

IBM

@server

iSeries

Quality of Service





@server

iSeries

Quality of Service

Содержание

Quality of Service (QoS)	1
Новое в версии V5R2	1
Как напечатать этот раздел	2
Сценарии QoS	3
Сценарий QoS: Выделенная доставка (телефонная связь IP)	3
Сценарий QoS: Ограничение потока данных браузера	6
Сценарий QoS: Ограничение числа входящих соединений	9
Сценарий QoS: Предсказуемый поток данных B2B	12
Сценарий QoS: Защита и предсказуемость (VPN и QoS)	14
Принципы QoS	17
Количество запросов на установление соединений и количество запросов URI	19
Ограничения на среднее и максимальное число соединений	20
Дифференцированные службы	20
Дифференцированные классы обслуживания	21
Кодовые знаки и обработка на транзитных участках	22
Обработчики потоков данных	23
Принципы работы сервера каталогов	24
Ключевые слова	25
Интегрированные службы	26
Функции управления потоком данных	28
Типы интегрированного обслуживания	28
Ограничения на набор маркеров и пропускную способность	29
Интегрированное обслуживание с использованием кодовых знаков дифференцированного обслуживания	30
Протокол RSVP и API QoS	30
Последовательность вызовов API QoS с установкой соединения	31
Последовательность вызовов API QoS без установки соединения	34
Планирование QoS	36
Требования к правам доступа	36
Требования к системе	37
Упорядочивание стратегий QoS	37
Соглашение об уровне обслуживания	38
Сетевое оборудование и программное обеспечение	38
Настройка QoS	39
Настройка сервера каталогов	39
Настройка QoS с помощью мастеров	40
Работа с мастерами QoS в Навигаторе	41
Управление QoS	42
Работа со справкой QoS в Навигаторе	43
Резервное копирование стратегий QoS	43
Копирование существующей стратегии	44
Монитор QoS	44
Устранение неполадок QoS	49
Ведение журнала стратегий QoS	49
Протоколы заданий сервера QoS	50
Отслеживание транзакций сервера	51
Сбор текущих статистических показателей сети	52
Трассировка приложений TCP	53
Чтение вывода трассировки	56
Связанная информация по QoS	56

Quality of Service (QoS)

Обычно всем потокам данных в сети присваивается одинаковый приоритет. Информация браузера обрабатывается так же, как важные данные деловых приложений. Если, например, исполнительный директор (CEO) компании проводит видеоконференцию, то главной задачей становится приоритетная обработка IP-пакетов. Это означает, что во время видеоконференции для данного приложения необходимо обеспечить более высокую производительность по сравнению с остальными приложениями.

QoS позволяет зарезервировать приоритет и пропускную способность сети для приложений TCP/IP. Это важно при работе с приложениями, которые должны выдавать надежные и предсказуемые результаты, например при работе со средствами мультимедиа.

Перед тем, как приступить к планированию правил стратегий, следует ознакомиться с общей информацией о QoS. Ниже приведены ссылки на информацию, которая поможет вам в реализации функций QoS.

Новое в версии V5R2

Сведения об изменениях в сетевой функции Quality of Service и содержимом Information Center.

Как напечатать этот раздел

Инструкции по печати содержимого раздела.

Сценарии QoS

Сценарии стратегий QoS демонстрируют работу с QoS на конкретных примерах.

Принципы QoS

Базовые сведения о QoS. Информация этого раздела дает представление о работе QoS и взаимодействии механизмов QoS.

Планирование QoS

Ссылки на Советник по планированию и источники информации, необходимой для эффективной работы с QoS.

Настройка QoS

Инструкции по созданию стратегий дифференцированного и интегрированного обслуживания.

Управление QoS

Инструкции по изменению стратегий. Здесь описаны процедуры удаления стратегий, трассировки стратегий, а также другие операции управления стратегиями.

Устранение неполадок QoS

Инструкции по устранению неполадок QoS.

Связанная информация по QoS

Ссылки на другие источники информации о QoS. Дополнительную информацию по этой теме можно найти в руководствах, на Web-сайтах, в документах RFC и спецификациях.

Новое в версии V5R2

В этом разделе описаны новые функции, добавленные в версии V5R2, а также некоторые усовершенствования структуры информации данного документа.

Новые функции



- **Связывание стратегий с локальными интерфейсами**
Стратегии можно связать с отдельным локальным интерфейсом или с диапазоном интерфейсов сервера iSeries^(TM). Эта функция позволяет применять к пакетам различные стратегии на основе целевого интерфейса.
- **Связывание стратегий с несколькими клиентами**
Стратегию можно связать с несколькими клиентами. Это позволяет создавать более гибкие определения стратегий.
- **Стратегии входящих соединений**
В новой версии можно создавать стратегии для управления потоком данных, поступающих на сервер. Два новых мастера позволяют настроить стратегии для потоков данных, запрашивающих предоставление доступа к определенному IP-адресу или значению URI в сети. Для получения дополнительной информации о входящих стратегиях воспользуйтесь приведенной выше ссылкой.
- **Данные монитора можно сохранить и распечатать**
Данные монитора теперь можно сохранить для последующего использования и распечатать. Для печати информации монитора в этой версии можно воспользоваться функцией “Экспортировать в формате HTML”.
- **Хранение стратегий на сервере каталогов LDAP**
В этой версии стратегии экспортируются на сервер каталогов с помощью протокола LDAP версии 3. Применение сервера каталогов обеспечивает более удобное управление QoS. Вместо того чтобы создавать одни и те же стратегии QoS на каждом из серверов, можно настроить на серверах применение данных стратегии, созданной на одном сервере. В этом случае стратегии хранятся на сервере каталогов. Воспользуйтесь этой ссылкой для получения дополнительной информации о настройке.
- **Изменение, связанное с расписаниями**
Расписания определяются временными интервалами. Ранее, поддерживались только временные интервалы в рамках одного дня. В этой версии временные интервалы могут задавать любые двадцать четыре часа, даже если в этот период попадает два календарных дня. Расписание определяет, когда применяется стратегия. Это позволяет создавать более гибкие определения стратегий.


Усовершенствования структуры раздела

- **Советник по планированию QoS**
Советник по планированию QoS теперь выводит рекомендации и информацию о предварительных требованиях перед настройкой стратегий. Этот инструмент представляет все аспекты стратегий в виде организованной структуры и, тем самым, облегчает процедуру планирования.
- **Новый сценарий входящей стратегии**
Добавлен новый сценарий, в котором продемонстрирована реализация входящей стратегии.

Условное обозначение новой и измененной информации

В этом документе технические изменения обозначены следующим образом:

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


Дополнительная информация о изменениях и нововведениях в данном выпуске приведена в документе [Информация для пользователей](#)  .

Как напечатать этот раздел

Для просмотра или загрузки версии в формате PDF выберите Quality of Service (около 378 Кб, или 53 страницы).

Для сохранения файла PDF на рабочей станции для просмотра и печати выполните следующие действия:

1. Откройте файл PDF в браузере (щелкните на приведенной выше ссылке).
2. В меню браузера выберите пункт **Файл**.
3. Выберите **Сохранить как...**
4. Укажите каталог для сохранения файла PDF.
5. Нажмите кнопку **Сохранить**.

Программу Adobe Acrobat Reader, необходимую для просмотра и печати файлов PDF, можно загрузить с Web-сайта фирмы Adobe .

Сценарии QoS

Один из лучших способов изучить функцию Quality of Service - это увидеть, как она работает в масштабах всей сети. В приведенных ниже примерах продемонстрированы основы применения стратегий Quality of Service.



Сценарий: Выделенная доставка (телефонная связь IP)

Если необходимы выделенная доставка и резервирование ресурсов, воспользуйтесь стратегией интегрированного обслуживания. Существует два типа стратегий интегрированного обслуживания: гарантированного обслуживания и управляемой нагрузки. В данном примере применяется гарантированное обслуживание.

Сценарий: Ограничение потока данных браузера

QoS позволяет управлять скоростью передачи потока данных. С помощью стратегии дифференцированного обслуживания можно ограничить или повысить производительность приложения в сети.

Сценарий: Ограничение количества входящих соединений

Для управления числом запросов на установление соединения, поступающих на сервер, применяются стратегии входящих соединений.

Сценарий: Предсказуемый поток данных B2B

Если необходима надежная доставка и резервирование ресурсов, воспользуйтесь стратегией интегрированного обслуживания. В данном примере применяется стратегия управляемой нагрузки.

Сценарий: Защита и предсказуемость (VPN и QoS)

Создавать стратегии Quality of Service можно и при работе с виртуальной частной сетью (VPN). Такая ситуация продемонстрирована в данном примере.



Примечание: Все IP-адреса и диаграммы вымышлены и приведены только в качестве примеров.

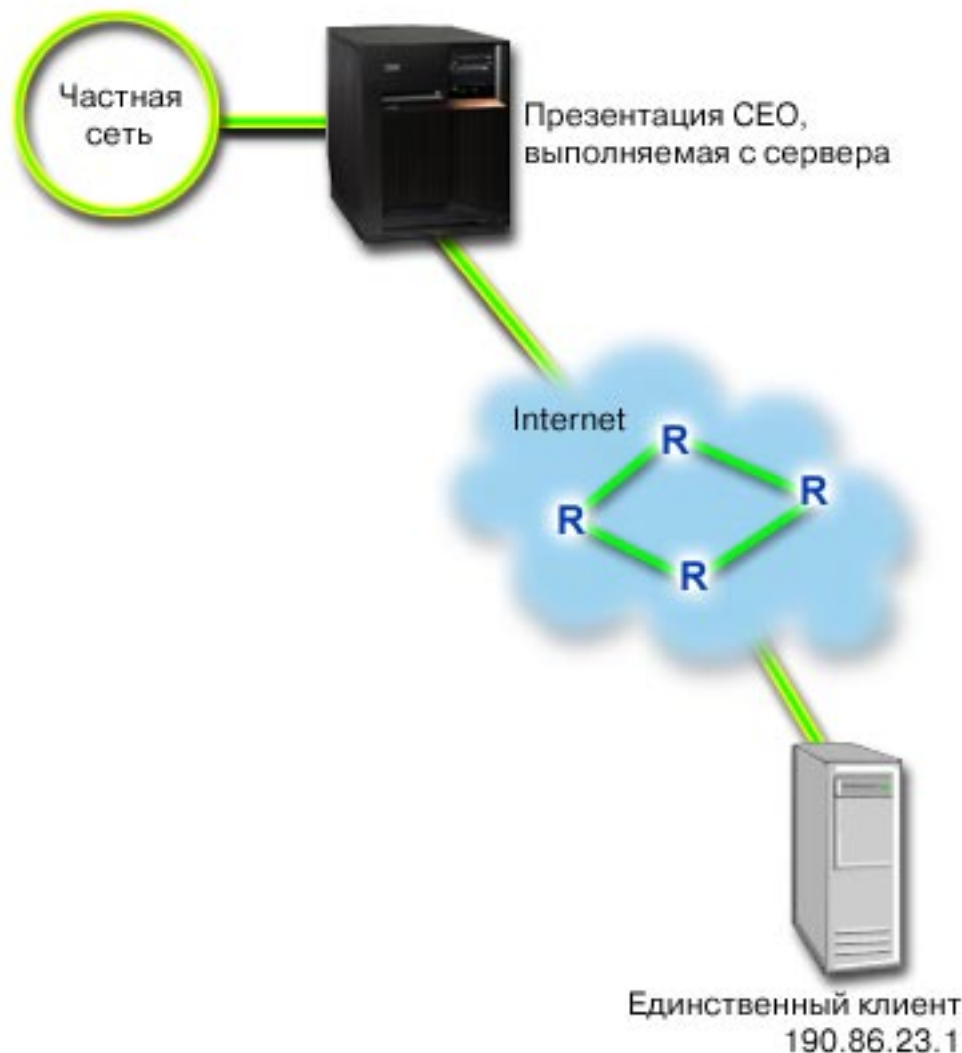
Сценарий QoS: Выделенная доставка (телефонная связь IP)



Ситуация

Исполнительный директор (chief executive officer - CEO) вашей компании дает электронную пресс-конференцию для клиента, находящегося на другом конце страны, с часу до двух дня. Вы должны обеспечить требуемую пропускную способность телефонной связи IP, чтобы пресс-конференция прошла без сбоев. В этом сценарии приложение находится на сервере. На следующем рисунке изображена конфигурация сети для этого сценария. На сервере iSeries установлена OS/400^(R) V5R2.

