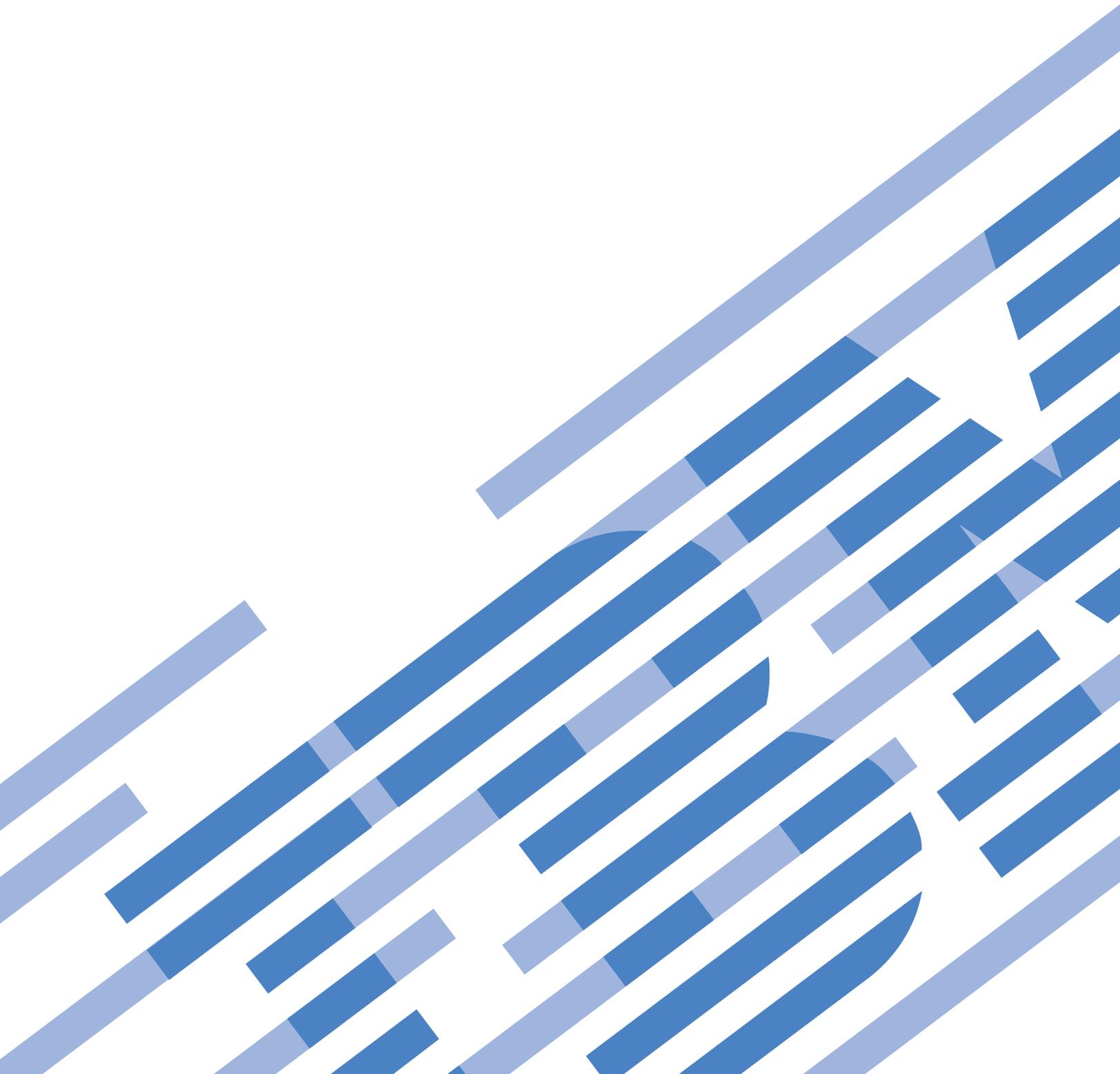




Система і

Сетевая маршрутизация
TCP/IP и распределение нагрузки

Версия 6 выпуск 1





Система і

Сетевая маршрутизация
TCP/IP и распределение нагрузки

Версия 6 выпуск 1

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 35.

Это издание относится к версии 6, выпуску 1, модификации 0 продукта IBM i5/OS (код продукта 5761-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).

© Copyright International Business Machines Corporation 1998, 2008. Все права защищены.

Содержание

Оптимизация маршрутизации TCP/IP и распределение нагрузки 1

Новое в V6R1	1
Файл PDF для маршрутизации TCP/IP и распределения нагрузки	2
Функции маршрутизации TCP/IP в различных выпусках.	2
Обработка пакетов	3
Общие правила маршрутизации	4
Способы маршрутизации соединений	4
Маршрутизация двухточечных соединений	4
Маршрутизация с помощью Протокола преобразования адресов Proxu.	8
Прозрачный доступ к подсетям	9
Динамическая маршрутизация	10
Протокол информации о маршрутизации	10
Протокол кратчайшего пути	11
Связывание маршрутов	15
Бесклассовая междоменная маршрутизация	16
Маршрутизация с помощью виртуальных IP-адресов	17
Устойчивость к сбоям	18
Маршрутизация с преобразованием сетевых адресов	19
Маскирующий NAT.	19
Обработка входящих сообщений маскирующим NAT (ответов и прочих сообщений):	20

Обработка исходящих сообщений маскирующим NAT.	20
Динамический NAT	21
Статический NAT	21
Маршрутизация в системе несколькими разделами с помощью OptiConnect	22
TCP/IP и OptiConnect	22
Маршрутизация виртуальных соединений OptiConnect в системе с несколькими разделами	23
Способы распределения нагрузки TCP/IP	25
Распределение нагрузки с помощью DNS	25
Распределение нагрузки по нескольким маршрутам	26
Распределение нагрузки с помощью виртуальных IP-адресов и проху ARP.	27
Сценарий: Аварийное переключение адаптера с помощью виртуальных IP-адресов и ARP проху	29
Переключение с помощью автоматического выбора интерфейса	32
Переключение с помощью списка предпочтительных интерфейсов	33
Дополнительная информация об оптимизации маршрутизации TCP/IP и распределении нагрузки	33

Приложение. Примечания 35

Информация об интерфейсе программирования	37
Товарные знаки	37
Terms and conditions	37

Оптимизация маршрутизации TCP/IP и распределение нагрузки

С помощью встроенных возможностей маршрутизации можно настроить и распределить поток TCP/IP системы, чтобы исключить использование внешнего маршрутизатора.

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

В чем состоит необходимость использования этих методов

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.

Новое в V6R1

Коллекции тем в about new содержат сведения о маршрутизации TCP/IP и распределении нагрузки.

Новый поддерживаемый протокол маршрутизации

В операционную систему i5/OS добавлена поддержка протокола маршрутизации Протокол кратчайшего пути (OSPF). *Протокол кратчайшего пути (OSPF)* - это протокол маршрутизации с выявлением маршрутов по состоянию связи, в котором маршрутизаторы или серверы из одной области поддерживают одну и ту же базу данных выявленных маршрутов, описывающих топологию области.

Расширение виртуального IP-адреса

Расширение виртуального IP-адреса, влияющее на маршрутизацию TCP/IP и распределение рабочей нагрузки, состоит в следующем:

- Поддержка виртуальных IP-адресов включает адреса IPv6.
- Интерфейс PPP или протокола L2TP может использовать виртуальный IP-адрес в качестве локального IP-адреса с целью обеспечения отказоустойчивости удаленных программ подключения.
- Виртуальный IP-адрес Proху можно настроить во время работы интерфейса виртуального IP-адреса.

Расширения IPv6 приведены в разделах “Маршрутизация с помощью виртуальных IP-адресов” на стр. 17 и “Устойчивость к сбоям” на стр. 18.

Документация нового метода распределения

Метод, использующий виртуальный IP-адрес и ARP Proху для распределения нагрузки, использовался в V6R1 и раньше, но не был документирован. В документацию добавлен раздел “Распределение нагрузки с помощью виртуальных IP-адресов и проху ARP” на стр. 27, содержащий описание данного метода распределения нагрузки.

Условное обозначение новой и измененной информации

Для упрощения поиска изменений в information center используются:

- Значок  обозначает начало новой или измененной информации.
- Значок  обозначает окончание новой или измененной информации.

В файлах PDF содержатся значки исправления (I) с левой стороны раздела с новой или измененной информацией.

Дополнительная информация об изменениях, связанных с выпуском, приведена в документации
Информация для пользователей.

Файл PDF для маршрутизации TCP/IP и распределения нагрузки

Файл PDF с данной информацией можно просмотреть и напечатать.

Для просмотра или загрузки этого документа в формате PDF выберите Маршрутизация TCP/IP и распределение нагрузки (около 1,40 Мб).

Сохранение файлов PDF

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

1. Щелкните правой кнопкой мыши на приведенной ссылке на документ PDF.
2. Щелкните на опции локального сохранения PDF.
3. Выберите каталог, в котором следует сохранить файл PDF.
4. Нажмите **Сохранить**.

Загрузка программы Adobe Reader

Для просмотра и печати файлов PDF необходимо установить программу Adobe Reader. Бесплатную копию этой программы можно загрузить с Web-сайта Adobe (www.adobe.com/products/acrobat/readstep.html) .

Ссылки, связанные с данной

“Дополнительная информация об оптимизации маршрутизации TCP/IP и распределении нагрузки” на стр. 33

Другие коллекции тем в information center содержат информацию о маршрутизации TCP/IP и распределении нагрузки.

Функции маршрутизации TCP/IP в различных выпусках

Перед окончательным определением функции маршрутизации, которая будет использоваться в вашей системе, убедитесь, что эта функция поддерживается в текущем выпуске операционной системы.

