Token-Ring.

Настройка двухточечных соединений OptiConnect с помощью виртуальных IP-адресов - это один из вариантов настройки ненумерованных двухточечных соединений.Помните, что при настройке ненумерованного двухточечного интерфейса для него должен быть определен соответствующий локальный интерфейс. Этот интерфейс определяет IP-адрес, с помощью которого удаленная конечная система будет подключаться к локальному серверу iSeries. Как показано ниже, с ненумерованным двухточечным интерфейсом может быть связан основной интерфейс локальной сети сервера iSeries. Роль такого интерфейса может играть и виртуальный интерфейс IP. В этом случае шина OptiConnect рассматривается как набор двухточечных соединений. Для каждой пары хостов настраивается ненумерованное соединение. При этом, как и в предыдущем случае, дополнительные маршруты создавать не требуется, и соединения между хостами из разных сетей устанавливаются автоматически. Преимуществом этого способа является то, что к любому серверу iSeries можно подключиться при наличии хотя бы одной активной сети.

Конфигурация локальной сети, эмулируемая OptiConnect

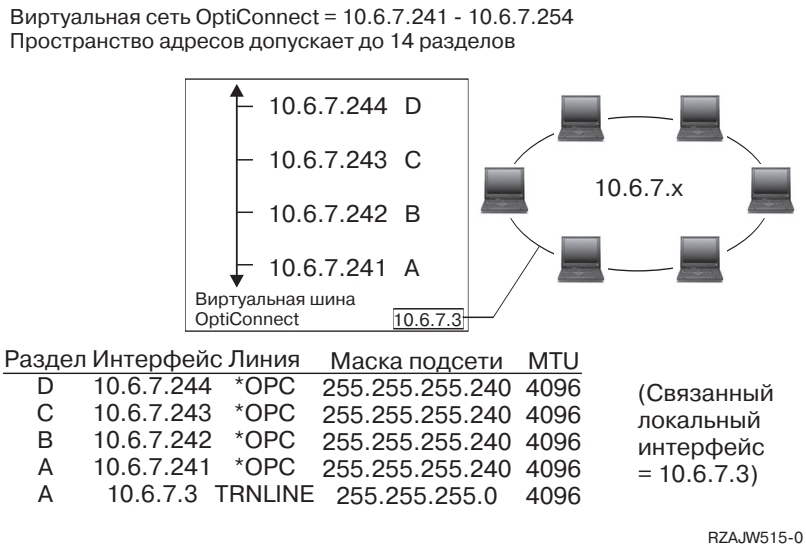


Маршрутизация виртуальных соединений OptiConnect в системе с несколькими логическими разделами

Сервер iSeries(TM) может представлять собой несколько виртуальных систем, называемых логическими разделами. Виртуальные интерфейсы TCP/IP, создаваемые с помощью OptiConnect, применяются для установления соединений между логическими разделами. У каждого раздела есть свое адресное пространство, свой экземпляр протокола TCP/IP, и, возможно, отдельные адаптеры ввода/вывода. С точки зрения протокола TCP/IP каждый раздел является отдельным сервером. Соединения TCP/IP между логическими разделами устанавливаются через шину OptiConnect. С точки

зрения функции маршрутизации TCP/IP маршрут к другому разделу ничем не отличается от маршрута к обычной системе, подключенной к физической шине OptiConnect.

Логические разделы: Виртуальные интерфейсы OptiConnect обеспечивают взаимодействие между разделами.



Раздел	Интерфейс	Линия	Маска подсети	MTU
D	10.6.7.244	*OPC	255.255.255.240	4096
C	10.6.7.243	*OPC	255.255.255.240	4096
B	10.6.7.242	*OPC	255.255.255.240	4096
A	10.6.7.241	*OPC	255.255.255.240	4096
A	10.6.7.3	TRNLINE	255.255.255.0	4096

(Связанный локальный интерфейс = 10.6.7.3)

RZAJW515-0

В приведенных примерах рассматривается система с одним сетевым адаптером. Адаптер размещен в разделе A, однако клиентам локальной сети требуется подключаться и к другим разделам системы. Для решения этой задачи необходимо определить подсеть с прозрачным доступом, связанную с виртуальной шиной OptiConnect. Адрес локальной сети равен 10.6.7.x. Для подключения к другим разделам необходимо определить IP-адреса. Для получения 12 адресов нужно задать маску подсети 255.255.255.240. Такая маска создает подсеть с диапазоном адресов с 10.6.7.241 по 10.6.7.254 (14 адресов). Предварительно необходимо проверить, что эти адреса еще не назначены никаким системам в локальной сети. После этого присвойте каждому разделу один из адресов подсети. Для этого нужно определить интерфейс и задать адрес раздела на виртуальной шине OptiConnect.