Рисунок 1. Пресс-конференция исполнительного директора, обеспечиваемая с помощью стратегии интегрированного обслуживания.



Вариант действий

Приложениям, для которых главное - это скорость передачи данных, требуется надежная связь. Поскольку приложению, обеспечивающему пресс-конференцию, необходимо, чтобы передача данных происходила непрерывно и без сбоев, вы решаете воспользоваться стратегией гарантированного интегрированного обслуживания. Гарантированное обслуживание ограничивает максимальное время ожидания в очереди, поэтому пакеты не задерживаются в очереди дольше указанного времени.

В силу требований, предъявляемых к соединению, вы можете воспользоваться стратегией гарантированного интегрированного обслуживания. Для применения стратегий интегрированного обслуживания необходимы приложения с поддержкой RSVP. Поскольку на сервере нет приложений, поддерживающих RSVP, вам придется создать их самостоятельно. Для создания приложений воспользуйтесь API Протокол настройки резервирования ресурсов (RAPI) или API сокетов QoS (qtoq).

Кроме того, для применения стратегий интегрированного обслуживания необходимо, чтобы на всем пути следования данных маршрутизаторы поддерживали RSVP. Более подробная информация приведена в разделе Интегрированные службы.

Настройка

1. Откройте QoS в Навигаторе.

1. В Навигаторе разверните значок сервера —> **Сеть** —> **Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
3. Откройте **Стратегии исходящих соединений**.
4. Щелкните правой кнопкой мыши на пункте **IntServ** и выберите **Создать стратегию**. Будет запущен Мастер создания стратегии IntServ.

2. Создайте стратегию интегрированного обслуживания.

Прежде всего, настройте стратегию интегрированного обслуживания с помощью мастера. Поскольку речь идет об информации, отправляемой исполнительным директором компании, вы можете назвать стратегию **CEO_guaranteed**. Клиент получает данные по IP-адресу **190.86.23.1**. Это вымышленное число, приведенное только для примера. Клиенту можно присвоить имя **Branch1**. Так как поток данных проходит через порт 2427, то приложению можно присвоить имя **port 2427**. Расписанию можно присвоить имя **1:00-2:00**. Задайте в окнах мастера следующие значения параметров:

Имя = CEO_guaranteed
Клиент = Branch1
Приложение = port 2427 (если это порт телефонной связи IP)
Локальный IP-адрес = 10.5.27.1
Протокол = TCP
Расписание = 1:00-2:00
Размер набора маркеров = 16 Кбит
Пропускная способность (R) = 10 Мбит/с
Число потоков = 1

Навигатор содержит список всех стратегий интегрированного обслуживания, созданных на сервере.

4. Проверьте работу стратегий с помощью монитора.

1. Выберите одну из папок Стратегии (DiffServ, IntServ, Запросы сервера—>URI или Число соединений).
2. Щелкните правой кнопкой мыши на стратегии, о которой необходимо собрать данные, и выберите пункт **Отслеживать**.

На следующем рисунке изображен вывод монитора с комментариями.

Рисунок 2. Монитор Quality of Service.

Имя стра...	Прото...	Диапазон целе...	Ограничение сре...	Ограничение...	Ограничени...	Всего пакет...	Всего бит	Несоответс...
CEO_Guaranteed	Все	190.86.231	10	16	20	577	4727 Кб	236 Кб

Наиболее интересны поля измеряемых значений, в которых указывается собранная информация о потоке данных. К ним относятся поля общего числа битов, числа профильных битов и числа профильных пакетов. Поле профильных битов указывает на остальную часть потока, задерживаемую или удаляемую для обеспечения требований стратегии интегрированного обслуживания. Описание всех полей монитора приведено в разделе Монитор.

3. При необходимости скорректируйте значения.

Просмотрев результаты монитора для этой стратегии, вы можете изменить значения, ранее созданные с помощью мастера.

1. Закройте монитор.
2. Щелкните правой кнопкой мыши на имени созданной стратегии.
3. Выберите пункт **Свойства**. Будет показано окно диалога Свойства IntServ_Guaranteed.
4. Выберите вкладку **Управление потоком** для изменения значений, контролирующих поток. Здесь же задаются параметры расписания, клиента, приложений и обработки потока данных.



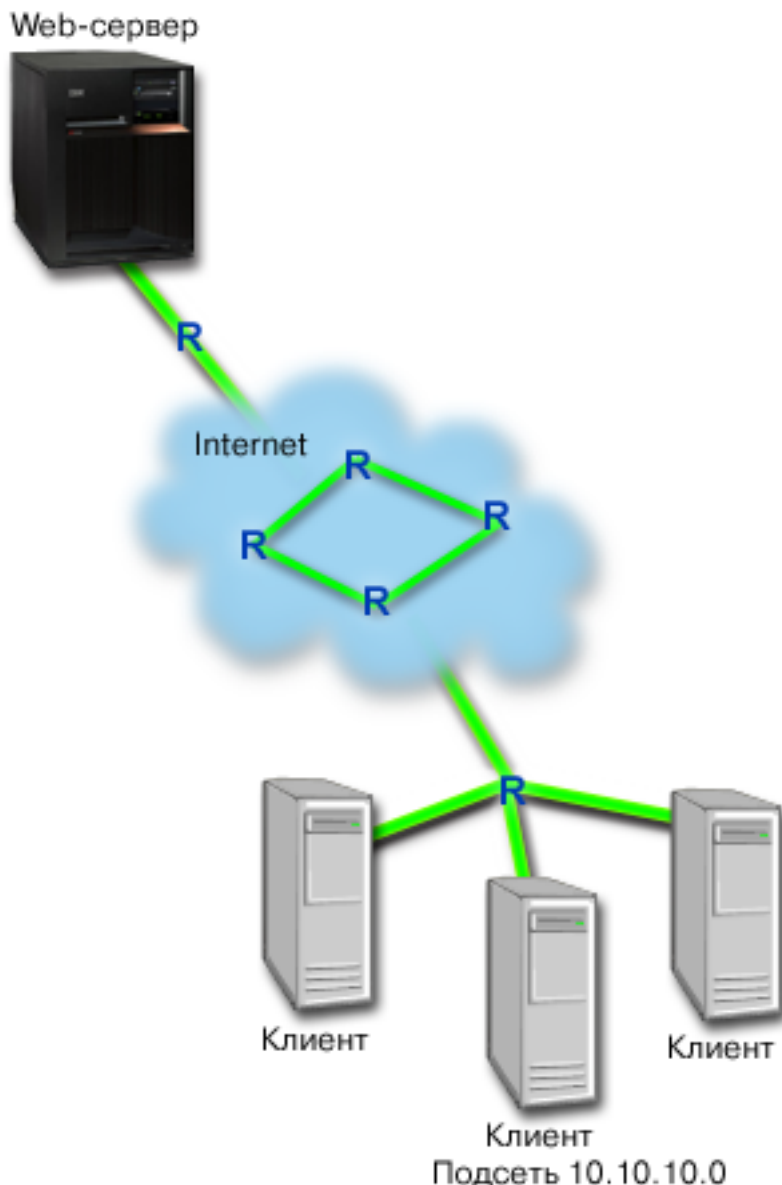
Сценарий QoS: Ограничение потока данных браузера



Ситуация

По пятницам в вашу компанию поступает большой объем данных браузера от группы дизайнеров (UCD). Этот поток мешает работе бухгалтерии, у которой пятница - также весьма загруженный день. Вы решаете ограничить поток данных браузера от группы UCD. На следующем рисунке изображена конфигурация сети для этого сценария. На сервере iSeries установлена OS/400^(R) V5R2.

Рисунок 3. Web-сервер, ограничивающий поток данных браузера для клиента.



Вариант действий

Для ограничения исходящего потока браузера вы можете создать стратегию дифференцированного обслуживания. Стратегия дифференцированного обслуживания разбивает поток на классы. Всему потоку, контролируемому этой стратегией, присваивается некоторый кодовый знак. Этот кодовый знак определяет способ обработки потока на маршрутизаторах. В данном сценарии стратегии присваивается небольшой кодовый знак, что означает низкий приоритет.

Настройка

1. Откройте QoS в Навигаторе.

1. В Навигаторе разверните значок сервера → **Сеть** → **Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
3. Откройте **Стратегии исходящих соединений**.

4. Щелкните правой кнопкой мыши на пункте **DiffServ** и выберите **Создать стратегию**. Будет запущен Мастер создания стратегии DiffServ.

2. Создайте стратегию дифференцированного обслуживания.

Поскольку вы намереваетесь ограничить поток данных браузера для группы дизайнеров (UCD), вы можете назвать стратегию **UCD**. Клиенты применяют адрес подсети **10.10.10.0**. Это вымышленное число, приведенное только для примера. Так как поток данных обычно проходит через порт 80, то приложению можно присвоить имя **port 80**. Далее, так как перегрузка сети возникает только по пятницам, вы можете назначить стратегии расписание с 9 утра до 5 вечера. Расписанию можно присвоить имя **Friday9-5**. Задайте в окнах диалога мастера следующие параметры:

Имя = UCD (можно присвоить любое имя)
Клиент = Subnet 10.10.10.0
Приложение = port 80 (стандартный порт потока HTTP)
Протокол = TCP
Расписание = Fridays9-5

Введите остальную информацию стратегии в окнах мастера Класс обслуживания, который будет автоматически запущен при продолжении процедуры.