V3R1: Пересылка пакетов, основанная на статических маршрутах

V3R7/V3R2: Протокол SLIP, маршрутизация с помощью Протокола преобразования адресов Proxu (ARP), а также поддержка нумерованных 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

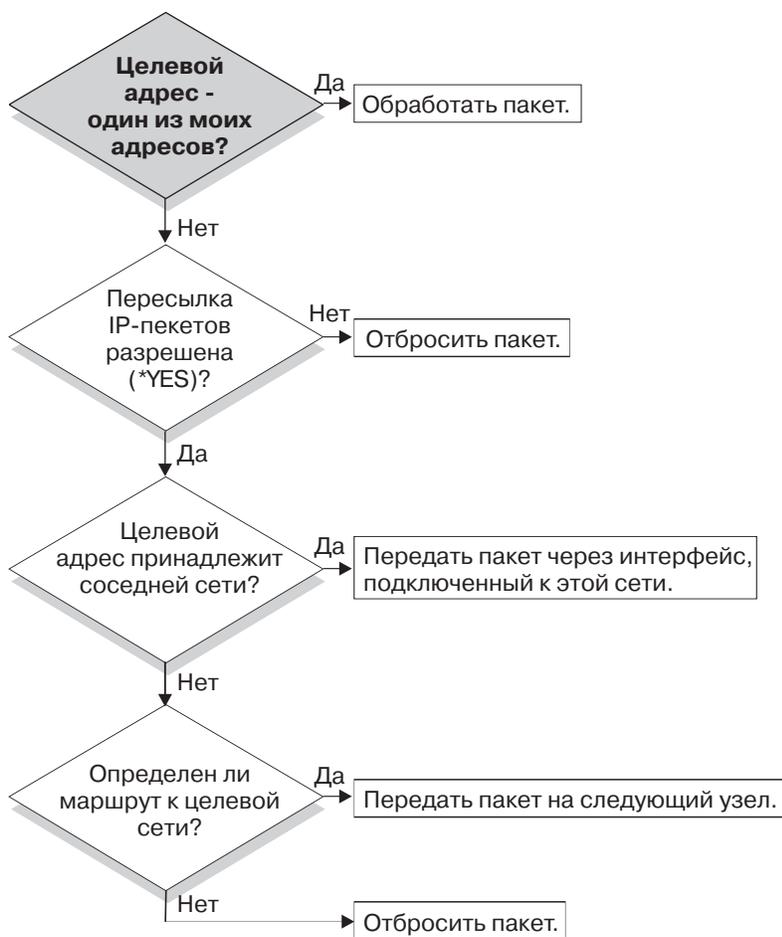
V5R4: Список предпочтительных интерфейсов

- | **V6R1:** Открыть протокол маршрутизации Протокол кратчайшего пути (OSPF) и поддержку виртуального IP-адреса для адресов IPv6

Обработка пакетов

Получив представление о том, каким образом сервер обрабатывает пакеты, вам будет проще настроить маршрутизацию в системе.

Ниже приведена упрощенная схема потоков, которая отображает логические процессы в операционной системе i5/OS во время получения пакета IP (дейтаграмма). 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 i5/OS 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

Эти правила применимы к TCP/IP в общем и к TCP/IP в операционной системе i5/OS.

Эти правила нужно учитывать при работе с функциями маршрутизации системы. Они помогут определить, что происходит с пакетами в вашей системе и там, куда они направляются. Как и из большинства правил, из них существуют исключения.

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

Примечание: Виртуальные IP-адреса (без установки соединения), присвоенные системе.

- 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 нумерованным интерфейсом, или же если активны IP NAT или фильтрация; в этом случае пакет может быть переслан или аннулирован.

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

Маршрут определяет путь, по которому может быть установлено соединение для передачи данных от отправителя получателю, а также способ создания этого соединения.

Маршрутизация двухточечных соединений

Двухточечное соединение устанавливается между локальной и удаленной системой для обмена данными.

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, некоммутируемым 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:

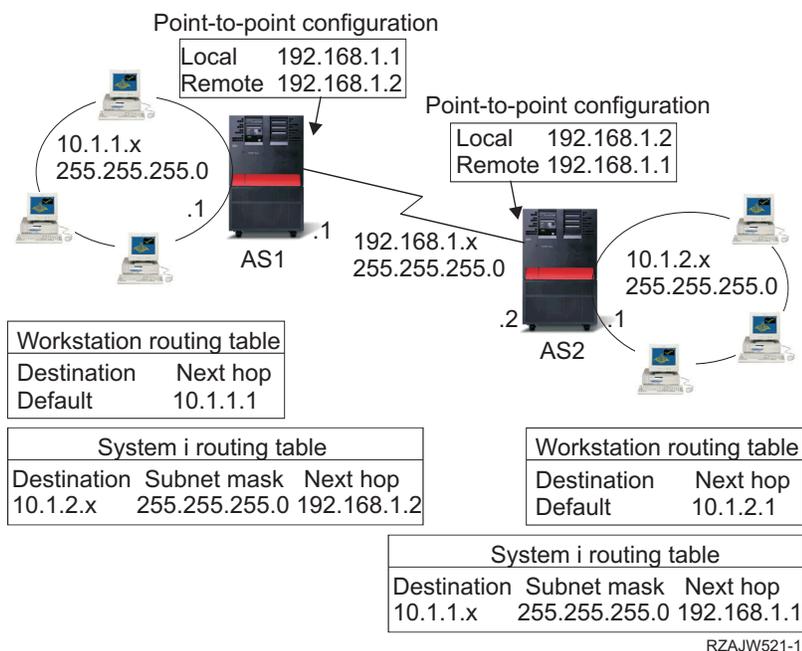
На первый взгляд, самый простой способ настройки двухточечного соединения - это создание нумерованного соединения. В определении нумерованного соединения для каждого конечного узла определен уникальный IP-адрес.

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 в системе будет определено двухточечное соединение, 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 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 платформами System i. Если необходимо просто установить соединение между 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.



Ненумерованные сетевые соединения:

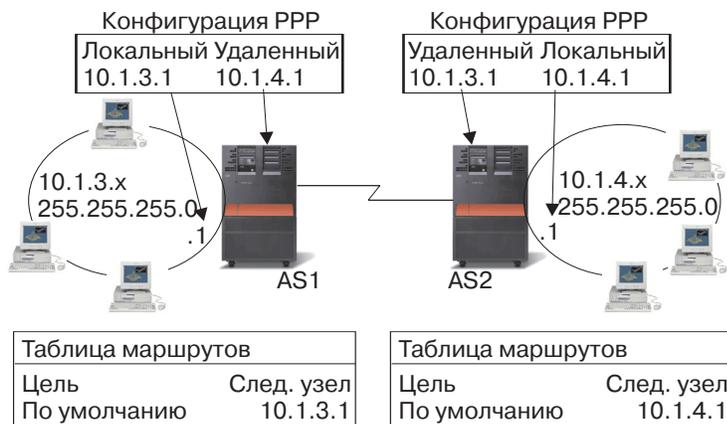
Для настройки ненумерованного соединения требуется выполнить более сложную процедуру, чем в случае с нумерованным соединением. Однако в дальнейшем вы сэкономите время на обслуживании такого соединения.

Процес выбора маршрута в i5/OS зависит от того, присвоены ли интерфейсам уникальные IP-адреса. При настройке ненумерованного соединения двухточечному интерфейсу не присваивается уникальный адрес. Фактически интерфейсу системы, через которую 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.



RZAJW502-0

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 системы. 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 нумерованного двухточечного соединения (PPP) (и не создавая запись маршрутизации в системе). В этом случае для определения маршрута будет применяться IP-адрес удаленной системы.

Передача данных по нумерованному и нумерованному соединению:

На следующем рисунке показаны адреса, применяемые при работе с нумерованным и нумерованным 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 нумерованного 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.



Исходный IP-адрес	Целевой IP-адрес	
192.168.1.1	192.168.1.2	Данные...
10.1.1.1	10.1.2.1	

Исходный IP-адрес	Целевой IP-адрес	
192.168.1.2	192.168.1.1	Данные...
10.1.2.1	10.1.1.1	



Исходный IP-адрес	Целевой IP-адрес	
10.1.3.1	10.1.4.1	Данные...

Исходный IP-адрес	Целевой IP-адрес	
10.1.4.1	10.1.3.1	Данные...

RZAJW503-0

Понятия, связанные с данным

Соединения PPP

Маршрутизация с помощью Протокола преобразования адресов Proxu

Протокол преобразования адресов (ARP) Proxu 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 Proxu.

Маршрутизация с помощью ARP позволяет представить несколько физических сетей в виде одной логической сети. Протокол ARP Proxu 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.

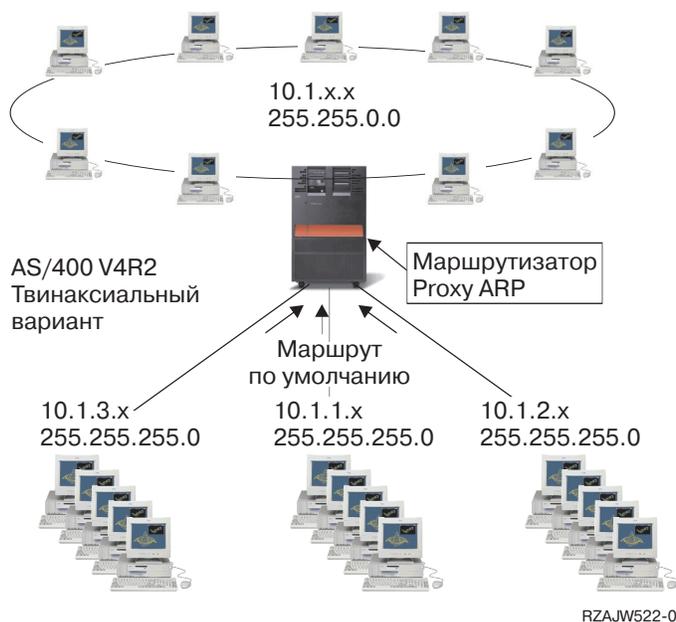


Когда локальной системе (10.1.1.x) потребуется отправить данные одной из удаленных систем, она отправит запрос ARP. В результате всем системам, подключенным к сегменту локальной сети, будет разослано оповещающее сообщение, запрашивающее адрес целевой системы. В удаленных системах оповещающие сообщения не отображаются. Но в системе с ARP Proxy хранится список удаленных систем. Когда система получает запрос ARP на получение адреса одной из удаленных систем, она отправляет в ответ на этот запрос адрес требуемой системы. После этого сервер получает данные и пересылает их удаленной системе. Для пересылки необходимо, чтобы в параметре Пересылка пакетов IP было указано значение *YES. Если соединение с удаленной системой не установлено, то сервер не отвечает на запрос ARP, поэтому локальная система не отправляет данные.

Прозрачный доступ к подсетям

Прозрачные подсети могут использоваться для расширения протокола proxy ARP. Роль Proxy для всей подсети или диапазона хостов может играть подсеть с прозрачным доступом. Функция прозрачного доступа к подсетям позволяет создать фиктивную сеть, которой будут присвоены адреса, не лежащие в адресном пространстве основной сети.

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).



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. В приведенном выше рисунке три сети подключены к локальной сети 10.1.x.x через платформу System i. 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 и 10.1.3.x. Все данные, отправляемые локальным компьютерам, автоматически отправляются серверу, расположенному в локальной сети. Сервер, в свою очередь, пересылает данные, отправленные локальным компьютером, соответствующему удаленному серверу. Удаленный сервер 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. На локальных рабочих станциях не нужно обновлять записи маршрутизации, так как никакие логические сети не создаются.

Динамическая маршрутизация

Динамическая маршрутизация обеспечивает автоматическое обновление таблиц маршрутизации при изменении конфигурации сети.

- | Функция динамической маршрутизации предоставляется Протоколами внутренних шлюзов (IGP).
- | Операционная система i5/OS поддерживает два протокола внутренних шлюзов (IGP): протокол информации о маршрутизации (RIP) и протокол кратчайшего пути (OSPF).