OPC	Раздел	Виртуальный адрес	Раздел	Интерфейс	Линия	Маска подсети	MTU	Локальный интерфейс
10.6.7.3	D	10.6.7.4	D	10.6.7.4	VIRTUALIP	255.255.255.255	4096	NONE
10.6.7.2			D	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.4
10.6.7.1			D	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.4
			D	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.4
10.6.7.4	C	10.6.7.3	C	10.6.7.3	VIRTUALIP	255.255.255.255	4096	NONE
10.6.7.2			C	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.3
10.6.7.1			C	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.3
			C	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.3
10.6.7.4	B	10.6.7.2	B	10.6.7.2	VIRTUALIP	255.255.255.255	4096	NONE
10.6.7.3			B	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.2
10.6.7.1			B	10.6.7.3	OPC	255.255.255.255	4096	10.6.7.2
			B	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.2
10.6.7.3	A	10.6.7.1	A	10.6.7.1	TRNLINE	255.255.255.0	4096	NONE
10.6.7.3			A	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.1
10.6.7.2			A	10.6.7.3	OPC	255.255.255.255	4096	10.6.7.1
Виртуальная шина OC			A	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.1

В интерфейс 10.6.7.x внешней локальной сети

rzajw516-0

Для того чтобы автоматически включился прозрачный доступ к подсети, должны быть выполнены следующие условия. Во-первых, размер виртуальной шины OptiConnect должен быть не больше

размера максимального блока передачи интерфейса физической локальной сети. Во-вторых, адреса подсети шины OptiConnect должны входить в диапазон адресов локальной сети. Если оба условия соблюдены, то автоматически включается прозрачный доступ к подсетям. Интерфейс 10.6.7.3 выполняет функции Proxy для всех интерфейсов, определенных в разделах. За счет этого локальные клиенты могут подключаться к различным разделам.

Способы распределения нагрузки TCP/IP

Распределение нагрузки заключается в перераспределении потока данных, передаваемых по сетевым соединениям, и работы, выполняемой сильно загруженными компьютерами, по нескольким процессорам, сетевым адаптерам или серверам хоста. Для того чтобы добиться максимальной производительности сервера iSeries(TM), необходимо распределить нагрузку, связанную с передачей данных по сети, по нескольким компонентам сервера.

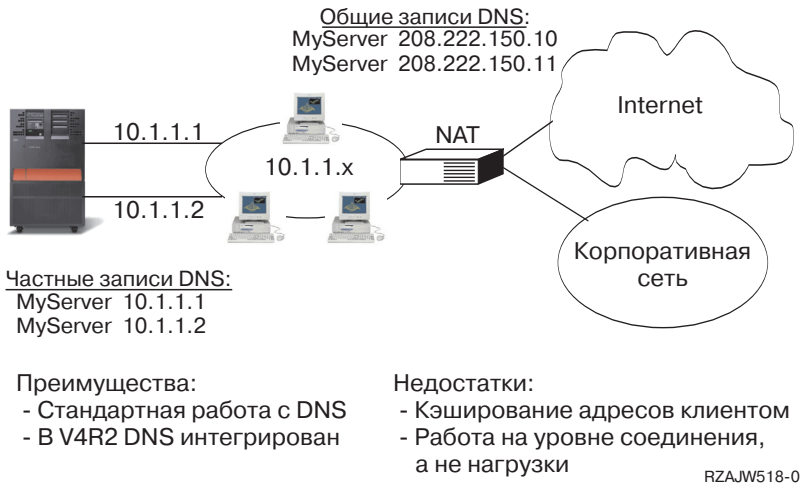
Для оптимизации нагрузки на сервер iSeries можно выбрать один из следующих способов маршрутизации TCP/IP:

- “Распределение нагрузки с помощью DNS”
  Этот способ применяется для распределения нагрузки, связанной с обслуживанием входящих соединений. В основном он используется для распределения нагрузки, связанной с обслуживанием локальных клиентов.
- “Распределение нагрузки по нескольким маршрутам” на стр. 23
  Этот способ позволяет распределить нагрузку, связанную с обслуживанием исходящих соединений, по нескольким интерфейсам. Это более гибкий способ распределения нагрузки по сравнению со способом, основанным на DNS, однако он неприменим для локальных клиентов.
- “Аварийное переключение адаптера с помощью виртуальных IP-адресов и ARP Proxy” на стр. 24
  Для реализации этого способа вам потребуется внешний компьютер для распределения нагрузки, например, IBM(R) eNetwork Dispatcher. Виртуальный IP-адрес в отличие от фактического присваивается системе, а не сетевому интерфейсу. Один адрес можно назначить нескольким серверам, что позволяет выбрать один из нескольких вариантов распределения нагрузки.

Распределение нагрузки с помощью DNS

DNS применяется для распределения нагрузки, связанной с обслуживанием входящих соединений. Для этого в таблице DNS нескольким IP-адресам хоста сопоставляется одно и то же имя хоста. В результате при обработке запросов клиентов на преобразование имени хоста сервер DNS может выбрать один из указанных IP-адресов. Преимуществом такого способа распределения нагрузки является использование стандартной функции DNS. К недостаткам можно отнести то, что IP-адреса часто кэшируются клиентами. Кроме того, такой способ основан на соединениях, а не на объеме нагрузки на сервер.

Первый способ распределения нагрузки заключается в использовании стандартной функции DNS, которая в ответ на запросы клиентов о преобразовании имени хоста отправляет разные адреса хоста. Другими словами, сервер DNS будет преобразовывать имя системы в разные IP-адреса. В приведенном ниже примере каждый адрес соответствует отдельной системе. Это позволяет распределить нагрузку по двум системам. При обработке запросов клиентов внутренней сети сервер DNS чередует адреса систем, возвращая их по-очереди. Это стандартная функция DNS. Заметьте, что на внешнем сервере DNS также задано две записи адреса. Эти адреса преобразуются функцией “Статический NAT” на стр. 18 таким образом, что хосты Internet могут подключаться к любой из двух систем.

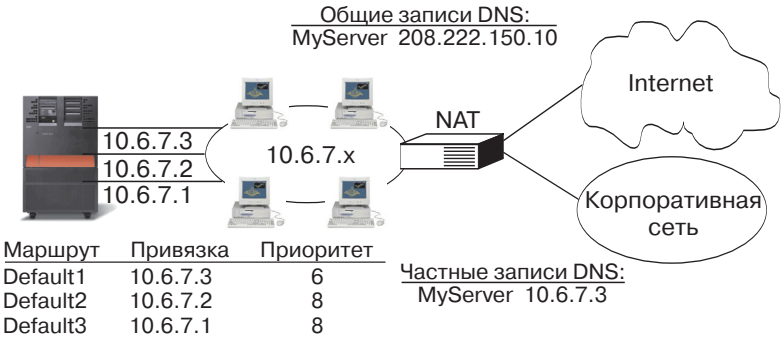


Если для работы программы необходимо, чтобы соединение было установлено с какой-то определенной системой, либо чтобы система не менялась при повторном подключении, то при каждом обращении к Web-странице или Web-серверу должно меняться имя системы, сообщаемое клиенту. Например, вы можете добавить записи DNS MyServer1 208.222.150.10 и MyServer2 208.222.150.11. В этом случае при первом обращении к Web-сайту может быть установлено соединение с системой MyServer1, а при следующем - соединение с системой MyServer2. Такой способ распределения нагрузки основан на равномерном распределении запросов на подключение. В большинстве случаев клиент отправляет запрос на преобразование имени хоста только один раз, после чего он заносит полученный адрес хоста в кэш. Такой способ распределения нагрузки не учитывает объем данных, обрабатываемых каждой системой. Обратите внимание, что описанный способ учитывает только нагрузку, связанную с обслуживанием входящих соединений, и может применяться в случае, когда в одной системе установлено два адаптера (а не один адаптер в двух системах).