Размер набора маркеров = 8 Кбит
Средняя скорость = 10 Мбит/с
Максимальная скорость = 20 Мбит/с
Обработка внепрофильных пакетов = Удалять пакеты (повторно переданные)

Навигатор содержит список всех стратегий дифференцированного обслуживания, созданных на сервере. После того, как вы закончите работу с мастером, стратегия появится в правой панели.

3. Создайте новый класс обслуживания.

При заполнении форм мастера потребуется указать способ обработки на транзитных участках, ограничения производительности и способ обработки внепрофильных потоков данных. Все эти параметры определяются в классе обслуживания.

Класс обслуживания фактически определяет скорость передачи потока данных, обеспечиваемую маршрутизатором. Для этого класса обслуживания можно задать имя **Bronze**, чтобы отразить низкий уровень обслуживания. Навигатор содержит список всех классов обслуживания, определенных на сервере.

Класс обслуживания = Bronze

4. Проверьте работу стратегий с помощью монитора.

Для того чтобы убедиться, что поток данных обрабатывается согласно заданной стратегии, запустите монитор.

1. Выберите одну из папок Стратегии (DiffServ, IntServ, Запросы сервера—>URI или Число соединений).
2. Щелкните правой кнопкой мыши на стратегии, о которой необходимо собрать данные, и выберите пункт **Отслеживать**.

На следующем рисунке изображен вывод монитора с комментариями.

Рисунок 4. Монитор Quality of Service.

Имя стра...	Ограничение средн...	Ограничение ра...	Ограничение пи...	Профильных па...	Профильны...	Внепрофильны...	Активных соедин...
UCD	10240 Кб/с	8	20480 Кб/с	507	392Кб	16Кб	0 объектов

Наиболее интересны поля, в которых указывается собранная информация о потоке данных. Просмотрите значения следующих полей: общее число бит, число профильных бит и число профильных пакетов. Значение в поле Число внепрофильных бит указывает на случаи, когда параметры потока данных превышают значения, определенные в стратегии. В стратегии дифференцированного обслуживания параметр внепрофильных данных указывает число удаляемых бит. Число профильных пакетов указывает, сколько бит было обработано с помощью этой стратегии (начиная с момента отправки пакета и до момента создания данного вывода монитора).

Кроме того, важную роль играет значение, указанное в поле Средняя скорость. При превышении этого ограничения сервер начинает удалять пакеты. В результате, растет число внепрофильных бит. Это означает, что стратегия работает в соответствии с заданными параметрами. Описание всех полей монитора приведено в разделе Монитор.

5. Измените любые значения, не относящиеся к данной стратегии.

Вы можете изменить любые значения стратегии.

1. Закройте монитор.
2. В левой панели выберите Классы обслуживания.
3. В правой панели щелкните правой кнопкой мыши на имени созданного класса обслуживания.
4. Выберите **Свойства**. Появится окно диалога Свойства CoS со значениями, управляющими потоком данных. Измените требуемые значения.



Сценарий QoS: Ограничение числа входящих соединений



Ситуация

Web-сервер перегружен поступающими запросами клиентов. Необходимо снизить скорость потока данных HTTP, поступающих на Web-сервер (10.1.1.4) через локальный интерфейс 10.1.1.1. QoS позволяет на основе атрибутов соединения (например IP-адреса) ограничить число принимаемых запросов. С этой целью вы решили настроить стратегию, ограничивающую число принимаемых запросов на установление соединения.

На рисунке изображены ваша компания и компания-клиент. Данная стратегия QoS управляет потоком данных только в одном направлении.

Рисунок 5. Ограничение числа входящих соединений TCP.



Предварительные требования:

- Работаящий сервер iSeries V5R2
- Настроенный и запущенный сервер LDAP

Вариант действий

Перед настройкой стратегии управления поступающими запросами на установление соединения необходимо решить, следует ли ограничить поток данных в локальный интерфейс или конкретное приложение, либо поток данных от определенного клиента. В данном примере необходимо создать стратегию, ограничивающую число запросов на установление соединения, поступающих от клиента Their_Company через порт 80 (протокол HTTP) локального интерфейса 10.1.1.1. Так как задается ограничение по IP-адресу, то следует создать стратегию числа соединений. Существует два типа стратегий управления входящим потоком данных: стратегии числа соединений и стратегии запросов сервера (URI). Стратегии URI ограничивают число запросов на установление соединения для конкретного относительного URI (это понятие схоже с относительным URL) или всех URL в системе. Дополнительная информация о стратегии URI приведена в разделе Стратегии управления входящим потоком данных.

Для создания этой стратегии числа соединений и завершения сценария откройте окно Навигатора и перейдите к функции QoS.

Настройка

1. Откройте QoS в Навигаторе.
 1. В Навигаторе разверните значок сервера → **Сеть** → **Стратегии IP**.
 2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
 3. Откройте **Стратегии управления входящим потоком данных**.
 4. Щелкните правой кнопкой мыши на пункте **Число соединений** и выберите **Создать стратегию**.
2. Следуйте указаниям мастера создания стратегии числа соединений.

Второй этап - работа с мастером создания стратегии числа соединений. Так как настраивается ограничение для входящего потока данных от клиента Their_Company, то этой стратегии можно присвоить имя **Restrict_TheirCompany**. Необходимо ограничить число запросов, отправляемых по локальному IP-адресу 10.1.1.1 клиентом Their_Company. Это вымышленное число, приведенное только для примера. Так как поток данных проходит через порт 80, то приложению можно присвоить имя **port 80**. Расписанию можно присвоить имя **Weekdays(9-5)**. Задайте в окнах мастера следующие значения параметров:

Имя = Restrict_TheirCompany

Клиент = Their_Company

Приложение = port 80

Локальный IP-адрес = 10.1.1.1

Расписание = Weekdays (9-5)

Среднее число соединений = 100 в секунду

Максимальное число соединений = 5 соединений

Приоритет = Средний

Навигатор содержит список всех стратегий числа соединений, созданных на сервере.

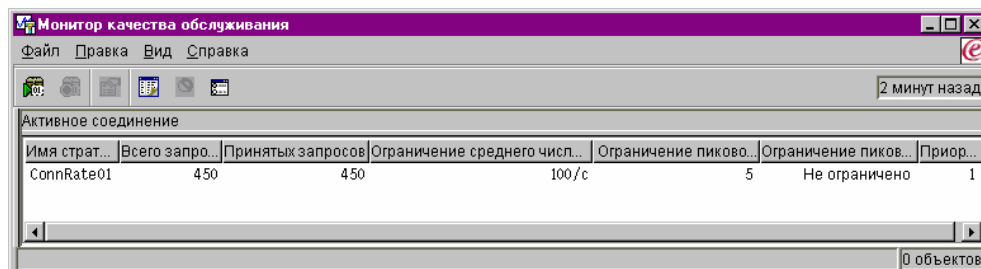
3. Соберите информацию о потоке данных, контролируемом этой стратегией, чтобы убедиться в достижении желаемых результатов.

Для того чтобы убедиться, что поток данных обрабатывается согласно заданной стратегии, запустите монитор.

1. Выберите одну из папок Стратегии (DiffServ, IntServ, Запросы сервера—>URI или Число соединений).
2. Щелкните правой кнопкой мыши на стратегии, о которой необходимо собрать данные, и выберите пункт **Отслеживать**.

На следующем рисунке изображен вывод монитора с комментариями.

Рисунок 6. Монитор Quality of Service.



Выберите все поля со статистическими показателями, такими как число принятых запросов, число отклоненных запросов, общее число запросов и число соединений. Значение в поле Число отклоненных запросов обозначает случаи, когда параметры потока данных превышают значения, определенные в стратегии. Число принятых запросов обозначает число битов, обработанных с помощью этой стратегии (начиная с момента отправки пакета и до момента создания данного вывода монитора).

Кроме того, важную роль играет значение, указанное в поле Среднее число запросов на установление соединения. При превышении этого ограничения сервер начинает удалять пакеты. В результате, растет число отклоненных запросов. Это означает, что стратегия работает в соответствии с заданными параметрами. Описание всех полей монитора приведено в разделе Монитор.

4. При необходимости, измените значения в панели свойств.

Закройте монитор. **Щелкните правой кнопкой** на стратегии Restrict_TheirCompany и выберите пункт **Свойства**. В этих панелях можно изменить свойства стратегии. Здесь же задаются параметры расписания, клиента, приложений и обработки потока данных.



Сценарий QoS: Предсказуемый поток данных B2B

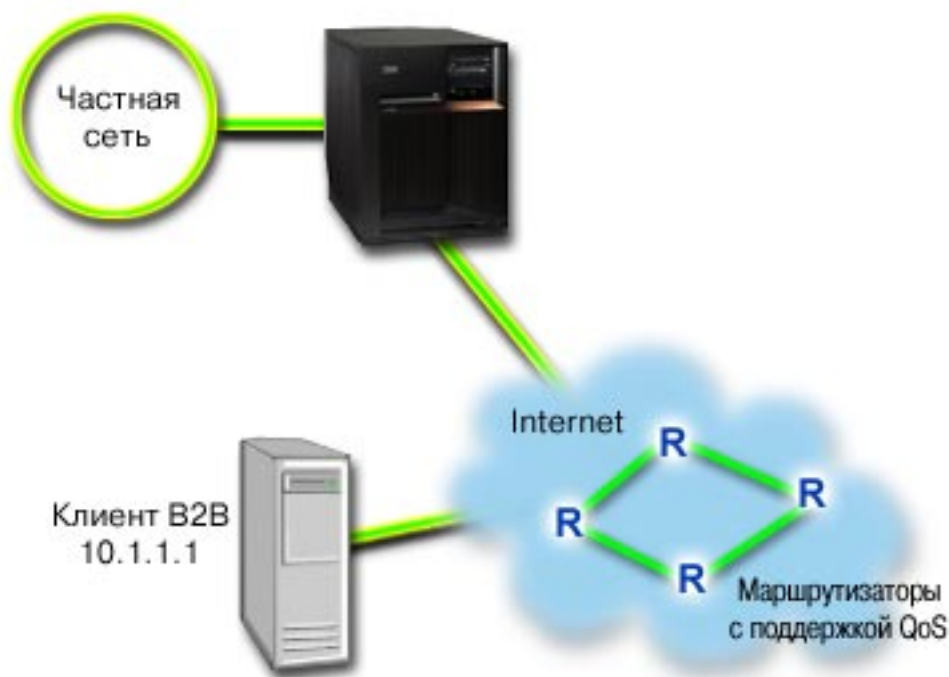


Ситуация

Торговый отдел сообщает о том, что данные по сети передаются не так, как ожидается. Сервер iSeries вашей компании работает в среде деловых приложений (business-to-business - B2B), требующей предсказуемого сетевого обслуживания. Вы должны обеспечить предсказуемость результатов транзакций заказчиков. По этой причине, вы хотите предоставить торговому отделу более высокий уровень обслуживания для их приложения заказов в наиболее загруженное время дня (с 10 утра до 4 вечера).

На приведенном ниже рисунке торговый отдел находится в пределах частной сети. Маршрутизаторы на пути следования потока к клиенту B2B поддерживают RSVP. Каждая буква R обозначает маршрутизатор на пути потока.