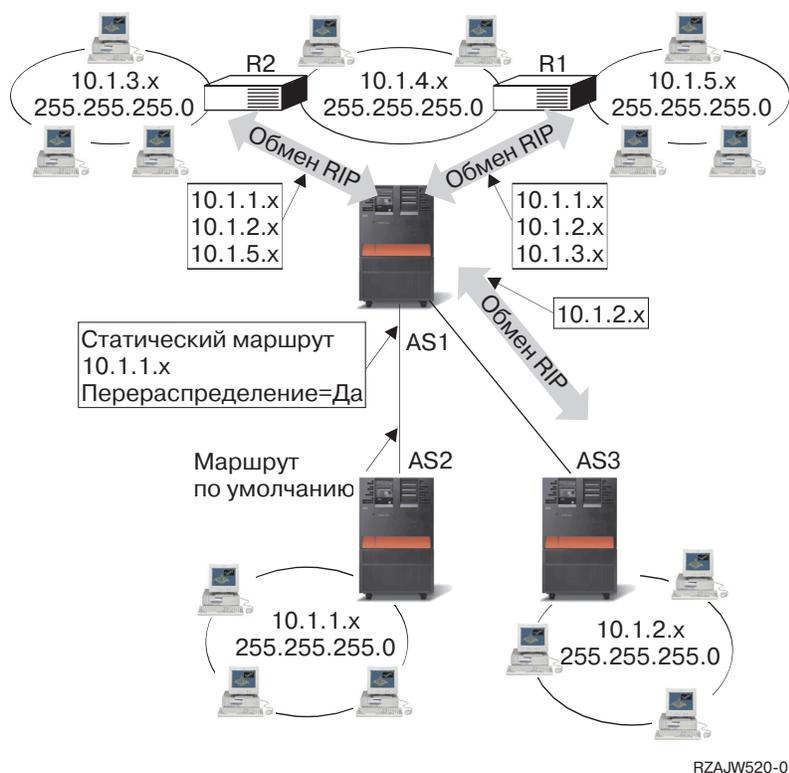
Протокол информации о маршрутизации

Протокол информации о маршрутизации (RIP) - это протокол дистанционно-векторной маршрутизации. Маршрутизаторы, работающие через этот протокол, отправляют всю или часть своей таблицы маршрутизации соседям в сообщении для обновления.

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 сети или остановке сетевой связи. В System i 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 на центральную платформу System i (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.



Следующий процесс описывает маршрутизацию потока в предыдущей схеме.

- 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.

| Протокол кратчайшего пути

| *Протокол кратчайшего пути (OSPF)* - это протокол маршрутизации с выявлением маршрутов по состоянию связи, разработанный для сетей IP и основанный на алгоритме поиска кратчайшего пути (SPF). OSPF - это протокол внутренних шлюзов (IGP).

| В сетях OSPF маршрутизаторы или системы из одной области поддерживают одну и ту же базу данных выявленных маршрутов, описывающую топологию области. Каждый маршрутизатор или система в области создает свою базу данных информации о состоянии каналов, которая состоит из объявлений маршрутов (LSAs), полученных от всех маршрутизаторов или систем в области, а также от LSA, генерирующихся самостоятельно. LSA - это пакет, содержащий сведения о соседях и оценку пути. Используя базы данных с

| выявлением маршрутов по состоянию связи, каждый маршрутизатор или сервер с помощью алгоритма
| поиска кратчайшего пути (SPF) строит остовное дерево путей, в котором корнем является сам
| маршрутизатор или сервер.

| Протокол OSPF обладает следующими ключевыми преимуществами:

- | • По сравнению с такими протоколами дистанционно-векторной маршрутизации, как протокол
| информации о маршрутизации (RIP), OSPF больше подходит для обслуживания больших неоднородных
| сетевых комплексов. OSPF позволяет вычислять пути маршрутизации за очень короткое время, если
| топология сети меняется.
- | • С помощью протокола OSPF можно разделить автономную систему (AS) на отдельные области и
| обрабатывать их топологии отдельно, чтобы снизить поток маршрутизации OSPF и уменьшить размер
| базы данных маршрутов каждой области.
- | • OSPF обеспечивает равноценную маршрутизацию с обходными путями. С помощью различных
| транзитных узлов можно добавлять дополнительные маршруты в стек TCP.

| **Протокол приветствия Hello и обмен базами данных маршрутов по состоянию сети**

| После того, как маршрутизаторы или серверы сети OSPF настраивают интерфейсы, они отправляют через
| интерфейсы OSPF пакеты Hello с помощью протокола приветствия Hello, для поиска соседей. Соседями
| являются маршрутизаторы или серверы, имеющие интерфейсы в общей сети. Затем они обмениваются
| собственными базами данных маршрутов для установления связи.

| На следующем рисунке изображен процесс поиска соседей и установления связи между двумя системами в
| подсети 9.7.85.0. Каждая система имеет интерфейс OSPF в общей подсети 9.7.85.0 (интерфейс 9.7.85.1 для
| системы А и интерфейс 9.7.85.2 для системы В). Подсеть 9.7.85.0 входит в область 1.1.1.1.

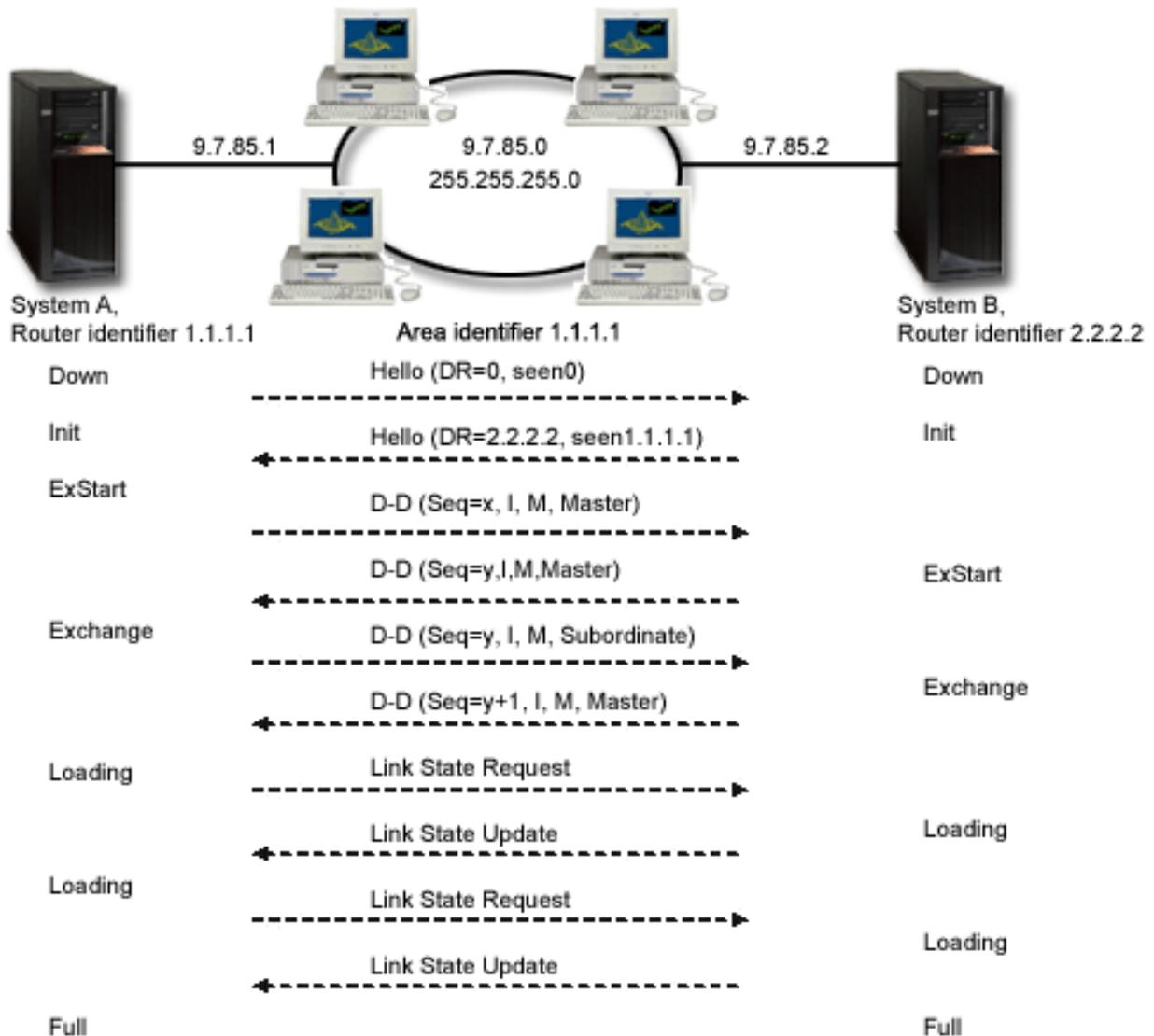


Рисунок 1. Протокол OSPF Hello и обмен базами данных

Этап EXSTART

Это первый этап обмена базами данных выявлением маршрутов по состоянию связи. Среди двух систем определяются главная и подчиненная.

Этап EXCHANGE

Две системы обмениваются пакетами описания баз данных для поиска пакетов LSA, которые отсутствуют в базе данных каждой системы. Найденные новые LSA система добавляет в список повторной передачи.

Этап LOADING

Каждый сервер отправляет соседу (в данном примере, другой системе) пакет с выявлением маршрутов по состоянию связи с запросом переслать все LSA, которые были добавлены с список повторной передачи на этапе EXCHANGE. В ответ на запрос сосед отправляет LSA в пакете обновления маршрутов.