Распределение нагрузки по нескольким маршрутам

Для распределения нагрузки, связанной с отправкой пакетов, по нескольким интерфейсам, можно создать дополнительный маршрут. Это более гибкий способ распределения нагрузки по сравнению со способом, основанным на DNS, однако он не применим для локальных клиентов. Преимущества такого способа заключаются в том, что он подходит для всех серверов iSeries(TM), является более гибким по сравнению с DNS и особенно эффективен для приложений, в которых основная часть потоков данных - исходящие, таких как HTTP и Telnet. К недостаткам можно отнести то, что этот способ основан на соединениях (а не на объеме нагрузки), и то, что он не применим для локальных клиентов. Кроме того, этот способ не предназначен для входящих потоков данных.

В приведенном ниже примере три адаптера системы подключены к одному сегменту локальной сети. Один из адаптеров обрабатывает только входящие пакеты, а остальные два - только исходящие. Локальные клиенты работают так же, как и раньше. Другими словами, с точки зрения клиентов интерфейс для отправки данных совпадает с интерфейсом для приема данных. Помните, что локальным клиентом является любая система, которой можно передать данные, минуя маршрутизатор. Таким образом, внутренняя сеть может быть довольно большого размера, если вместо маршрутизаторов в ней установлены коммутаторы.



Повторяющиеся непрямые маршруты с приоритетом >5 будут выбираться в соответствии с приоритетом.

Преимущества:
- Применяется только AS/400
- Большая гибкость, чем в DNS
- Удобно для HTTP, Telnet

Недостатки:
- Работа на уровне соединения, а не нагрузки
- Не действует на локальные клиенты и входящие запросы

RZAJW511-0

Процедура настройки

Для настройки такого способа распределения нагрузки вызовите команду Добавить маршрут TCP/IP, либо воспользуйтесь программой Навигатор iSeries. В первом случае нужно настроить приоритет дополнительного маршрута, а во втором - предпочитаемый интерфейс для связывания. Если приоритет дополнительного маршрута равен 5 (значение по умолчанию), то никакие действия не выполняются. Если приоритет больше 5, то соединения распределяются между маршрутами с одинаковым приоритетом. Предпочитаемый интерфейс для связывания позволяет задать IP-адрес интерфейса, с которым будет связан маршрут. Если это значение не задано, то маршрут связывается с первым интерфейсом, найденным системой.

В приведенном выше примере приоритет дополнительного маршрута, связанный с адаптером входящих соединений (10.6.7.3), равен 6. У остальных двух адаптеров приоритет дополнительного маршрута равен 8. Так как приоритет дополнительного маршрута одного из адаптеров равен 6, этот адаптер не будет выбран для обслуживания исходящих соединений до тех пор, пока есть хотя бы один интерфейс, у которого приоритет маршрута равен 8.

У всех исходящих интерфейсов должен быть одинаковый приоритет. В противном случае будет использоваться только интерфейс с максимальным приоритетом.

Заметьте, что в DNS указан интерфейс 10.6.7.3. Следовательно, этот интерфейс будет являться входящим. Даже если вы не будете задавать приоритет дополнительного маршрута, для каждого интерфейса нужно определить маршрут к внешней сети по умолчанию, задав предпочитаемый интерфейс для связывания.

Аварийное переключение адаптера с помощью виртуальных IP-адресов и ARP Proxy

Ситуация

Рабочая система iSeries(TM) получает данные от удаленных и локальных клиентов. Хранящаяся в системе информация необходима для работы компании. Вместе с ростом компании увеличивается зависимость от работы системы iSeries и пропускной способности сети. В результате становится необходимым постоянный доступ к системе iSeries. При выходе из строя одного из адаптеров его место должен занимать другой без каких-либо действий со стороны клиентов.