Рисунок 7. Стратегия интегрированного обслуживания для клиента B2B, применяющая маршрутизаторы с поддержкой RSVP.



Вариант действий

Служба управляемой нагрузки обеспечивает работу приложений, высокочувствительных к перегруженности сети, однако допускающих небольшие потери и задержки данных. Если приложение применяет службу управляемой нагрузки, то его производительность не будет падать при увеличении нагрузки на сеть. Для потока данных обеспечивается уровень обслуживания, сходный с уровнем обслуживания в сети при низкой нагрузке. Поскольку для рассматриваемого приложения допускаются небольшие задержки, вы решаете воспользоваться стратегией интегрированного обслуживания, применяющей службу управляемой нагрузки.

Для применения стратегий интегрированного обслуживания необходимы приложения с поддержкой RSVP. Поскольку на сервере нет приложений, поддерживающих RSVP, вам придется создать их самостоятельно. Для создания приложений воспользуйтесь API Протокол настройки резервирования ресурсов (RAPI) или API сокетов QoS (qtq).

Кроме того, для применения стратегий интегрированного обслуживания необходимо, чтобы на всем пути следования данных маршрутизаторы поддерживали RSVP. Более подробная информация приведена в разделе Интегрированные службы.

Настройка

1. Откройте QoS в Навигаторе.

1. В Навигаторе разверните значок сервера —> **Сеть** —> **Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
3. Откройте **Стратегии исходящих соединений**.
4. Щелкните правой кнопкой мыши на пункте **IntServ** и выберите **Создать стратегию**. Будет запущен Мастер создания стратегии IntServ.

2. Создайте стратегию интегрированного обслуживания.

Так как вы хотите обеспечить предсказуемый поток для заказчиков, вы можете назвать стратегию **B2B_CL**. Клиент получает транзакцию по IP-адресу **10.1.1.1**. Это вымышленное число, приведенное только для примера. Так как поток данных проходит через различные порты с номерами от 7000 до 8000, то приложению можно присвоить имя **port 7000-8000**. Поскольку транзакция происходит в период с 10 утра до 4 дня, расписание можно назвать **Primetime**. Задайте в окнах диалога мастера следующие параметры:

Имя = B2B_CL
Клиент = 10.1.1.1
Приложение = port 7000-8000
Протокол = TCP
Расписание = Primetime
Размер набора маркеров = 8 Кбит
Скорость = 25 Мбит/с
Размер набора маркеров (r) = 75 Кбит
Число потоков = 5

Навигатор содержит список всех стратегий интегрированного обслуживания, созданных на сервере.

3. Проверьте работу стратегий с помощью монитора.

Для того чтобы убедиться, что стратегия работает правильно, запустите монитор.

1. Выберите одну из папок Стратегии (DiffServ, IntServ, Запросы сервера—>URI или Число соединений).
2. Щелкните правой кнопкой мыши на стратегии, о которой необходимо собрать данные, и выберите пункт **Отслеживать**.

На следующем рисунке изображен вывод монитора с комментариями.

Рисунок 8. Монитор Quality of Service.

Имя стра...	Прото...	Диапазон целе...	Ограничение сре...	Ограничение...	Ограничени...	Всего пак...	Всего бит	Несоответ...
B2B_CL	TCP	190.86.23.1	25 Мб/с	8	76800 Мб/с	2045	16753 Кб	

Наиболее интересны поля, в которых указывается собранная информация о потоке данных. К ним относятся поля общего числа битов, числа профильных битов и числа профильных пакетов. Поле профильных битов указывает на остальную часть потока, задерживаемую или удаляемую для обеспечения требований стратегии интегрированного обслуживания. Полное описание полей монитора приведено в разделе **Монитор**.

4. При необходимости скорректируйте значения.

После того, как вы создали стратегию с помощью монитора, вы можете изменить ее значения.

1. Закройте монитор.
2. Щелкните правой кнопкой мыши на имени созданной стратегии.
3. Выберите пункт **Свойства**. Будет показано окно диалога **Свойства B2B_CL**.
4. Выберите вкладку **Управление потоком** для изменения значений, контролирующих поток.

Здесь же задаются параметры расписания, клиента, приложений и обработки потока данных.



Сценарий QoS: Защита и предсказуемость (VPN и QoS)



Ситуация

Соединение с деловым партнером вашей компании установлено через виртуальную частную сеть (VPN). Вы хотите совместить VPN и QoS с целью обеспечить защищенную и предсказуемую передачу важных данных. Конфигурация QoS действует только в одном направлении. По этой причине, в случае аудио- или видеоприложения вам необходимо настроить QoS для приложения на обоих концах соединения.

На рисунке показано соединение VPN между хостами сервера и клиента. Каждая буква R обозначает маршрутизатор, поддерживающий дифференцированные службы, на пути следования потока. Вы видите, что стратегии QoS действуют только в одном направлении.

Рисунок 9. Соединение VPN между хостами, использующее стратегию дифференцированного обслуживания QoS.



Вариант действий

С помощью VPN и QoS вы установите не только защиту, но и приоритет для данного соединения. Прежде всего, вы должны настроить соединение VPN между хостами. Пример см. в разделе Соединение VPN между хостами. После настройки соединения VPN вы можете приступить к созданию стратегии QoS. Создайте стратегию дифференцированного обслуживания. В данном сценарии стратегии присваивается большой кодовый знак, что означает высокий приоритет потока и ускоренную доставку.

Настройка

1. Настройте соединение VPN между хостами. Пример см. в разделе Соединение VPN между хостами.
2. Откройте QoS в Навигаторе.
 1. В Навигаторе разверните значок сервера —> **Сеть** —> **Стратегии IP**.
 2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
 3. Откройте **Исходящие стратегии**.

- Щелкните правой кнопкой мыши на пункте **DiffServ** и выберите **Создать стратегию**. Будет запущен Мастер создания стратегии DiffServ.

3. Создайте стратегию дифференцированного обслуживания.

Так как вы хотите повысить производительность приложений B2B, то этой стратегии можно присвоить имя **B2B**. Клиенты применяют адрес **192.83.63.1**. Это вымышленное число, приведенное только для примера. Поскольку поток B2B может передаваться через любой порт, приложение можно назвать **All ports**. Далее, так как перегрузка сети возникает только с 9 утра до 5 вечера, вы можете назначить стратегии расписание 9-5. Его можно назвать **Firstshift**. Задайте в окнах диалога мастера следующие параметры:

Имя = B2B
Клиент = VPNCient
Приложение = All port
Протокол = All
Расписание = Firstshift

Введите остальную информацию стратегии в окнах мастера Класс обслуживания, который будет автоматически запущен при продолжении процедуры.

Размер набора маркеров = 8 Кбит
Средняя скорость = 90 Мбит/с
Максимальная скорость = Не ограничена
Обработка внепрофильных пакетов = Удалять пакеты (повторно переданные)

Навигатор содержит список всех стратегий дифференцированного обслуживания, созданных на сервере.

4. Создайте новый класс обслуживания.

При заполнении форм мастера потребуется задать класс обслуживания. Класс обслуживания определяет ограничения производительности, кодовые знаки и способ обработки внепрофильных пакетов. В рассматриваемой стратегии вы должны выбрать кодовый знак, соответствующий высокому приоритету и ускоренной доставке. По этой причине, класс обслуживания можно назвать **EF_VPN** (expedited forwarding - ускоренная доставка).

Класс обслуживания = EF_VPN

6. Проверьте работу стратегий с помощью монитора.

Для того чтобы убедиться, что поток данных обрабатывается согласно заданной стратегии, запустите монитор.

- Выберите одну из папок Стратегии (DiffServ, IntServ, Запросы сервера—>URI или Число соединений).
- Щелкните правой кнопкой мыши на стратегии, о которой необходимо собрать данные, и выберите пункт **Отслеживать**.

На следующем рисунке изображен вывод монитора с комментариями.

Рисунок 10. Монитор Quality of Service.

Имя стра...	Ограничение средн...	Ограничение ра...	Ограничение пи...	Профильных па...	Профильны...	Внепрофильны...	Активных соедин...
QoS_VPN	10240 Кб/с	8	20480 Кб/с	507	384 Кб	16 Кб	

Как и в примере 1, наиболее интересны поля, в которых указывается собранная информация о потоке данных. К ним относятся поля общего числа битов, числа профильных битов и числа профильных пакетов. Значение в поле Число внепрофильных бит указывает на случаи, когда параметры потока данных превышают значения, определенные в стратегии. Значение в поле Число профильных пакетов указывает, сколько пакетов контролируется данной стратегией. Важную роль играет значение, заданное в поле Средняя скорость. При превышении этого ограничения сервер начинает удалять пакеты. В результате, растет число профильных битов. Различие между рассматриваемой стратегией и стратегией из примера 1 заключается в том, что в данном случае пакеты защищены посредством VPN. Вы видите, что стратегия QoS совместима с соединением VPN. Описание всех полей монитора приведено в разделе Монитор.

5. При необходимости скорректируйте значения.

Вы также можете изменить параметры созданного класса обслуживания.

1. Закройте монитор.
2. В левой панели выберите **Классы обслуживания**.
3. В правой панели щелкните правой кнопкой мыши на имени созданного класса обслуживания.
4. Выберите **Свойства**. Появится окно диалога Свойства CoS со значениями, управляющими потоком данных. Измените требуемые значения.



Принципы QoS



Существует множество источников информации о функции Quality of service (QoS), поэтому данный раздел содержит только основные сведения, непосредственно связанные с сервером iSeries.

Важнейшим элементом концепции Quality of service является сам сервер. Для успешной реализации этой функции необходимо иметь представление не только об описанных ниже понятиях, но о той роли, которую играет сервер. Сервер iSeries может выступать только в качестве клиента или сервера, но не маршрутизатора. Этот момент следует учитывать при планировании Quality of service.

Реализация QoS предполагает создание стратегий для потоков данных. Стратегией называется набор правил, описывающих различные действия. Обычно эти правила описывают уровень обслуживания, предназначенное для определенных клиентов, приложений и расписаний. Возможно создание стратегий четырех типов. Все стратегии подразделяются на две основных категории: пропускной способности исходящего потока и управления доступом входящего потока. Стратегии исходящих соединений делятся на два типа обслуживания: стратегию интегрированного обслуживания и стратегию дифференцированного обслуживания. Стратегии входящих соединений также подразделяются на два типа обслуживания: стратегии числа запросов на установление соединений и стратегии числа запросов URI.

Входящими называют стратегии, которые управляют соединениями, установленными с вашей сетью из другой сети. Стратегии исходящих соединений устанавливают ограничения или улучшают передачу потока данных, направленного из вашей сети. Тип применяемой стратегии определяется целями использования QoS. Информация о ситуациях, в которых применяется тот или иной тип стратегии, приведена ниже.