Этап FULL

После того как системы завершают обмен LSA и синхронизируют свои базы данных, между ними устанавливается соответствие.

| После установления такого соответствия каждый маршрутизатор и сервер периодически отправляет свои
| LSA соседям для обновления всех баз данных. Путем сравнения полученных LSA маршрутизаторы или
| серверы одной области отслеживают все изменения в топологии области и соответственно обновляют свои
| базы данных маршрутов.

| **Отмеченный маршрутизатор и резервный отмеченный маршрутизатор**

| В сетях OSPF с параллельным доступом, в которых есть не меньше двух присоединенных маршрутизаторов,
| отмеченный маршрутизатор и резервный отмеченный маршрутизатор выбираются с помощью протокола
| приветствия Hello. (Сеть с параллельным доступом - это сеть, в которой несколько устройств могут
| подключаться и обмениваться данными одновременно.)

| Отмеченный маршрутизатор создает LSA для всей сети с параллельным доступом, передает их другим
| маршрутизаторам сети и определяет смежные маршрутизаторы. Все остальные маршрутизаторы сети
| являются смежными для отмеченного маршрутизатора. Отмеченный маршрутизатор уменьшает сетевой
| поток и размер базы данных маршрутов сети.

| Резервный отмеченный маршрутизатор отличается от остальных только тем, что для него необходимо
| отдельно устанавливать смежность со всеми маршрутизаторами сети (включая отмеченный). Резервный
| отмеченный маршрутизатор становится основным, если предыдущий отмеченный маршрутизатор выходит
| из строя.

| На Рисунке 1, подсеть 9.7.85.0 является коммутационной сетью. Таким образом, маршрутизаторы в подсети
| 9.7.85.0 выбирают основной и резервный отмеченные маршрутизаторы с помощью протокола приветствия.
| На данном примере, сервер А выбран основным отмеченным маршрутизатором, а сервер В - резервным.

| **Разделение автономной сети OSPF на области**

| В отличие от RIP, OSPF может работать внутри иерархии. Самой большой сущностью иерархии является
| автономная система. Автономная система - это группа сетей с общим администрированием и стратегией
| маршрутизации. Автономная система может быть разделена на области, соединенные между собой с
| помощью маршрутизаторов. Область состоит из группы смежных сетей и присоединенных хостов.
| Топология области является невидимой для сущностей вне области. Маршрутизаторы внутри области
| имеют одинаковые базы данных с информацией о состоянии каналов. Топология отдельных областей
| позволяет сократить потоки маршрутизации и уменьшить базу данных информации о состоянии каналов
| для каждой отдельной области.

| Маршрутизатор, расположенный на границе областей OSPF и соединяющий эти области с сетевой
| магистралью, называется граничным маршрутизатором. Граничный маршрутизатор имеет несколько
| интерфейсов для нескольких областей и поддерживает отдельные базы данных информации о состоянии
| каналов для каждой области.

| В следующем примере настроены две области (область 1.1.1.1 и область 2.2.2.2). Сервер В является
| граничным маршрутизатором с интерфейсом 9.7.85.2, подключенным к области 1.1.1.1, и интерфейсом
| 9.5.104.241, подключенным к области 2.2.2.2. Сервер В имеет две базы данных информации о состоянии
| каналов, по одной для каждой области. Сервер В устанавливает смежность между сервером А и
| маршрутизатором С в области 1.1.1.1 через интерфейс 9.7.85.2, и между сервером D в области 2.2.2.2 через
| интерфейс 9.5.104.241.

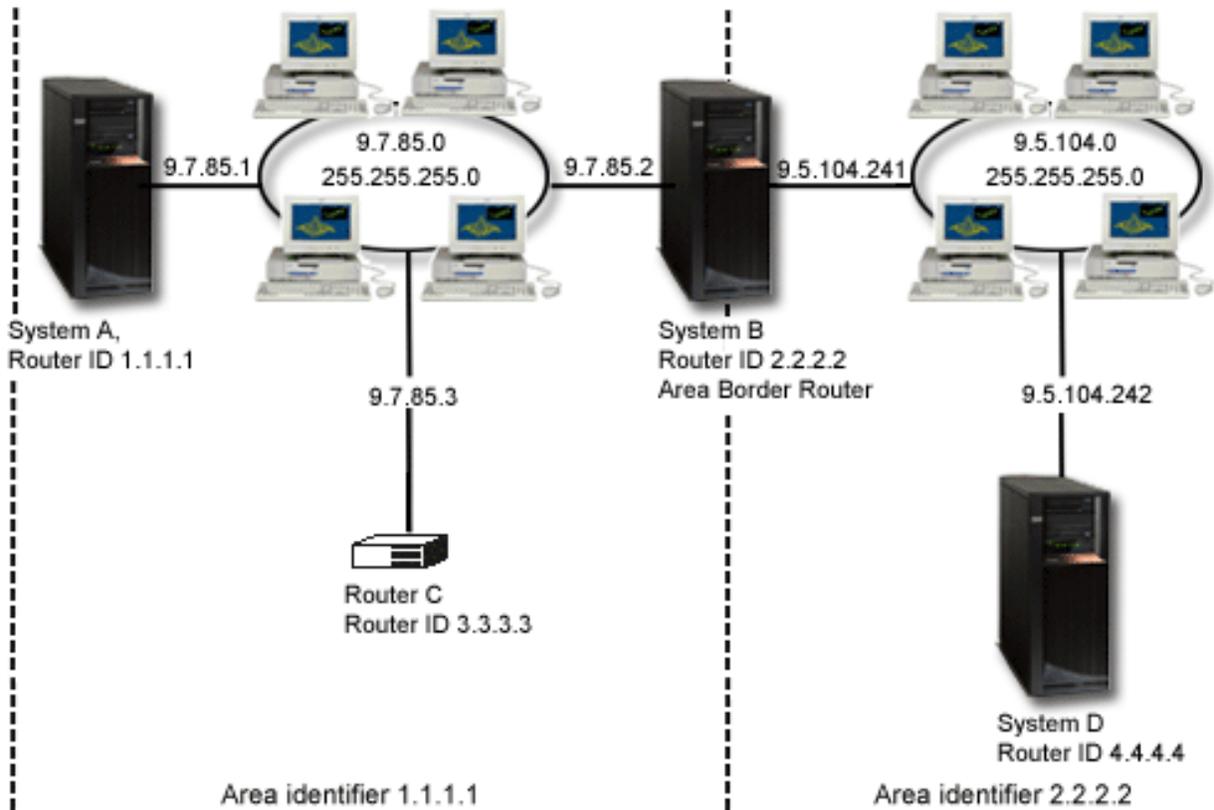


Рисунок 2. Разделение автономной сети OSPF на области

Понятия, связанные с данным

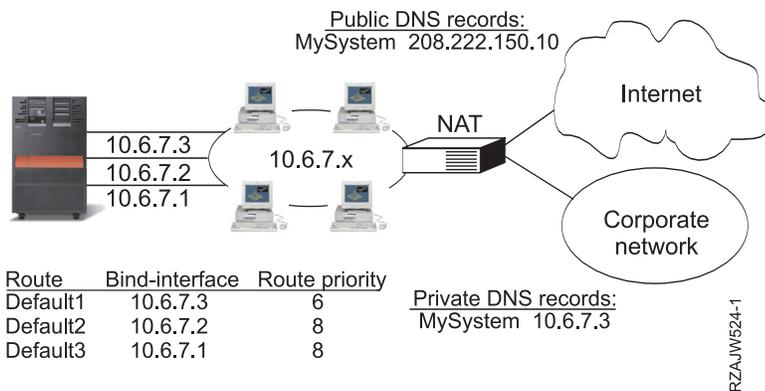
Протокол кратчайшего пути (OSPF)

Связывание маршрутов

Связывание маршрутов позволяет задать интерфейс для отправки пакетов, содержащих ответ на сообщение.

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 следующей схеме приведен пример системы, в которой три интерфейса связаны с одной сетью. Для того чтобы все входящие запросы могли приниматься через все интерфейсы, необходимо продублировать маршруты для каждого интерфейса. В данном примере добавляется при маршрута по умолчанию; каждый из которых явно связан с соответствующим интерфейсом. Связи между интерфейсами и маршрутами не зависят от порядка включения и выключения интерфейсов.



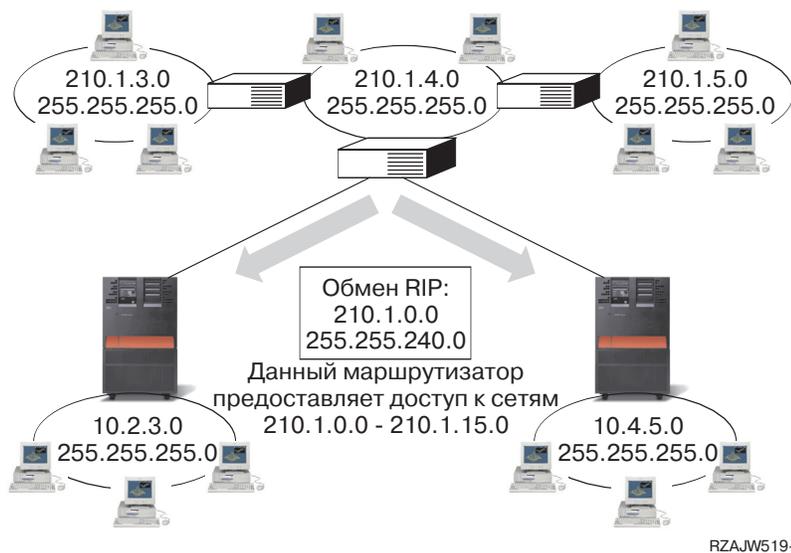
Бесклассовая междоменная маршрутизация

Бесклассовая междоменная маршрутизация позволяет сократить размер таблиц маршрутизации и увеличить число свободных IP-адресов.

Бесклассовая междоменная маршрутизация (CIDR или supernetting) предоставляет способ для объединения нескольких диапазонов адресов класса С в одну сеть, или маршрут. Такой способ маршрутизации позволяет увеличить число IP-адресов класса С. 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 С 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 С. При этом задача настройки маршрутов значительно усложнялась.

Теперь CIDR позволяет объединять смежные адреса класса С в один диапазон сетевых адресов с помощью маски подсети. Например, если у вас есть четыре сетевых адреса класса С (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.

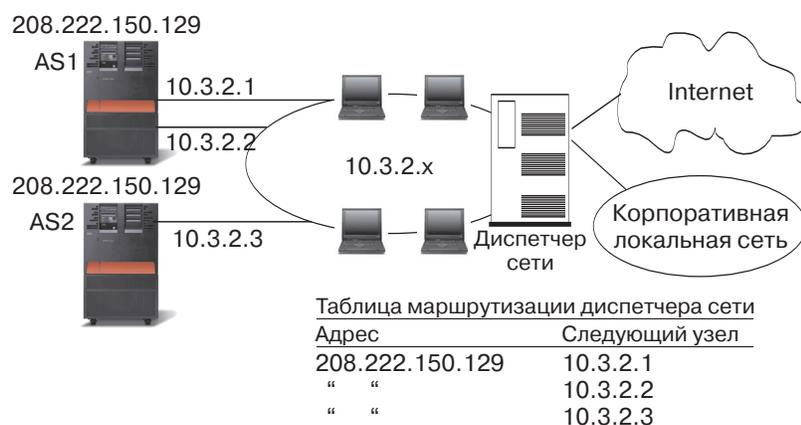


В этом примере маршрутизатор отправляет одно сообщение RIP с адресом сети 210.1.0.0 и маской подсети 255.255.240.0. Таким образом, система будет получать сообщения RIP для сетей с 210.1.0.0 по 210.1.15.0, отправленные через этот маршрутизатор. В данном случае с помощью CIDR вместо шестнадцати сообщений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

Маршрутизация с помощью виртуальных IP-адресов

Виртуальные IP-адреса, или циклические интерфейсы, - это мощное средство для присвоения адресов одному или нескольким серверам без необходимости присваивать адреса физическим интерфейсам.

За счет этого, в частности, можно запустить несколько экземпляров сервера, связанных с различными адресами, или другой службы, которая работает с портом по умолчанию. Чаще всего виртуальные адреса применяются в случаях, когда необходимо создать несколько логических каналов для передачи данных между шлюзом и платформой System i, например, с целью распределения нагрузки или обеспечения устойчивости к сбоям. Для этого на сервере необходимо создать несколько дополнительных интерфейсов и приобрести дополнительные, не виртуальные IP-адреса, как показано на следующем рисунке.