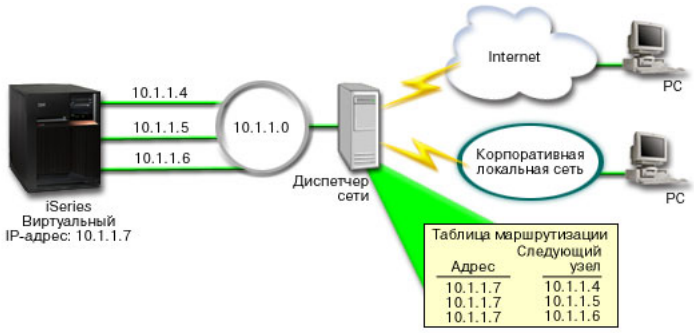
Цели

Обеспечение постоянной готовности тесно связано с избыточностью и заменой вышедших из строя компонентов. Цель данного сценария - обеспечить готовность связи клиенты-сервер в случае сбоя одного из адаптеров.

Подробности

Один из способов реализации описанного выше сценария - создать несколько физических соединений системы iSeries с локальной сетью. Обратите внимание на следующий рисунок.

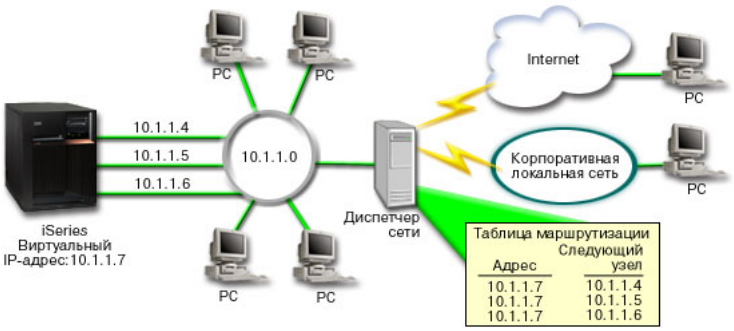
Рисунок 1. Аварийное переключение адаптера без локальных клиентов



Каждому из физических соединений будет присвоен свой IP-адрес. Затем системе можно присвоить виртуальный IP-адрес. Клиентам система будет известна по виртуальному IP-адресу. Все удаленные клиенты (клиенты, не подключенные физически к той же локальной сети, что и сервер iSeries) будут обращаться к системе iSeries через внешний сервер распределения нагрузки или диспетчер сети. Диспетчер сети передает запросы от удаленных клиентов, полученные по виртуальному IP-адресу, одному из сетевых адаптеров системы iSeries.

Если часть клиентов системы iSeries находится в ее локальной сети, работа этих клиентов через диспетчер ограничит пропускную способность, поскольку создаст излишнюю нагрузку на диспетчер. Можно создать в системе каждого клиента записи маршрутизации, аналогичные записям диспетчера, но этот подход может быть неудобным при большом числе клиентов. Система с локальными клиентами показана на следующем рисунке.

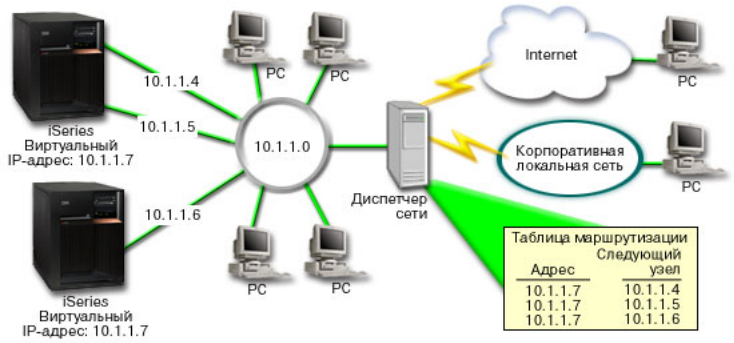
Рисунок 2. Аварийное переключение адаптера с локальными клиентами



В OS/400(R) версии V5R2 локальные клиенты (подключенные к той же локальной сети, что и iSeries) могут устанавливать соединение с виртуальным адресом системы iSeries через ARP. Это позволяет локальным клиентам также использовать аварийное переключение адаптера.

Данное решение поддерживает применение нескольких систем iSeries, дублирующих друг друга. Если одна из систем становится недоступной, ее заменяет другая. Схема применения двух серверов iSeries показана на следующем рисунке:

Рисунок 3. Аварийное переключение адаптера с несколькими системами iSeries и локальными клиентами



Маршрутизация пакетов для удаленных клиентов совпадает; для локальных клиентов есть отличия. Если с несколькими системами iSeries связан один и тот же IP-адрес, доступ к одной из них возможен только через Proxy. В этом случае одна из систем с двумя интерфейсами может играть роль Proxy.