Дополнительная информация приведена в следующих разделах:

Дифференцированные службы

Это первый тип исходящей стратегии, которую можно создать на сервере. Дифференцированные службы подразделяют потоки данных на классы. Для реализации функции Quality of service в сети необходимо определить классификацию потоков данных и способы обработки для каждого из классов. После этого можно создать классы обслуживания, применяемые стратегией дифференцированных служб.

Дифференцированные классы обслуживания

В этом разделе описаны элементы класса обслуживания. Создание стратегии дифференцированных служб предполагает также создание класса обслуживания.

Интегрированные службы

Второй тип исходящей стратегии - стратегия интегрированного обслуживания. Интегрированные службы позволяют приложениям IP запрашивать и резервировать пропускную способность с помощью протокола RSVP. С помощью этого протокола интегрированные службы гарантируют доставку данных из одной точки в другую. Это самый высокий и самый сложный уровень обслуживания. При создании стратегии интегрированного обслуживания необходимо задать один из классов обслуживания: гарантированное обслуживание или управляемую нагрузку.

Интегрированные службы с применением кодовых знаков дифференцированных служб

Этот тип стратегии интегрированных служб применяется в смешанной сетевой среде. В смешанной сетевой среде не все узлы поддерживают протокол RSVP.

Протокол RSVP и API QoS

В этом разделе описан протокол и API, применяемые для резервирования ресурсов интегрированными службами. Здесь приведена информация о функциях, которые должен поддерживать маршрутизатор для работы с протоколом RSVP.

Число соединений

Этот тип входящей стратегии применяется для управления потоками данных, запрашивающими предоставления доступа в сеть (по IP-адресу). Существует два типа стратегий управления входящим потоком данных: числа соединений и URI. Этот раздел содержит описание входящих стратегий обоих типов.

URI

Этот тип входящей стратегии применяется для управления потоками данных, запрашивающими предоставления доступа в сеть (по URI). Существует два типа стратегий управления входящим потоком данных: числа соединений и URI. Этот раздел содержит описание входящих стратегий обоих типов.

Сервер каталогов

Стратегии QoS теперь экспортируются на сервер каталогов. Этот раздел содержит информацию о преимуществах применения сервера каталогов, принципах и настройке LDAP, а также о схеме QoS.

Перед настройкой QoS, необходимо тщательно изучить информацию об этой службе и убедиться, что она позволяет решить поставленные задачи. Ссылки на дополнительные источники информации приведены в разделе информация, связанная с QoS.



Количество запросов на установление соединений и количество запросов URI

» Стратегии входящих соединений предназначены для управления потоком данных, поступающих на сервер. Существует два типа стратегий, с помощью которых можно настроить параметры регулирования входящих потоков данных: стратегии URI и стратегии количества соединений. Ниже приведено описание этих типов стратегий.

Стратегии количества запросов URI

Стратегии количества запросов URI - это составная часть комплекса мер, предназначенных для защиты сервера от перегрузок. В стратегиях этого типа контроль доступа, за счет которого ограничивается количество запросов URI, принимаемых сервером, основан на информации уровня приложений. Другое название такого способа - *контроль запросов на соединение на основе заголовков*. Для установки приоритетов в нем используются URI.

По сравнению со стратегиями количества соединений, стратегии URI обеспечивают более тщательный контроль, поскольку проверяют не только заголовки, но и содержимое пакетов. Такое содержимое может включать имя URI и другую информацию, связанную с приложением. В iSeries стратегия определяется с помощью относительного имени URI. Например, `/products/clothing`. Ниже приведены примеры относительных URI.

Относительный URI

Относительный URI - это часть абсолютного URI (аналогичного прежнему абсолютному URL). Рассмотрим в качестве примера адрес `http://www.ibm.com/software`. Адрес `http://www.ibm.com/software` - это абсолютный URI. Часть адреса `/software` - это относительный URI. Относительный URI должен начинаться с одинарной косой черты (`/`). Ниже приведены примеры относительных URI:

- `/market/grocery#D5`
- `/software`
- `/market/grocery?q=green`

Примечание: Протокол, имя хоста и номер порта по умолчанию наследуются из параметров сервера HTTP. Кроме того, в относительный URI неявно добавляется символ подстановки. Например, значение `/software` задает любой объект, находящийся в каталоге `software`.

Стратегии URI считаются входящими стратегиями, так как они контролируют запросы входящего потока данных. Частью этого контроля является указание приоритетов обработки запросов URI после того, как они были приняты стратегией. Присваивая приоритеты стратегиям, вы фактически создаете очередь входящих запросов, основанную на приоритетах для каждого соединения.

Стратегии количества соединений

Стратегии количества соединений также предназначены для защиты сервера от перегрузок. В стратегиях этого типа контроль доступа, за счет которого ограничивается количество запросов на соединение, принимаемых сервером, основан на информации уровня соединений. Другое название такого способа - *стратегия TCP SYN*.

Стратегии количества соединений принимают или отклоняют поступающие запросы на основе определенного в стратегии среднего числа соединений, устанавливаемых в секунду, и максимального числа одновременно существующих соединений. Среднее число соединений и максимальное число соединений можно задать с помощью мастера в Навигаторе. Когда запросы на соединение поступают на сервер, он анализирует информацию в заголовке пакета и сравнивает полученные данные с данными стратегии. Затем система сравнивает полученную информацию с параметром числа соединений. Если стратегия разрешает прием данного пакета, он помещается в очередь. В противном случае пакет отбрасывается.

Как и стратегии URI, стратегии количества соединений считаются входящими стратегиями, так как они контролируют число входящих соединений. Частью этого контроля является указание приоритетов обработки соединений после того, как они были приняты стратегией. Присваивая приоритеты стратегиям, вы фактически создаете очередь входящих запросов, основанную на приоритетах для каждого соединения.

Как в стратегиях URI, так и в стратегиях количества соединений необходимо задавать ограничения на среднее и максимальное число соединений для потоков данных, определенных в каждой из стратегий. Эти ограничения позволяют контролировать число соединений, устанавливаемых с сервером. Среднее число соединений ограничивает количество соединений, устанавливаемых за единицу времени, либо количество запросов URI, принимаемых за единицу времени. <<

Ограничения на среднее и максимальное число соединений

➤ Ограничения на среднее и максимальное число соединений называются ограничениями скорости. Эти ограничения позволяют контролировать число соединений, устанавливаемых с сервером. Ограничения скорости задаются во всех входящих стратегиях, т.е. стратегиях URI и стратегиях количества соединений.

Ограничение на максимальное число соединений

Ограничение на максимальное число соединений определяет размер буфера, в котором хранятся запросы на соединения. Запросы на соединения могут поступать настолько часто, что сервер не будет успевать их обрабатывать или их число превысит допустимое значение. Когда число соединений с сервером достигнет установленного ограничения, все дополнительные запросы на соединения будут отклоняться.

Ограничение на среднее число соединений

Это значение ограничивает количество соединений, устанавливаемых за единицу времени, либо количество запросов URI, принимаемых за единицу времени. Если при получении запроса будет обнаружено, что установленное ограничение уже достигнуто, сервер отклонит запрос. Среднее число запросов на соединения измеряется числом соединений в секунду.

Совет: Для определения необходимых ограничений рекомендуется запустить монитор. Пример стратегии, позволяющей собрать информацию о большинстве потоков данных на сервере, приведен в разделе Сбор текущих статистических показателей сети. На основе полученных результатов можно настроить необходимые ограничения. <<

Дифференцированные службы

Дифференцированные службы разбивают поток на классы. Для того чтобы применять функцию Quality of Service в сети, вы должны определить, каким образом следует классифицировать данные сетевого потока и обрабатывать различные классы.

Уровень обслуживания пакета IP определяется сервером по битам в заголовке IP пакета. Маршрутизаторы и коммутаторы выделяют свои ресурсы в зависимости от способа обработки на транзитных участках (PHB), указанного в поле TOS заголовка IP. Поле TOS было переопределено в RFC 1349 и OS/400^(R) V5R1. PHB - это тип пересылки пакета на промежуточном узле. Он обозначается шестнадцатеричным числом - кодовым знаком. Пакетам могут быть присвоены кодовые знаки как на сервере, так и на других узлах сети, например на маршрутизаторе. Для того чтобы пакет мог получить запрошенное обслуживание, каждый узел сети должен поддерживать дифференцированные службы. Иными словами, сетевое оборудование должно обеспечивать заданные способы обработки на транзитных участках. Для реализации PHB необходимо, чтобы сетевой узел поддерживал управление очередями и приоритетами пакетов. Дополнительная информация о поддержке дифференцированных служб приведена в разделе Обработчики потоков данных.

Если пакет проходит через маршрутизатор или коммутатор, не поддерживающий дифференцированные службы, то он теряет свой уровень обслуживания. Заметьте, что пакет по-прежнему будет обрабатываться, однако по-другому. На сервере iSeries вы можете воспользоваться стандартными кодовыми знаками PNB или определить свой собственный класс. Не рекомендуется создавать собственные кодовые знаки для применения за пределами частной сети.

В отличие от интегрированных служб, в дифференцированных службах отсутствуют резервирование и различная обработка пакетов в зависимости от их типа. Все пакеты, относящиеся к одному и тому же классу, обрабатываются одинаково.

Дифференцированные службы также применяются для управления входящими и исходящими потоками сервера. Это означает, что с помощью дифференцированных служб сервер iSeries ограничивает производительность. Ограничение ресурсов, выделяемых менее важному приложению, позволяет более важному приложению быстрее завершить работу в сети. При создании стратегии вы задаете различные ограничения на сервере. К ограничениям производительности относятся размер набора маркеров, максимальное число соединений и среднее число соединений. Более подробная информация об этих ограничениях приведена в справке по функции QoS в Навигаторе.

Эту информацию можно считать введением в тему "Дифференцированные службы". Присвоение кодовых знаков рассмотрено в разделе Кодовые знаки и способы обработки на транзитных участках. Если после прочтения этого раздела вы по-прежнему испытываете затруднения в выборе кодовых знаков, попробуйте подобрать их опытным путем. Создайте пробные стратегии, включите их отслеживание и корректируйте стратегии на основе получаемых результатов.

Дифференцированные классы обслуживания

В разделе, посвященном дифференцированному обслуживанию, рассмотрено разбиение потока данных на классы, выполняемое функциями дифференцированного обслуживания. Большая часть этих операций выполняется аппаратно, однако общее управление распределением потока по классам и присвоение приоритетов осуществляется пользователем.

Если вы решили применять QoS, то прежде всего вы должны создать стратегии. Стратегии определяют все операции, выполняемые в рамках QoS. Затем вы должны присвоить выбранной стратегии класс обслуживания. Классы обслуживания определяются отдельно и могут использоваться стратегиями повторно. Класс обслуживания состоит из способа обработки на транзитных участках, ограничений на параметры потока и способа обработки непрофильных пакетов.