Преимущество: Недостаток:
 - Диспетчеризация в соответствии с нагрузкой - Требуется внешний диспетчер сети

RZAJW510-0

О наличии нескольких интерфейсов должно быть известно только в локальной сети. Удаленным клиентам не должны быть известны все IP-адреса сервера. 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. Для того чтобы скрыть эту информацию, применяются виртуальные IP-адреса. Локальные клиенты подключаются к серверу с помощью любого из физических адресов, в то время как удаленные клиенты подключаются через виртуальный интерфейс IP.

Поддержка виртуальных IP-адресов в основном предназначена для тех серверов, которые обслуживают удаленных клиентов. Немаловажно, что виртуальный IP-адрес и физические интерфейсы расположены в разных подсетях. Более того, виртуальный IP-адрес позволяет представить сервер во внешней сети в виде отдельного хоста, которые 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 никогда не отвечает на запросы
- | Протокола преобразования адресов (ARP), кроме того случая, когда проху ARP включен для виртуального
- | IP-адреса. Другими словами, если включить проху ARP, то локальный интерфейс может отвечать на запросы
- | ARP от имени виртуального IP-адреса. В противном случае удаленная система должна обладать заданным
- | маршрутом для нахождения адреса. Теперь можно настраивать виртуальный IP-адрес проху ARP для
- | виртуального интерфейса IP, когда интерфейс запущен.

В приведенном ниже примере на всех рабочих станциях в качестве следующего промежуточного шлюза задан один из интерфейсов 10.3.2 сервера. Сервер 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.

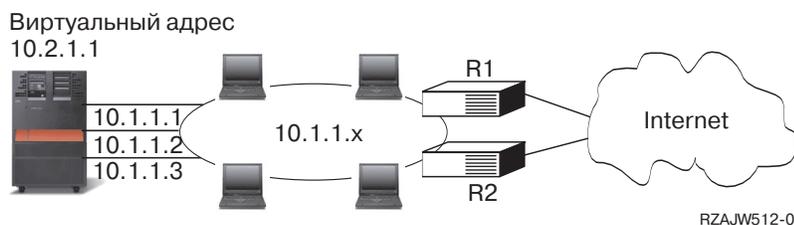
- | Теперь виртуальные IP-адреса поддерживают адреса IPv6.

Устойчивость к сбоям

Виртуальные IP-адреса также применяются для защиты от сбоя маршрутизатора. В этом разделе описано несколько способов восстановления маршрута после 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.

Сбой в сети: Выбираются другие маршруты, если они доступны



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.

- | Интерфейс PPP или протокола L2TP может использовать виртуальный IP-адрес в качестве локального IP-адреса с целью обеспечения отказоустойчивости удаленных программ подключения.

Маршрутизация с преобразованием сетевых адресов

Такой способ маршрутизации может применяться для защиты внутренней сети при подключении к внешним сетям, например, Internet. Функция Маршрутизации с преобразованием сетевых адресов (NAT) позволяет скрыть IP-адреса локальных компьютеров.

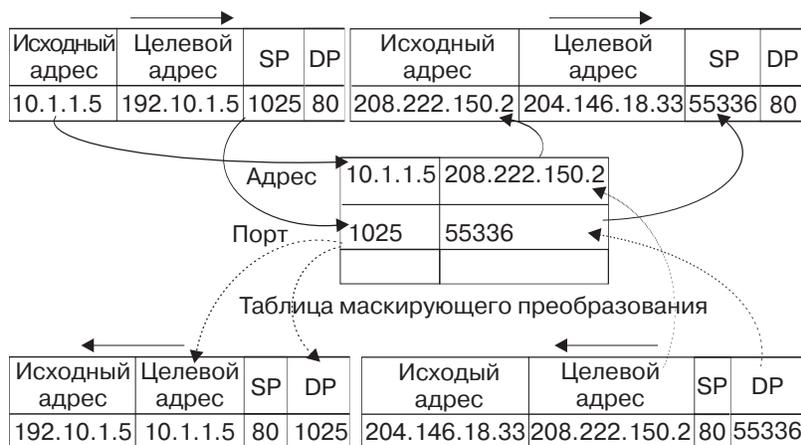
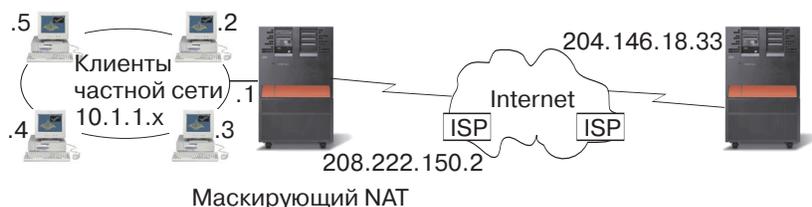
NAT применяется при подключении ко внешним сетям, в частности, Internet, для защиты внутренней сети. Она позволяет скрыть IP-адреса локальных компьютеров, расположенных за брандмауэром.

Маскирующий NAT

Маскирующий NAT позволяет скрыть частную сеть, присвоив ей только один адрес внешней сети, который будет представлять всю частную сеть.

Чаще всего 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 в помощью операционной системы i5/OS. Провайдер Internet передает серверу i5/OS IP-адрес шлюза в Internet. Термин *локальный присоединенный компьютер* относится ко всем компьютерам внутренней сети, независимо от способа их подключения (LAN или WAN) и удаленности расположения. Термин *внешние системы* обозначает компьютеры, расположенные в сети Internet. На схеме ниже показана схема работы маскирования NAT.



RZAJW507-0

С точки зрения хостов Internet все соединения, устанавливаемые локальными рабочими станциями, устанавливаются одним компьютером; это вызвано тем, что с системой и рабочей станцией связан общий IP. 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 i5/OS. В тот момент, когда рабочая станция отправляет серверу i5/OS 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 защиты. 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 входящих сообщений маскирующим NAT (ответов и прочих сообщений)::

Этот процесс, работающий вместе с исходящим маскирующим NAT, позволяет по исходящему сообщению получить правильный источник информации.

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.

Обработка исходящих сообщений маскирующим NAT:

Этот процесс заменяет исходный порт исходящего сообщения уникальным номером логического порта, когда сообщение отправляется из внутренней сети в Internet.

Исходящим сообщением на предыдущей иллюстрации называется пакет, который отправляется из 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. Ниже описана процедура обработки исходящих сообщений маскирующим NAT:

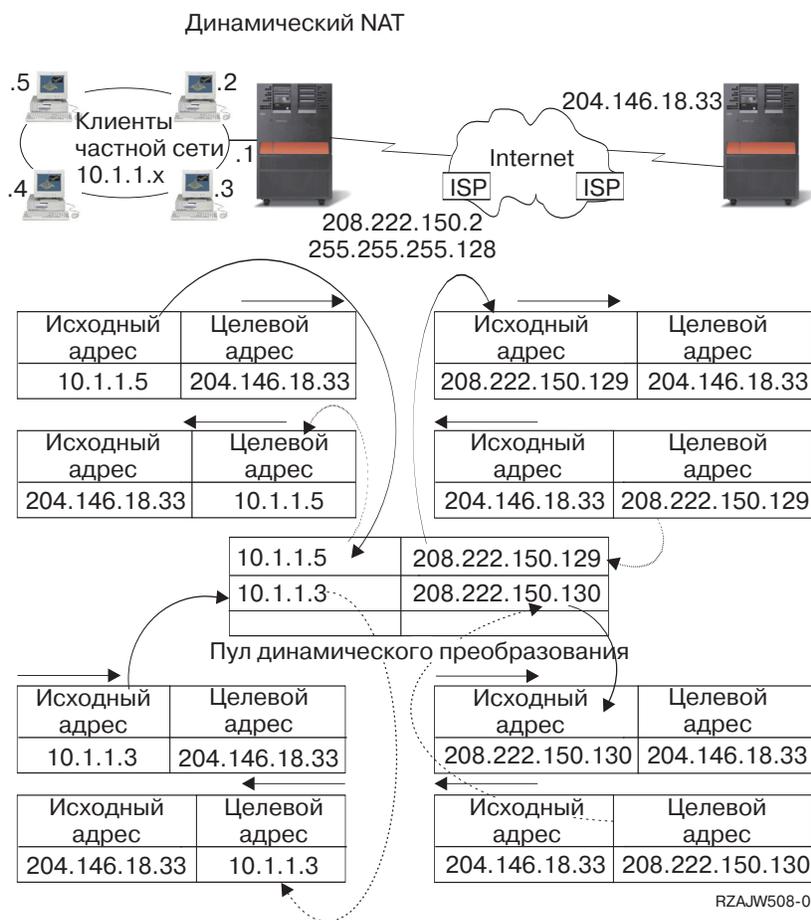
1. При обработке исходящих сообщений маскирующий NAT предполагает, что все получаемые им пакеты IP адресованы внешним хостам. Он не проверяет, что пакет действительно должен быть отправлен во внешнюю сеть, а не локальной рабочей станции.

- 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.
- Преобразуется IP-адрес отправителя.
- Пакет обычным образом обрабатывается протоколом IP и передается указанному внешнему хосту.

Динамический NAT

Динамический NAT применяется при подключении компьютеров внутренней сети к хостам внешней сети.

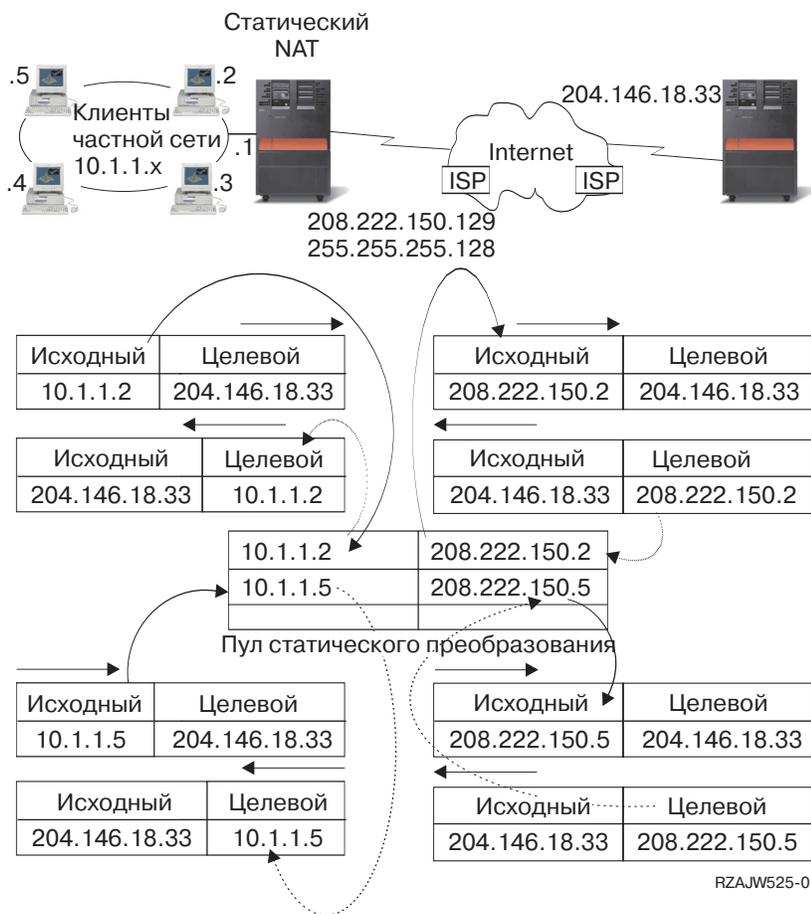
При таком способе преобразования адресов создается пул сетевых адресов, применяемый для установления соединений с внешней сетью. Каждому соединению присваивается уникальный внешний адрес. Максимальное число активных соединений ограничено числом внешних адресов в пуле. Другими словами, между соединениями и адресами устанавливается взаимно-однозначное соответствие. Динамический NAT позволяет подключаться к Internet с помощью IP-адреса, выделенного из пула. На следующей схеме приведен пример динамического NAT.