Инструкции по настройке

Конфигурация с распределением нагрузки, применяющая виртуальный IP-адрес и ARP Proxy очень похожа на обычную конфигурацию TCP/IP, к которой добавлен виртуальный интерфейс TCP/IP. При аварийном переключении адаптера с локальными клиентами необходимо выполнить следующие действия:

1. **Настройте виртуальный интерфейс TCP/IP.**

   Создайте виртуальный интерфейс TCP/IP с помощью Навигатора iSeries. Запустите Мастер создания виртуального интерфейса, выбрав следующие опции:
   Сеть -> **Конфигурация TCP/IP** -> **IPv4** -> **Интерфейсы**. Щелкните правой кнопкой мыши на пункте **Интерфейсы** и выберите **Создать интерфейс** -> **Виртуальный IP**.

   В описываемом примере следует указать IP-адрес 10.1.1.7 с маской подсети 255.255.255.255. После создания виртуального интерфейса щелкните на нем правой кнопкой и выберите **Свойства**. Перейдите на страницу **Дополнительные** и выберите опцию **Включить ARP Proxy**.

2. **Создайте интерфейсы TCP/IP для всех физических подключений к локальной сети.**

   С помощью мастера Создать интерфейс TCP/IP создайте нужные интерфейсы TCP/IP. Для запуска мастера в Навигаторе iSeries выберите:
   Сеть -> **Конфигурация TCP/IP** -> **IPv4** -> **Интерфейсы**. Щелкните правой кнопкой мыши на пункте **Интерфейсы** и выберите **Создать интерфейс** -> **Локальная сеть**. Следуйте инструкциям мастера; повторите операцию для каждого подключения к локальной сети.

   В описываемом примере следует запустить мастер три раза для адресов 10.1.1.4, 10.1.1.5 и 10.1.1.6 с маской подсети 255.255.255.0. После создания каждого интерфейса щелкните на нем правой кнопкой и выберите **Свойства**. На странице **Дополнительные** свяжите каждый интерфейс с виртуальным интерфейсом, созданным на шаге 1. Для этого выберите виртуальный интерфейс в списке **Связанный локальный интерфейс**.

Дополнительная информация об оптимизации маршрутизации TCP/IP и распределении нагрузки

DNS - это эффективная система управления именами хостов TCP/IP, связанными с IP-адресами.В данном разделе описаны основные принципы работы DNS, а также некоторые процедуры настройки и управления DNS.

Раздел Логические разделы содержит дополнительную информацию об основных принципах работы системы.

Раздел Настройка фильтров NAT и IP содержит информацию о работе с правилами фильтрации.В частности, вы сможете узнать, каким образом можно изменить и просмотреть правила фильтрации, а также добавить к ним комментарий.

OptiConnect  содержит информацию о маршрутизации в OptiConnect. Полное название этого электронного руководства по серверу iSeries(TM) - *OptiConnect for OS/400(R)*.

Двухточечный протокол обычно применяется для подключения компьютера к Internet.PPP относится к числу стандартных протоколов Internet. Этот протокол поддерживается практически всеми провайдерами Internet (ISP).

Приложение. Примечания

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Товарные знаки

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

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

Условия загрузки и печати публикаций

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

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

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

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

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

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

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

Отказ от гарантий на предоставляемый код

В данной документации содержатся примеры программных кодов.

IBM предоставляет вам полную лицензию на использование этих кодов. Вы можете создавать на их основе похожие функции, приспособленные для ваших конкретных целей.

Все коды примеров предоставляются IBM исключительно для наглядности. Эти примеры не подвергались всестороннему тестированию в различных условиях. IBM не несет ответственности за надежность, удобство и работоспособность этих программ.

Все включенные в данную документацию программы предоставляются на условиях ″как есть″ без предоставления каких-либо гарантий. Мы также отказываемся от подразумеваемых гарантий о соблюдении авторских прав, коммерческой ценности или применения для каких-либо конкретных целей.

Напечатано в Дании