Обработка на транзитных участках

Функция Quality of Service присваивает потоку способы обработки на транзитных участках с помощью рекомендуемых кодовых знаков. На основе этих кодовых знаков маршрутизаторы и коммутаторы устанавливают приоритеты потоков. Серверу эти кодовые знаки недоступны, поскольку он не выполняет функции маршрутизатора. Вы должны выбрать набор кодовых знаков в зависимости от потребностей конкретной сети. Вы должны определить, какие приложения наиболее важны и каким стратегиям следует присвоить более высокий приоритет. Самое важное - быть последовательным в выборе кодовых знаков и реализации выбранной стратегии. Только в этом случае можно добиться желаемого результата. Кодовые знаки играют первостепенную роль в распределении данных по различным классам обслуживания.

Ограничения производительности

Функция Quality of Service контролирует потоки в сети с помощью ограничений производительности. Это размер набора маркеров, максимальное число соединений и среднее число соединений. Более подробная информация об этих параметрах приведена в разделе Ограничения на набор маркеров и пропускную способность.

Обработка внепрофильных пакетов

Последний компонент класса обслуживания - способ обработки внепрофильных пакетов. При настройке ограничений производительности вы задаете параметры, ограничивающие те или иные характеристики потока. В случае превышения этих ограничений пакеты считаются внепрофильными. Способ обработки внепрофильных пакетов указывает, что нужно сделать с этими пакетами: удалить, задержать или передать далее. Если вы решите удалить внепрофильные пакеты, то они будут передаваться повторно через указанное время. Если вы решите задерживать внепрофильные пакеты, то они будут переформатироваться в соответствии с заданными характеристиками. Если вы решите пометить внепрофильные пакеты кодовыми знаками дифференцированных служб (DSCP), то им будут присваиваться новые кодовые знаки. Когда во время работы с мастером вы указываете эти инструкции по обработке, вы можете нажать кнопку Справка и просмотреть дополнительную информацию.

Кодовые знаки и обработка на транзитных участках

Ниже перечислены рекомендуемые кодовые знаки, применяемые функцией Quality of Service для присвоения способа обработки на транзитном участке потоку данных. Вы должны выбрать набор кодовых знаков в зависимости потребностей конкретной сети. Решение о целесообразности использования того или иного набора кодовых знаков может быть принято только вами. Вы должны определить, какие приложения наиболее важны и каким стратегиям следует присвоить более высокий приоритет. Самое важное - быть последовательным в выборе кодовых знаков и реализации выбранной стратегии. Только в этом случае можно добиться желаемого результата.

Приведенная ниже таблица содержит рекомендуемые кодовые знаки. Вы можете также создать свои собственные способы обработки на транзитных участках.

Ускоренная доставка (См. 22)	Селектор класса (См. 23)	Надежная доставка (См. 23)
101110	Класс 0 - 000000	Надежная доставка, Класс 1, Низкий - 001010
	Класс 1 - 001000	Надежная доставка, Класс 1, Средний - 001100
	Класс 2 - 010000	Надежная доставка, Класс 1, Высокий - 001110
	Класс 3 - 011000	Надежная доставка, Класс 2, Низкий - 010010
	Класс 4 - 100000	Надежная доставка, Класс 2, Средний - 010100
	Класс 5 - 101000	Надежная доставка, Класс 2, Высокий - 010110
	Класс 6 - 110000	Надежная доставка, Класс 3, Низкий - 011010
	Класс 7 - 111000	Надежная доставка, Класс 3, Низкий - 011100
		Надежная доставка, Класс 3, Высокий - 011110
		Надежная доставка, Класс 4, Низкий - 100010
		Надежная доставка, Класс 4, Средний - 100100
		Надежная доставка, Класс 4, Высокий - 100110

Ускоренная доставка

Ускоренная доставка - один из способов обработки на транзитных участках, применяемых дифференцированными службами. Главным образом, этот способ применяется для обеспечения гарантированного обслуживания в сети. При ускоренной доставке резервируется пропускная способность сетевых каналов и за счет этого обеспечивается передача потока данных между конечными узлами с низкой долей потерь и низкими помехами. Пропускная способность резервируется перед отправкой пакета. Главная цель - отсутствие задержек и своевременная доставка пакета.

Примечание: Это достаточно дорогостоящий вид обслуживания, поэтому применять его постоянно не рекомендуется.

Селектор класса

Кодовые знаки селектора классов являются еще одним типом обработки, применяемым дифференцированными службами. Существует 7 классов. Класс 0 присваивает пакетам самый низкий приоритет, а Класс 7 - самый высокий приоритет среди значений кодовых знаков селектора классов. Эта группа способов обработки на транзитных участках является самой распространенной, поскольку к настоящему времени большинство маршрутизаторов уже применяет схожие кодовые знаки.

Надежная доставка

Надежная доставка подразделяется на четыре класса обработки на транзитных участках, в каждом из которых возможен низкий, средний или высокий приоритет удаления пакетов. Приоритет удаления определяет вероятность удаления пакетов данного класса. Для каждого класса существуют собственные ограничения пропускной способности. Класс 1, Высокий присваивает стратегии самый низкий приоритет, а Класс 4, Низкий - самый высокий. Низкий приоритет удаления означает, что пакеты в данной стратегии будут удалены в данном классе с наименьшей вероятностью.

Обработчики потоков данных

Для применения стратегий Quality of Service сетевое оборудование должно поддерживать QoS. Это означает, что в сетевом оборудовании - маршрутизаторах, коммутаторах и пр. - должны поддерживаться функции классификации, измерения, маркировки, формирования и удаления пакетов. Эти функции называются *обработчиками потоков данных*. Если в сетевом оборудовании есть все обработчики потоков данных, то говорят, что оно поддерживает QoS.

Логическая схема функционирования обработчиков потоков данных приведена на следующем рисунке.

Рисунок 11. Обработчики потоков данных



Ниже приведено подробное описание каждого обработчика потоков данных.

Функция классификации

Функция классификации выбирает пакеты из потока на основе содержимого их заголовков. На сервере iSeries определено два типа классификаторов. Функция BA (Behavior aggregate) классифицирует пакеты исключительно по их кодовым знакам дифференцированных служб. Функция MF (Multi-field) отбирает пакеты на основе значений одного или нескольких полей заголовка, например, адреса отправителя, адреса получателя, поля дифференцированных служб, ИД протокола, порта отправителя и порта получателя.

Функция измерения

Функция измерения определяет, соответствуют ли пакеты IP, пересылаемые классификатором, профайлу заголовков IP потока. Соответствие проверяется согласно стратегии QoS для этого потока. Измеритель передает информацию другим обработчикам для выполнения действия. Действие выполняется для каждого пакета, как профильного, так и внепрофильного.

Функция маркировки

Функция маркировки задает значение поля дифференцированных служб (DS). Она преобразует кодовый знак дифференцированных служб в набор байтов. Маркировщик может пометить все пакеты одним кодовым знаком, либо набором кодовых знаков (последние определяют способ обработки на транзитных участках).

Функция формирования

Функция формирования задерживает некоторые (или даже все) пакеты потока с целью привести поток в соответствие с его профайлом. Размер буфера формирователя ограничен, и задержанные пакеты могут быть отброшены, если они не умещаются в буфере.

Функция удаления

Функция удаления отбрасывает некоторые (или даже все) пакеты потока. Это позволяет привести поток в соответствие с его профайлом.

Принципы работы сервера каталогов

» Конфигурации стратегий QoS хранятся на сервере каталогов LDAP. При работе с сервером LDAP следует применять последнюю версию протокола LDAP - версию 3.

Преимущества применения сервера каталогов

Применение сервера каталогов упрощает работу с QoS. Вместо того чтобы настраивать стратегии QoS на каждом сервере, вы можете сохранить данные конфигурации на локальном сервере каталогов, сделав их доступными для всех систем. Однако совместное использование данных необязательно. Существует два других способа применения сервера каталогов с функциями QoS.

1. Настройку, хранение и использование данных может выполнять только одна система.
2. Данные конфигурации можно разместить на сервере каталогов, содержащем данные других систем. При этом данные не обязательно будут использоваться этими системами. Таким образом, данные для нескольких систем и их резервная копия могут храниться на одном сервере.

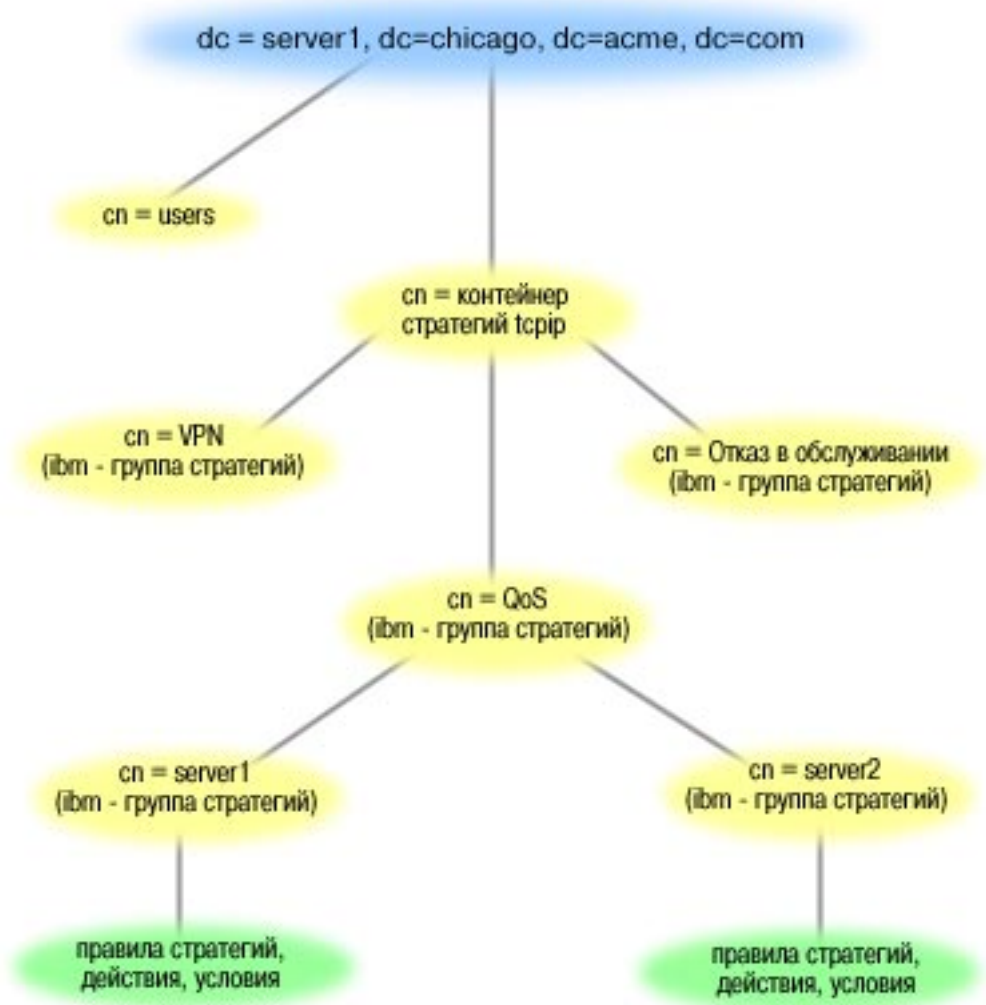
Ресурсы LDAP

Перед тем, как приступить к применению QoS, необходимо ознакомиться с принципами работы LDAP и структурами каталогов. Обратитесь к разделу Базовые понятия LDAP в категории Службы каталогов (LDAP) iSeries Information Center.