Статический NAT

Статический NAT применяется при подключении внешних хостов к внутренней сети.

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.



Понятия, связанные с данным

“Распределение нагрузки с помощью DNS” на стр. 25

Этот способ применяется для распределения нагрузки, связанной с обслуживанием входящих соединений. В основном он используется для распределения нагрузки, связанной с обслуживанием локальных клиентов.

Маршрутизация в системе несколькими разделами с помощью OptiConnect

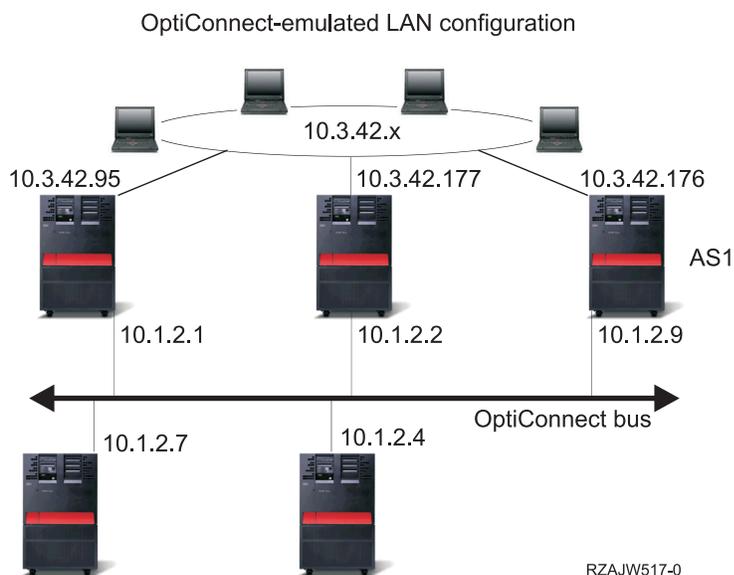
OptiConnect позволяет подключить несколько платформ System i с помощью высокоскоростной оптоволоконной шины передачи данных. В системе с несколькими разделами и шиной OptiConnect также могут применяться основные функции маршрутизации - протокол ARP Proxu, двухточечный протокол и виртуальные интерфейсы IP.

TCP/IP и OptiConnect

Соединения TCP/IP можно определять через шину OptiConnect. Для соединений TCP/IP через шину OptiConnect могут применяться другие методы маршрутизации, основанные на ARP Proxu, нумерованных двухточечных соединениях и виртуальных интерфейсах IP.

Для настройки маршрутизации TCP/IP через шину OptiConnect 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 настройке двухточечного соединения OptiConnect для каждой пары хостов OptiConnect настраивается нумерованный 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 дополнительные описания маршрутов. Соединение между хостами из разных сетей устанавливается автоматически. Другим преимуществом является то, что если обе сети активны, то данные, которыми обмениваются эти сети, 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 нумерованных двухточечных соединений. Помните, что при настройке нумерованного 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. Как показано на схеме ниже, с нумерованным двухточечным интерфейсом может быть связан основной интерфейс локальной сети системы. Роль такого интерфейса может играть и виртуальный интерфейс IP.

В конфигурации двухточечного соединения OptiConnect с помощью виртуального IP-адреса шина OptiConnect рассматривается как набор двухточечных соединений. Для каждой пары хостов настраивается нумерованное соединение. При этом, как и в соединении через OptiConnect, дополнительные маршруты создавать не требуется, и соединения между хостами из разных сетей устанавливаются автоматически. Преимуществом этого способа является то, что к любому серверу, запущенному в операционной i5/OS можно подключиться при наличии хотя бы одной активной системы.

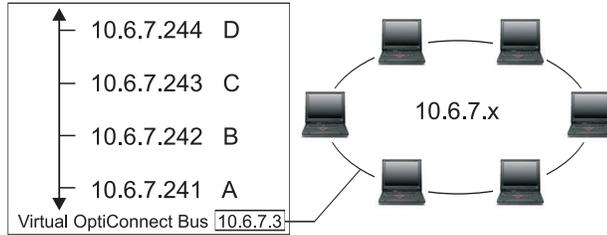
Маршрутизация виртуальных соединений OptiConnect в системе с несколькими разделами

Система 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. В TCP/IP каждый раздел представляет собой отдельную систему. 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.

Logical partitions: Virtual OptiConnect TCP/IP interfaces are used as inter partition communication paths.

Virtual OptiConnect network = 10.6.7.241 - 10.6.7.254
This provides addresses for up to 14 partitions



Partition	Interface	Line	Subnet mask	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

(Associated local interface = 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.

Виртуальный								Локальный
OPC	Раздел	адрес	Раздел	Интерфейс	Линия	Маска подсети	MTU	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
10.6.7.1			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
10.6.7.1			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
10.6.7.1			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
10.6.7.2			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 по сетевым соединениям, и работы, выполняемой сильно загруженными системами, по нескольким процессорам, сетевым адаптерам или серверам хоста.

Для получения максимальной производительности операционной системы i5/OS, необходимо распределить нагрузку, связанную с передачей данных по сети, по нескольким компонентам сервера.

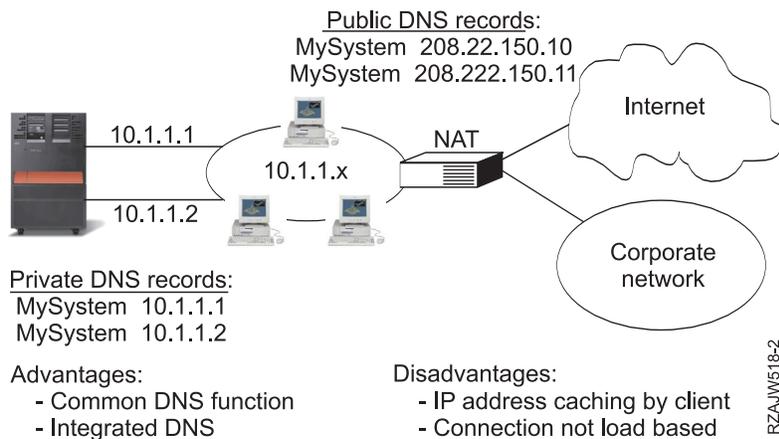
Для оптимизации нагрузки на систему можно выбрать один из следующих способов маршрутизации TCP/IP.

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.

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 сервера 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 статического NAT 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 - соединении 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).

Понятия, связанные с данным

“Статический NAT” на стр. 21

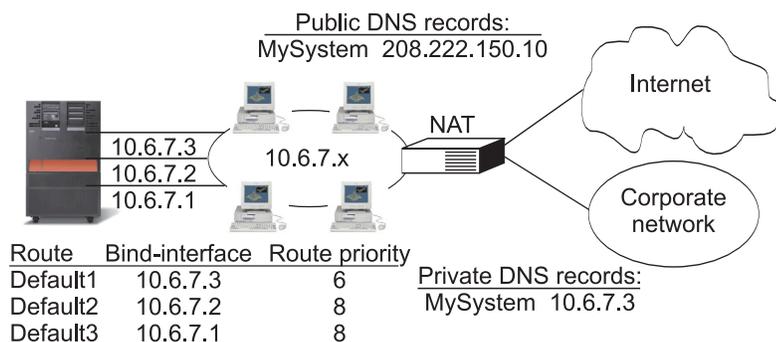
Статический NAT применяется при подключении внешних хостов к внутренней сети.

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 заключается в том, что он подходит для всех серверов i5/OS, является более гибким по сравнению с DNS и особенно эффективен для приложений, в которых основная часть потоков - 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.



Duplicate, indirect routes, with priority >(5) default will be selected according to route priority

Advantages:

- More flexibility than DNS
- Good for HTTP, Telnet

Disadvantages:

- Connection based, not load based
- Not active for local clients
- No effect on inbound requests

RZAJW511-2

Распределение нагрузки по нескольким маршрутам можно настроить с помощью команды Add TCP/IP Route (ADDTCPRTE) или с помощью интерфейса System i Navigator. Способ заключается в настройке приоритетов распределения маршрутов или предпочитаемых интерфейсов 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.

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.

Распределение нагрузки с помощью виртуальных IP-адресов и проху ARP

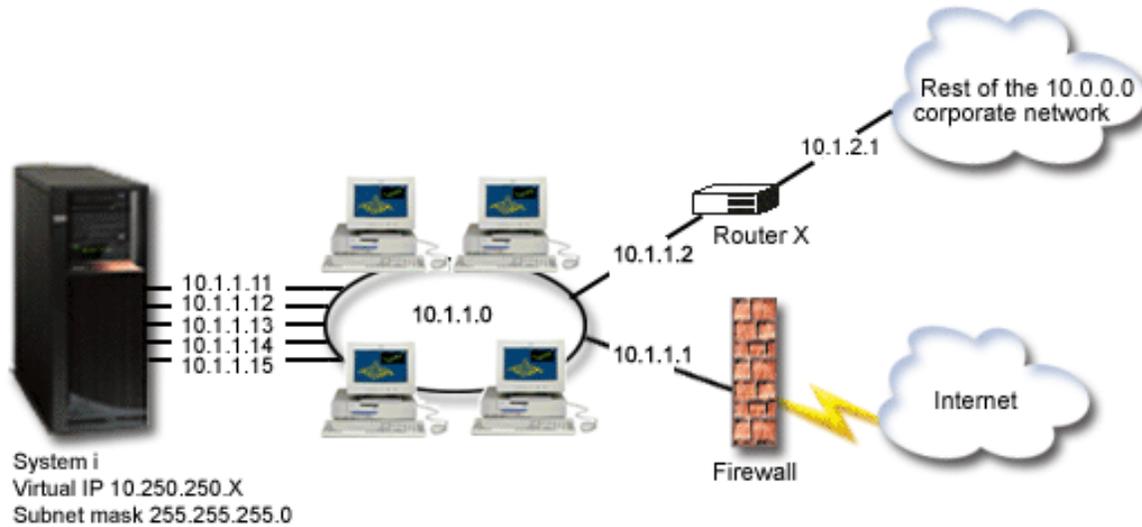
Для распределения нагрузки среди нескольких интерфейсов можно использовать виртуальный IP-адрес и проху ARP. Этот метод поддерживается для распределения нагрузки как для входящих задач, так и для исходящих.