Иерархическая структура QoS

Если вы хотите работать с каким-либо подкаталогом, вы должны указать **Отличительное имя (DN)** или (по выбору) ключевое слово. Отличительное имя задается при настройке сервера каталогов. Как правило, оно состоит из имени самой записи, а также вышестоящих объектов в иерархической структуре каталога. Серверу доступны все объекты каталога ниже указанного DN. Например, предположим, что сервер LDAP содержит каталог следующей структуры:

Рисунок 12. Пример каталога QoS



Объект Server1 вверху (dc=server1,dc=chicago,dc=acme,dc=com) - это система, в которой находится сервер каталогов. Другие объекты, такие как стратегии cn=QoS и cn=tcpip, представляют другие серверы QoS. Таким образом, на сервере cn=server1 DN по умолчанию будет cn=server1,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com. На сервере cn=server2 DN по умолчанию будет cn=server2,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com.

При работе с каталогом важно указывать правильный сервер в DN, например cn или dc. Будьте внимательны при изменении DN, так как эта строка обычно не умещается на экране полностью. Информация о настройке сервера каталогов Quality of Service в Навигаторе приведена в разделе Настройка сервера каталогов.

Ссылки на дополнительные источники информации о LDAP приведены в разделе Связанная информация по QoS. <<

Ключевые слова



В процессе настройки сервера каталогов вы должны будете решить, следует ли связать ключевые слова с различными конфигурациями QoS. Поля ключевых слов заполнять необязательно. Далее приведена информация о ключевых словах и способах их применения.

Мастер создания конфигурации Quality of Service настраивает сервер каталогов. В процессе настройки необходимо указать, является ли настраиваемый сервер основным сервером каталогов или вспомогательной системой. Сервер, применяемый для обслуживания всех стратегий QoS, называется основной системой.

Ключевые слова служат для идентификации конфигураций, созданных основным сервером. Хотя ключевые слова создаются в основной системе, они применяются вспомогательными системами. С их помощью вспомогательные системы загружают конфигурации, созданные основной системой. Ниже приведено более подробное описание ключевых слов и их применения в различных системах.

Ключевые слова и основные системы

Ключевые слова, связанные с конфигурациями QoS, создаются и обслуживаются основной системой. Они служат для идентификации конфигураций, созданных основной системой, во вспомогательных системах.

Ключевые слова и вспомогательные системы

Ключевые слова упрощают поиск конфигураций во вспомогательных системах. Вспомогательная система загружает и применяет конфигурации, созданные основной системой. Ключевые слова можно выбрать при настройке вспомогательной системы. Вспомогательная система будет загружать все конфигурации, связанные с выбранными ключевыми словами. Применение ключевых слов позволяет вспомогательной системе загружать конфигурации, созданные различными основными системами.

При настройке сервера каталогов с помощью Навигатора более подробные инструкции можно найти в справке по выполнению задач QoS.



Интегрированные службы

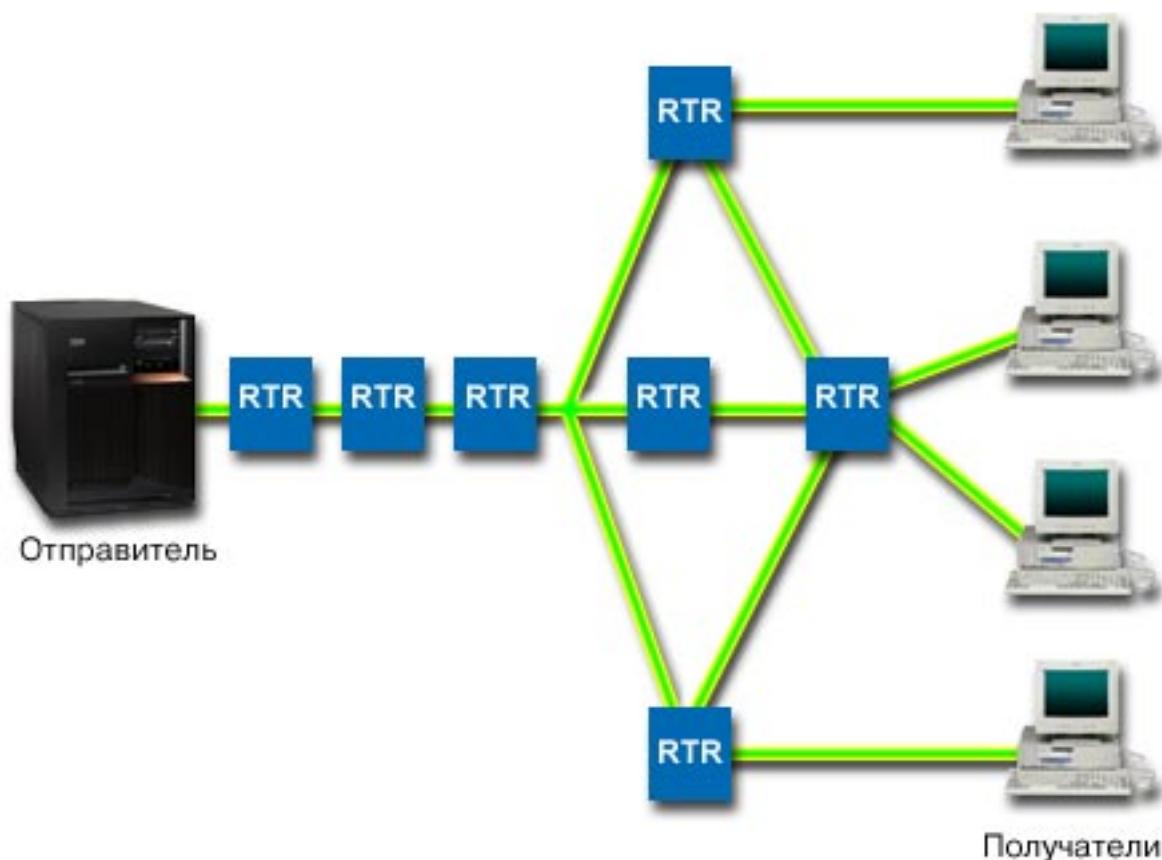
Интегрированные службы отвечают за длительность доставки данных и присвоение специальных инструкций по обработке отдельным потокам данных. Помните, что слишком часто прибегать к помощи интегрированных служб не рекомендуется, поскольку стоимость гарантированного обслуживания данных остается достаточно высокой. Вместе с тем, резервирование излишних ресурсов может обернуться еще большими издержками.

» До того, как начнется отправка данных, интегрированные службы резервируют ресурсы для определенной стратегии. Перед отправкой данных маршрутизаторы получают сигнал, и сеть принимает запрос и обеспечивает передачу данных из одной точки в другую согласно стратегии. **Стратегией** называется набор правил, описывающих различные действия. В принципе, это список управления доступом. При резервировании клиент отправляет запрос на предоставление требуемой пропускной способности. Если все маршрутизаторы, через которые проходит поток данных, примут требования, указанные в запросе клиента, то этот запрос поступит на сервер и в стратегию интегрированных служб. Если запрос отвечает ограничениям, определенным в стратегии, то сервер QoS разрешит установить соединение RSVP и зарезервирует заданную пропускную способность для приложения. Резервирование выполняется с помощью протокола резервирования ресурсов (RSVP) и API RAPI и/или API сокетов QoS. Дополнительная информация приведена в разделе Протокол RSVP и API QoS. «

Все узлы, через которые проходит поток данных, должны поддерживать протокол RSVP. Маршрутизаторы обеспечивают обслуживание с помощью функций управления потоком данных: планировщика пакетов, классификатора пакетов и функций управления доступом. Поддержка этих

функций управления потоком данных часто называется поддержкой RSVP. Соответственно, главная задача при реализации стратегий интегрированных служб - обеспечение управления и прогнозирования использования ресурсов в сети. Для получения ожидаемых результатов все узлы сети должны поддерживать протокол RSVP. Если поток данных проходит через маршрутизаторы, не поддерживающие RSVP, то это может вызвать непредвиденное снижение производительности. Соединение будет установлено, однако маршрутизатор не сможет гарантировать производительность, необходимую для нормальной работы приложения. Работа функции интегрированного обслуживания продемонстрирована на приведенной ниже схеме.

Рисунок 13. Маршрут RSVP между клиентом и сервером.



Приложение на сервере, поддерживающее RSVP, обнаруживает запрос на соединение, полученный от клиента. В ответ приложение сервера отправляет клиенту команду PATH. Эта команда отправляется с помощью API RAPI или API сокетов QoS и содержит информацию об IP-адресах маршрутизаторов. Команда PATH содержит информацию о свободных ресурсах сервера и о маршрутизаторах на выбранном пути, а также о самом маршруте между клиентом и сервером. Затем приложение с поддержкой RSVP в системе клиента отправляет команду RESV на сервер, сигнализируя о том, что ресурсы выделены. С помощью этой команды выполняется резервирование на основе информации о маршрутизаторах, указанной в команде PATH. Сервер и все маршрутизаторы, через которые пройдет поток данных, резервируют ресурсы для соединения RSVP. После получения сервером команды RESV приложение начинает передачу данных клиенту. Данные передаются по тому же маршруту, что и запрос на резервирование. Это еще раз показывает, насколько важную роль в успешной реализации стратегий играют возможности маршрутизаторов.

В отличие от HTTP, интегрированные службы не предназначены для кратковременных соединений RSVP. Выбор, конечно, остается за вами. Только вы можете определить оптимальную конфигурацию собственной сети. Подумайте, какие приложения чувствительны к падению производительности и требуют применения функций Quality of Service. Приложения, применяемые в стратегии интегрированных служб, должны поддерживать протокол RSVP. В настоящий момент на сервере нет приложений, поддерживающих RSVP, поэтому вам придется создать их самостоятельно. Более подробная информация приведена в разделе RSVP.

При поступлении пакетов, требующих дальнейшей пересылки, сервер определяет, достаточно ли ресурсов для отправки пакетов. Результат такой проверки зависит от размера свободного пространства в наборе маркеров. Такие параметры, как число битов в наборе маркеров, ограничения пропускной способности, ограничения на скорость передачи маркера и максимальное число соединений с сервером, настраиваются вручную. Эти значения называются ограничениями производительности. Если при приеме входящих пакетов ограничение набора маркеров превышает, то такие пакеты считаются внепрофильными. Сервер может обрабатывать внепрофильные пакеты по-разному. Он может задержать, заново сформировать, повторно передать или удалить пакеты. Пакеты, не нарушающие ограничений сервера, считаются профильными и передаются далее. В интегрированных службах каждому соединению присваивается отдельный набор маркеров. В дифференцированных службах вся подсеть или диапазон клиентов используют один и тот же набор маркеров.