Данный метод имеет следующие преимущества:

- Поддерживает входящие и исходящие задачи.
- Поддерживает локальные клиенты.
- Обеспечивает большую гибкость, чем другие методы распределения нагрузки по нескольким маршрутам, а также методы, основанные на DNS.

К недостаткам данного метода можно отнести то, что он основан на соединениях, а не на объеме нагрузки на сервер. Нагрузка на каждый отдельные интерфейсы не учитывается. Недостаток состоит в том, что на все соединения подается одинаковая нагрузка.

Следующий пример показывает все преимущества использования виртуальных IP-адресов. Кроме предоставления каждому приложению уникального виртуального IP-адреса, данный пример обеспечивает распределение нагрузки входящих и исходящих задач и определенный уровень отказоустойчивости.



i5/OS TCP/IP route entries				
Destination	Subnet mask	Next hop	Preferred binding interface	Duplicate route priority
10.1.1.0	255.255.255.0	10.1.1.11	10.1.1.11	6
10.1.1.0	255.255.255.0	10.1.1.12	10.1.1.12	6
10.1.1.0	255.255.255.0	10.1.1.13	10.1.1.13	7
10.1.1.0	255.255.255.0	10.1.1.14	10.1.1.14	7
10.1.1.0	255.255.255.0	10.1.1.15	10.1.1.15	7
10.0.0.0	255.0.0.0	10.1.1.2	10.1.1.11	6
10.0.0.0	255.0.0.0	10.1.1.2	10.1.1.12	6
10.0.0.0	255.0.0.0	10.1.1.2	10.1.1.13	7
10.0.0.0	255.0.0.0	10.1.1.2	10.1.1.14	7
10.0.0.0	255.0.0.0	10.1.1.2	10.1.1.15	7
*dftroute	*none	10.1.1.1	10.1.1.11	6
*dftroute	*none	10.1.1.1	10.1.1.12	6
*dftroute	*none	10.1.1.1	10.1.1.13	7
*dftroute	*none	10.1.1.1	10.1.1.14	7
*dftroute	*none	10.1.1.1	10.1.1.15	7

X

Y

Z

Virtual IP	Application
10.250.250.1	SYSNAME
10.250.250.2	HTTPSVR1
10.250.250.2	HTTPSVR2
10.250.250.11	DOM1
10.250.250.12	DOM2
10.250.250.13	DOM3

Router X routing table		
Destination	Subnet mask	Next hop
10.250.250.0	255.255.255.0	10.1.1.11
10.250.250.0	255.255.255.0	10.1.1.12

- Advantages:
- Effective for both inbound and outbound workload.
 - Effective for local clients.
 - More flexibility than the DNS-based and duplicate route-based load balancing methods.

- Disadvantage:
- Connection-based, not load-based.

Рисунок 3. Распределение нагрузки с помощью виртуальных IP-адресов и протоколу ARP

В данном примере распределение входящей нагрузки осуществляется с помощью присвоенного системе виртуального IP-адреса, а также с помощью внешнего маршрутизатора, брандмауэра и переключателя для трехуровневой маршрутизации сети. Распределение исходящих подключений осуществляется с помощью

предпочитаемого интерфейса связывания, а также дублирования параметров приоритетов маршрутов в записях маршрутов TCP/IP в i5/OS. Исходящие соединения циклически распределяются между интерфейсами с одинаковым приоритетом дополнительных маршрутов, если значение этого приоритета больше значения по умолчанию - 5. Если все интерфейсы одного приоритета становятся недоступны, система подключает интерфейсы более низкого приоритета.

Согласно директив маршрутизации в маршрутизаторе X, основные входящие интерфейсы - интерфейсы 10.1.1.11 и 10.1.1.12. Входящие соединения циклически распределяются между интерфейсами 10.1.1.11 и 10.1.1.12. Функцию распределения в основном выполняют маршрутизаторы.

Согласно записям маршрутов TCP/IP в операционной системе i5/OS, интерфейсы 10.1.1.13, 10.1.1.14 и 10.1.1.15 с приоритетом дополнительного маршрута 7 установлены как основные исходящие интерфейсы. Исходящие соединения циклически распределяются между интерфейсами 10.1.1.13, 10.1.1.14 и 10.1.1.15. Если все три интерфейса недоступны, то задействуются интерфейсы 10.1.1.11 и 10.1.1.12 с приоритетом 6 и используются для входящих и исходящих соединений.

На данном примере записи маршрутов TCP/IP в i5/OS состоят из трех групп. Группа X обеспечивает распределение исходящих соединений для локального сегмента корпоративной сети (10.1.1.0). Группа Y обеспечивает распределение входящих сообщений через маршрутизатора для остальной части сети (10.0.0.0). Группа Z используется для распределения исходящих соединений с Internet через брандмауер.

Понятия, связанные с данным

“Сценарий: Аварийное переключение адаптера с помощью виртуальных IP-адресов и ARP проху”

Виртуальный IP-адрес в отличие от фактического присваивается системе, а не сетевому интерфейсу. Один адрес можно назначить нескольким системам, что позволяет использовать многие новые возможности распределения нагрузки.

Сценарий: Аварийное переключение адаптера с помощью виртуальных IP-адресов и ARP проху

Виртуальный IP-адрес в отличие от фактического присваивается системе, а не сетевому интерфейсу. Один адрес можно назначить нескольким системам, что позволяет использовать многие новые возможности распределения нагрузки.

Примечание: Данный сценарий переключения используется для отдельных адаптеров локальной сети, а не для основных типов простых систем. Для его реализации потребуется внешний компьютер для распределения нагрузки.

Ситуация

Рабочая система получает данные от удаленных и локальных клиентов. Хранящаяся в системе информация необходима для работы компании. Вместе с ростом компании увеличивается зависимость от системы System i и пропускной способности сети. В результате становится необходимым постоянный доступ к системе. При выходе из строя одного из адаптеров его место должен занимать другой адаптер сервера 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 клиентов с системой в случае сбоя одного из адаптеров.

Сведения

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

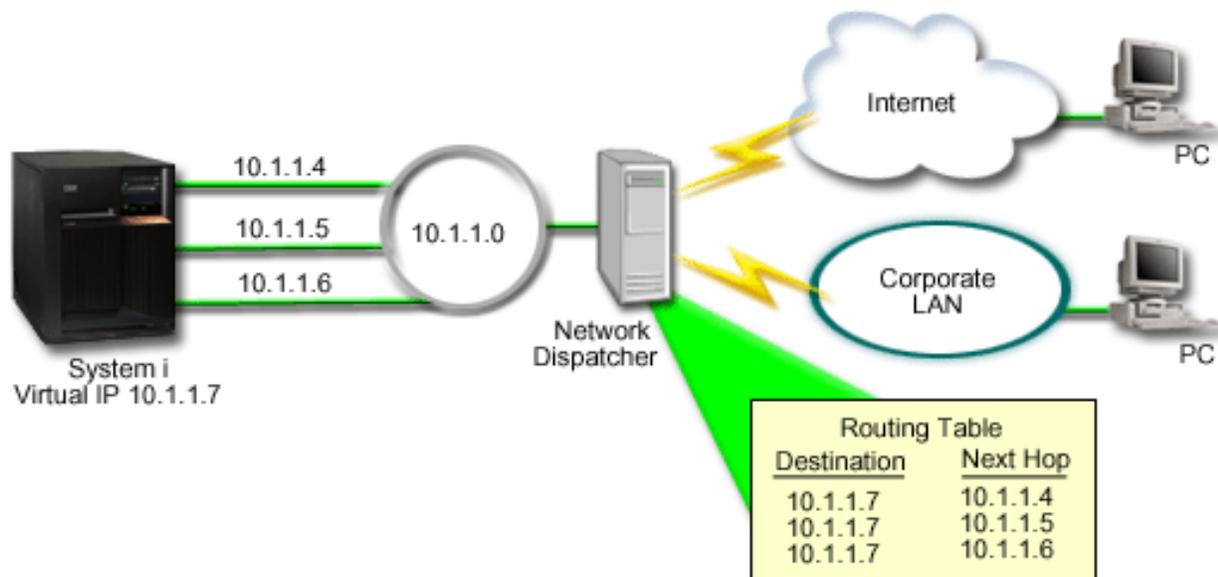


Рисунок 4. Аварийное переключение адаптера без участия локальных клиентов

Каждому физическому соединению присваивается особый 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 платформа System i) будут обращаться к системе 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.

Если часть клиентов системы 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 локальной сети. Такая ситуация показана на следующем рисунке.

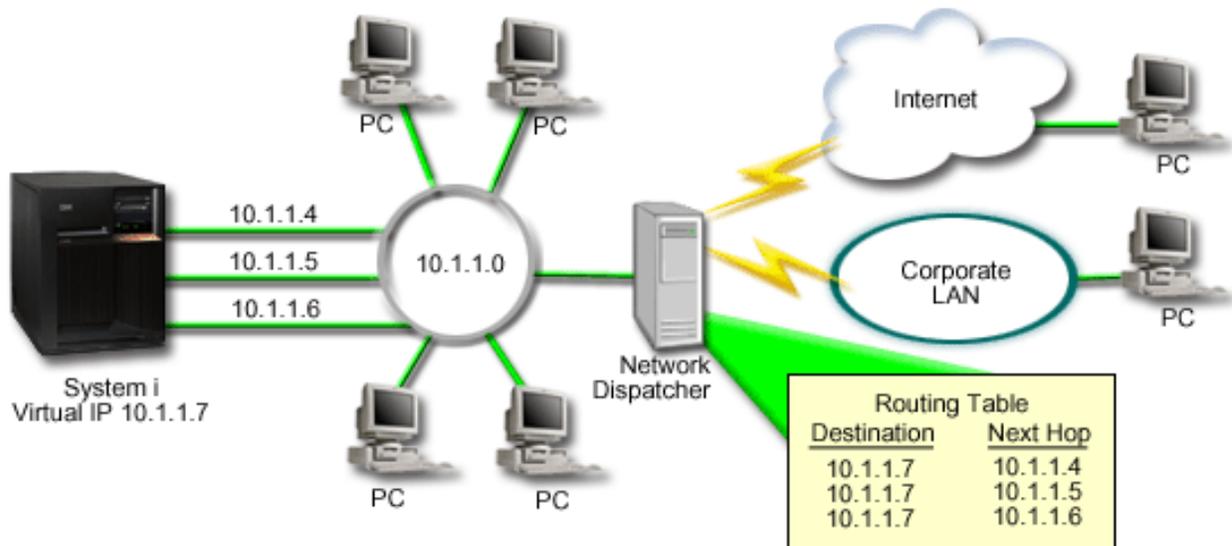


Рисунок 5. Аварийное переключение адаптера с участием локальных клиентов

Локальные клиенты (клиенты, подключенные к одной локальной сети) не могут устанавливать соединение с виртуальным IP-адресом системы через ARP. Это позволяет локальным клиентам также использовать аварийное переключение адаптера.

Обычно ни локальные, ни удаленные клиенты не узнают об аварийном переключении, даже если оно происходит. Система выбирает, какие адаптеры и IP-адреса являются предпочтительным интерфейсом для виртуального IP-адреса (VIP) для выбора агента Proxu (ARP).

Можно вручную выбирать, какие адаптеры и IP-адреса являются предпочтительным интерфейсом для VIP для выбора агента проху ARP. Можно выбрать, какой интерфейс использовать, создавая список предпочтительных интерфейсов на случай аварийного переключения адаптера. Список предпочтительных интерфейсов - это упорядоченный список адресов интерфейсов, которые включатся вместе сбойного адаптера. Для того чтобы настроить список предпочтительных интерфейсов, можно использовать или System i Navigator, или API Изменить интерфейс TCP/IP IPv4 (QTOCC4IF). Его можно также настроить одновременно для интерфейсов виртуального Ethernet и виртуального IP-адреса.

На Схеме 2 показано, как удаленные клиенты обмениваются данными с локальной системой, используя виртуальный IP-адрес 10.1.1.7. Предположим, что 10.1.1.4 является начальным локальным адаптером, который используется для обмена данными, а 10.1.1.5 должен заменить 10.1.1.4, если он выйдет из строя. К тому же интерфейс 10.1.1.6 должен заменить оба адаптера для 10.1.1.4 и 10.1.1.5, если они выйдут из строя. Для контроля того, в каком порядке эти интерфейсы будут использоваться при сбое, нужно задать список предпочтительных интерфейсов для виртуального IP-адреса 10.1.1.7. В таком случае это будет упорядоченный список адресов интерфейсов, который состоит из 10.1.1.4, 10.1.1.5 и 10.1.1.6.

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

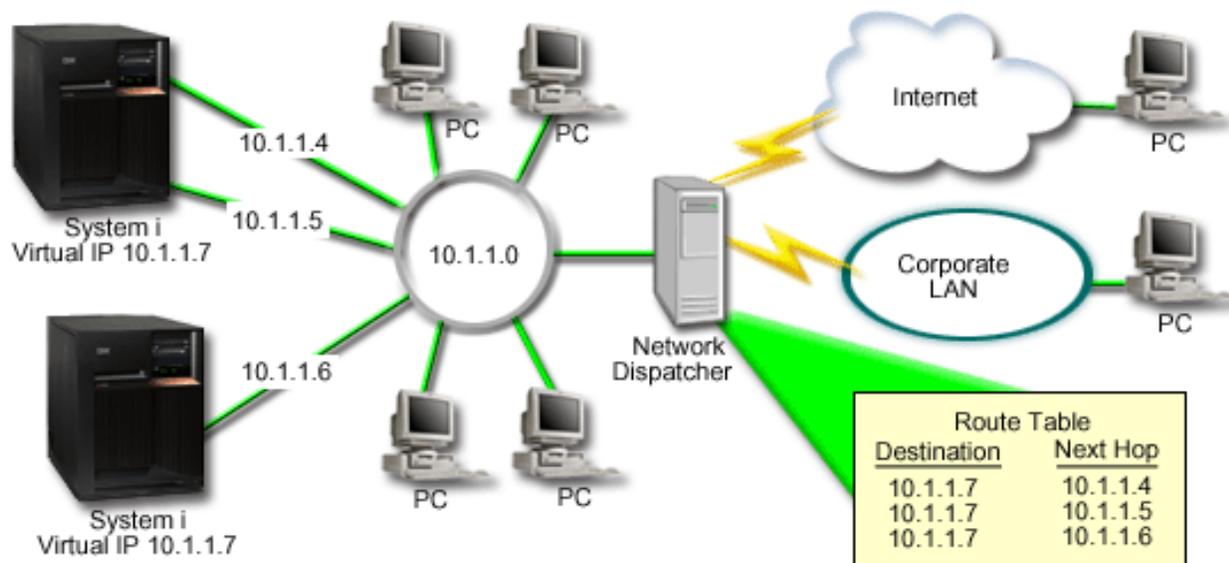


Рисунок 6. Аварийное переключение адаптера с несколькими платформами System i и локальными клиентами

Маршрутизация пакетов для самой системы и ее клиентов совпадает; для локальных клиентов есть отличия. Если с несколькими системами связан один и тот же виртуальный IP-адрес, доступ к одной из этих систем возможен только через Proxu. В этом случае одна из систем с двумя интерфейсами локальной сети может играть роль Proxu.

Шаги настройки

Конфигурация с распределением нагрузки, применяющая виртуальный IP-адрес и ARP Proxu, очень похожа на обычную конфигурацию TCP/IP, к которой добавлен виртуальный интерфейс TCP/IP.

Понятия, связанные с данным

“Распределение нагрузки с помощью виртуальных IP-адресов и proxu ARP” на стр. 27

Для распределения нагрузки среди нескольких интерфейсов можно использовать виртуальный IP-адрес и проху ARP. Этот метод поддерживается для распределения нагрузки как для входящих задач, так и для исходящих.

Переключение с помощью автоматического выбора интерфейса

Выполните следующие действия для настройки виртуального IP-адреса и протокола преобразования адресов (ARP) прокси-сервера для ситуаций переключения адаптера в данном сценарии.

Рисунок 2 - пример того, какими будут основные шаги по настройке:

1. Настройка виртуального интерфейса TCP/IP.

Создайте виртуальный интерфейс TCP/IP с помощью System i Navigator. Запустите Мастер создания виртуального интерфейса, выбрав следующие опции: **Сеть** → **Конфигурации TCP/IP** → **IPv4** → **Интерфейсы**. Щелкните правой кнопкой мыши на пункте **Интерфейсы** и выберите **Создать интерфейс** → **Виртуальный IP**.

Например, введите IP-адрес 10.1.1.7 с маской подсети 255.255.255.255. После создания виртуального интерфейса щелкните на нем правой кнопкой мыши и выберите **Свойства**. Щелкните на вкладке **Дополнительные** и выберите переключатель **Включить проху ARP**.

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

С помощью мастера Создать интерфейс TCP/IP создайте нужные интерфейсы TCP/IP. Этот мастер находится в System i Navigator и может быть запущен следующим образом: **Сеть** → **Настройка TCP/IP** →

IPv4 → Интерфейсы. Затем щелкните правой кнопкой мыши **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 мыши и выберите **Свойства**. Выберите вкладку **Дополнительно** и поставьте флажок в поле **Связанный локальный интерфейс**, чтобы связать интерфейс с виртуальным интерфейсом IP, созданным на этапе 1.

Переключение с помощью списка предпочтительных интерфейсов

Список предпочтительных интерфейсов создается для управления порядком, в котором локальные интерфейсы используются при выходе из строя адаптера.

Для создания списка предпочтительных интерфейсов выполните следующие действия:

1. В System i Navigator разверните список **Сеть → Настройка TCP/IP → IPv4**.
2. Нажмите **Интерфейсы**.
3. Из списка показанных интерфейсов выберите интерфейс для виртуального IP-адреса или виртуального Ethernet, для которого требуется создать список предпочтительных интерфейсов.
На Схеме 2 показано, как выбрать виртуальный IP-адрес 10.1.1.7.
4. Щелкните правой кнопкой мыши на значке интерфейса и затем выберите **Свойства**.
5. Щелкните на вкладке **Дополнительные**.
6. Выберите в окне адреса интерфейсов из списка доступных интерфейсов и нажмите **Добавить**.
На Схеме 2 показано, как выбрать интерфейсы 10.1.1.4, 10.1.1.5 и 10.1.1.6 и добавить их в список предпочтительных интерфейсов по одному.
Можно также удалить интерфейс из списка предпочтительных интерфейсов на правой панели с помощью кнопки **Удалить** или переместить интерфейс вверх или вниз по списку с помощью кнопок **Выше** и **Ниже**.
7. Выберите переключатель **Включить проху ARP** над списком Доступные интерфейсы, чтобы список вступил в силу.
8. Нажмите **ОК**, чтобы сохранить созданный список предпочтительных интерфейсов.

Примечание: В списке предварительных интерфейсов может быть не больше десяти записей. Если их будет больше, список будет усечен до 10.

Дополнительная информация об оптимизации маршрутизации TCP/IP и распределении нагрузки

Другие коллекции тем в information center содержат информацию о маршрутизации TCP/IP и распределении нагрузки.

Прочая информация

- 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.
- Логические разделы
 - Этот раздел содержит более основательную информацию и подробности.
- Фильтрация IP и преобразование сетевых адресов
 - Информация этого раздела помогает управлять правилами фильтрации. В частности, вы сможете узнать, каким образом можно изменить и просмотреть правила фильтрации, а также добавить к ним комментарий.
- OptiConnect

Этот раздел знакомит с информацией о маршрутизации OptiConnect.

- Службы удаленного доступа: соединения PPP

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

Ссылки, связанные с данной

“Файл PDF для маршрутизации TCP/IP и распределения нагрузки” на стр. 2
Файл PDF с данной информацией можно просмотреть и напечатать.

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 YBWA
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 этом документе 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, Соглашения о лицензии на машинный код 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.

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для того чтобы примеры были максимально наглядными, в них указаны имена людей, а также названия компаний, товарных знаков и продуктов. Все они являются вымышленными, и любое совпадение с реально существующими именами и названиями случайно.

Лицензия на продукты, защищенные авторским правом:

Эта информация содержит примеры приложений на исходном языке, иллюстрирующие приемы программирования в различных операционных платформах. Разрешается бесплатно копировать, изменять и распространять в любой форме эти примеры с целью разработки, использования и распространения прикладных программ для интерфейсов, соответствующих той операционной платформе, для которой созданы примеры. Работа примеров не была проверена во всех возможных условиях. По этой причине, IBM не может гарантировать их надежность и пригодность.

Любая копия или часть этих примеров программ, а также произведений, созданных на их основе, должна содержать следующее заявление об авторских правах:

© (название вашей фирмы) (год). Этот код частично создан на основе примеров программ фирмы IBM Corp.
© Copyright IBM Corp. _год или годы_. Все права защищены.

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

Информация об интерфейсе программирования

Публикация о маршрутизации TCP/IP и распределение нагрузки документирует рекомендуемые интерфейсы программирования, позволяющие писать программы, использующие службы IBM i5/OS.

Товарные знаки

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

i5/OS
IBM
IBM (логотип)
System i

Adobe, логотип Adobe, PostScript и логотип PostScript являются товарными знаками Adobe Systems Incorporated в США и/или других странах.

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Напечатано в Дании