Функции управления потоком данных

Понятие функции управления потоком данных относится только к стратегиями интегрированного обслуживания. Для достижения ожидаемых результатов все оборудование маршрута потока данных должно поддерживать протокол RSVP. Для работы с протоколом RSVP маршрутизаторы должны поддерживать некоторые функции управления потоком данных. Таким маршрутизаторы часто называются поддерживающими RSVP или QoS. Ваша система играет роль клиента или сервера. В этом случае, она не может выступать в качестве маршрутизатора.

Существуют следующие функции управления потоком данных:

Планировщик пакетов

Планировщик пакетов управляет пересылкой пакетов на основе информации, указанной в заголовке IP. Планировщик пакетов обеспечивает доставку пакетов в соответствии с параметрами стратегии. Планировщик действует в очереди пакетов.

Классификатор пакетов

Классификатор пакетов присваивает пакетам в потоке IP определенные уровни обслуживания на основе информации заголовка IP. Каждому входящему пакету классификатором присваивается определенный класс. Все пакеты одного класса обрабатываются одинаково. Этот способ обработки определяется параметрами стратегии.

Управление доступом

Функция управления доступом реализует алгоритм принятия решения, с помощью которого маршрутизатор определяет, достаточно ли ресурсов для обеспечения запрошенного уровня обслуживания QoS для нового потока. В случае отсутствия необходимого объема ресурсов новым поток не принимается. Если поток принят, то маршрутизатор выделяет классификатор и планировщик пакетов для резервирования необходимого уровня обслуживания QoS. Функция управления доступом выполняется на каждом из маршрутизаторов, через которые проходит поток данных.

В этот раздел не содержит полной информации о классификаторах о планировщиках. Ссылки на источники дополнительной информации приведены в разделе Информация, связанная с QoS.

Типы интегрированного обслуживания

» Существует два типа интегрированного обслуживания: управляемая нагрузка и гарантированное.

Управляемая нагрузка

Служба управляемой нагрузки обеспечивает работу приложений, высокочувствительных к перегруженности сети, таких как приложения, работающие в режиме реального времени. При этом приложения должны справляться с небольшими потерями данных и кратковременными задержками. Если приложение применяет службу управляемой нагрузки, то его производительность не будет падать при увеличении нагрузки на сеть. Для потока данных обеспечивается уровень обслуживания, сходный с уровнем обслуживания в сети при низкой нагрузке.

Для обслуживания управляемой нагрузки маршрутизаторы должны зарезервировать необходимую пропускную способность и достаточные ресурсы для обработки пакетов. Для этого они должны поддерживать QoS и интегрированные службы. Информацию о том, поддерживает ли маршрутизатор Quality of Service и функцию управления потоком данных, можно получить из документации маршрутизатора. Управление потоком данных состоит из следующих компонентов: планировщика пакетов, классификатора пакетов и функций управления доступом.

Гарантированное обслуживание

Гарантированное обслуживание обеспечивает доставку пакетов за заданное время. Гарантированное обслуживание применяется, например, системами видео- и аудиовещания, использующими потоковые технологии. Гарантированное обслуживание ограничивает максимальное время ожидания в очереди, поэтому пакеты не задерживаются в очереди дольше указанного времени. Для обеспечения гарантированного обслуживания все маршрутизаторы на пути пакета должны поддерживать функции RSVP. Гарантированное обслуживание определяется ограничениями набора маркеров и пропускной способности. «

Ограничения на набор маркеров и пропускную способность

» Ограничения на набор маркеров и пропускную способность называются ограничениями производительности. Эти ограничения позволяют обеспечить надежную доставку пакетов в исходящих стратегиях как интегрированного, так и дифференцированного обслуживания.

Размер набора маркеров

Размер набора маркеров определяет размер буфера, применяемого в случае, если информация поступает на сервер быстрее, чем сервер передает ее дальше. Если приложение слишком быстро передает данные серверу, этот буфер заполняется. Если приложение передает данные медленнее, чем сервер передает их дальше, то буфер опустошается. Если данные поступают на сервер с той же скоростью, с какой они передаются дальше, размер набора маркеров не меняется. После заполнения буфера QoS обрабатывает все дополнительные пакеты как внепрофильные. В пределах данной стратегии вы можете задать способ обработки внепрофильных потоков данных.

Ограничение на скорость передачи маркера

Ограничение скорости (пропускной способности) определяет долгосрочную скорость передачи данных, или число битов, проходящих по сети за одну секунду. Любой клиент, отправляющий запрос RSVP, запрашивает определенную пропускную способность (ограничение на поток). Стратегия QoS сравнивает запрошенную пропускную способность со значениями, заданными для этой стратегии. Если выполнение запроса сервером приведет к превышению ограничения, то сервер отклоняет запрос. Ограничение на скорость передачи маркера используется только для управления доступом в стратегиях интегрированного обслуживания. Оно измеряется в Кбит/с. Допустимы значения от 10 Кбит/с до 1 Гбит/с.

Средняя скорость должна быть меньше максимальной скорости, чтобы ресурсы интерфейса не использовались полностью. Например, если у вас есть модем со скоростью передачи данных 36 Кбит/с или меньше, то необходимо установить такую среднюю скорость, чтобы ресурсы интерфейса использовались не полностью.

Совет: Для определения необходимых ограничений рекомендуется запустить монитор. Создайте стратегию с набором маркеров, достаточным для сбора информации о большей части потоков сети. Запустите сбор данных для этой стратегии. Пример одного из способов сбора сведений обо всех

потоках данных приложений и сети приведен в разделе Сбор текущих статистических показателей сети. Исходя из полученных результатов, установите необходимые ограничения.

Дополнительная информация приведена в разделах Дифференцированные классы обслуживания и Интегрированные службы. <<

Интегрированное обслуживание с использованием кодовых знаков дифференцированного обслуживания

Эта стратегия чаще всего применяется в смешанной среде. Среда называется смешанной в том случае, когда запросы на резервирование интегрированного обслуживания передаются через различные маршрутизаторы, не поддерживающие резервирование интегрированного обслуживания, но поддерживающие дифференцированные службы. Так как для передачи потоков данных применяются неодинаковые домены, соглашения об уровне обслуживания и функции оборудования, то необходимый уровень обслуживания достигим не всегда.

Для исправления ситуации вы можете добавить в стратегию интегрированных служб кодовые знаки дифференцированных служб. Если в стратегии применяется маршрутизатор, не поддерживающий протокол RSVP, то это позволит сохранить некоторый приоритет в стратегии. Добавляемые кодовые знаки обозначают способ обработки на транзитном участке.

>> Без сигналов

Кроме кодовых знаков, описанных выше, вы теперь можете применять функцию “Без сигналов”. Параметр “Без сигналов” задается в стратегии интегрированного обслуживания. Этот параметр можно указать в панели **Свойства** любой стратегии интегрированного обслуживания.

1. В Навигаторе разверните значок сервера —> **Сеть** —> **Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
3. Откройте **Стратегии исходящих соединений** —> **IntServ**.
4. Щелкните правой кнопкой мыши на имени созданной стратегии и выберите пункт **Свойства**. Будет показано окно диалога Свойства IntServ.
5. Для включения или выключения опции “Без сигналов” выберите вкладку **Управление потоком данных**. Здесь же задаются параметры расписания, клиента, приложений и обработки потока данных.

С помощью API с функцией “без сигналов” можно создать приложение, загружающее на сервер правило RSVP, которому для обеспечения поддержки RSVP необходимо только приложение сервера. Обработка сигналов RSVP от имени клиента выполняется автоматически. При этом соединение RSVP устанавливается для приложения, даже если приложение клиента не поддерживает протокол RSVP. <<

Дополнительная информация приведена в разделах дифференцированные классы обслуживания и интегрированные службы.

Протокол RSVP и API QoS



Для резервирования интегрированного обслуживания применяется Протокол резервирования ресурсов (RSVP) вместе с API RAPI или API сокетов QoS (qtq). Все узлы, через которые проходит поток данных, должны поддерживать протокол RSVP. Возможность применения стратегий интегрированных служб часто называется поддержкой RSVP. Дополнительная информация о функциях маршрутизатора, необходимых для применения протокола RSVP, приведена в разделе Функции управления потоком данных.

С помощью протокола RSVP резервируются ресурсы RSVP на всех узлах маршрута потока данных. Срок резервирования зависит от уровня обслуживания, указанного в стратегии. При резервировании определяется способ обработки и пропускная способность для потока данных. Все узлы сети соглашаются обеспечить зарезервированный способ обработки.

RSVP - это простой протокол, в котором резервирование выполняется в одном направлении (от получателя). В более сложных соединениях, применяемых, например, в аудио- и видеоконференциях, отправители одновременно являются и получателями. В этом случае, необходимо установить по два сеанса RSVP для каждой из участвующих сторон.

Для работы с интегрированными службами необходимо, чтобы протокол RSVP поддерживали не только маршрутизаторы, но и приложения. Поскольку на сервере iSeries нет стандартных приложений, поддерживающих RSVP, вам потребуется создать собственные приложения, использующие API RAPI или API сокетов QoS (qtoq). Эти API позволяют приложению работать с протоколом RSVP. Существует множество источников подробной информации об этих моделях, принципе их действия и системе обмена сообщениями. Вам следует изучить протокол RSVP и ознакомиться с документом RFC 2205.

API сокетов QoS (qtoq)

API сокетов QoS (qtoq) позволяют упростить процесс настройки протокола RSVP в системе iSeries. API сокетов qtoq вызывают API RAPI и выполняют некоторые из наиболее сложных задач. API сокетов qtoq менее гибки по сравнению с API RAPI, но зато позволяют сэкономить ваши усилия. С помощью версии "без сигналов" этих API можно создать следующие приложения:

- Приложение, загружающее правило RSVP на сервер.
- Приложение, которому для поддержки RSVP необходимо только серверное приложение диалога TCP/IP.

Обработка сигналов RSVP от имени клиента выполняется автоматически.

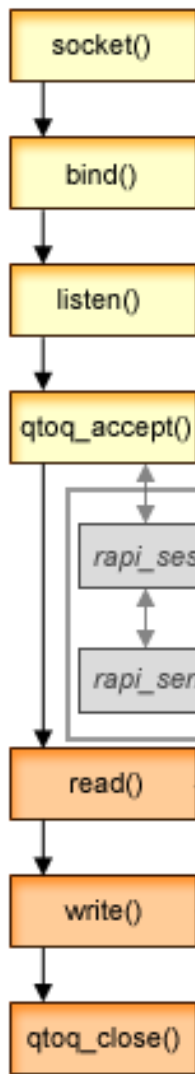
Информация о типичной последовательности вызовов API QoS для приложения/протокола, применяющего сокет QoS с установкой или без установки соединения, приведена в разделах Последовательность вызовов API QoS с установкой соединения и Последовательность вызовов API QoS без установки соединения. <<

Последовательность вызовов API QoS с установкой соединения

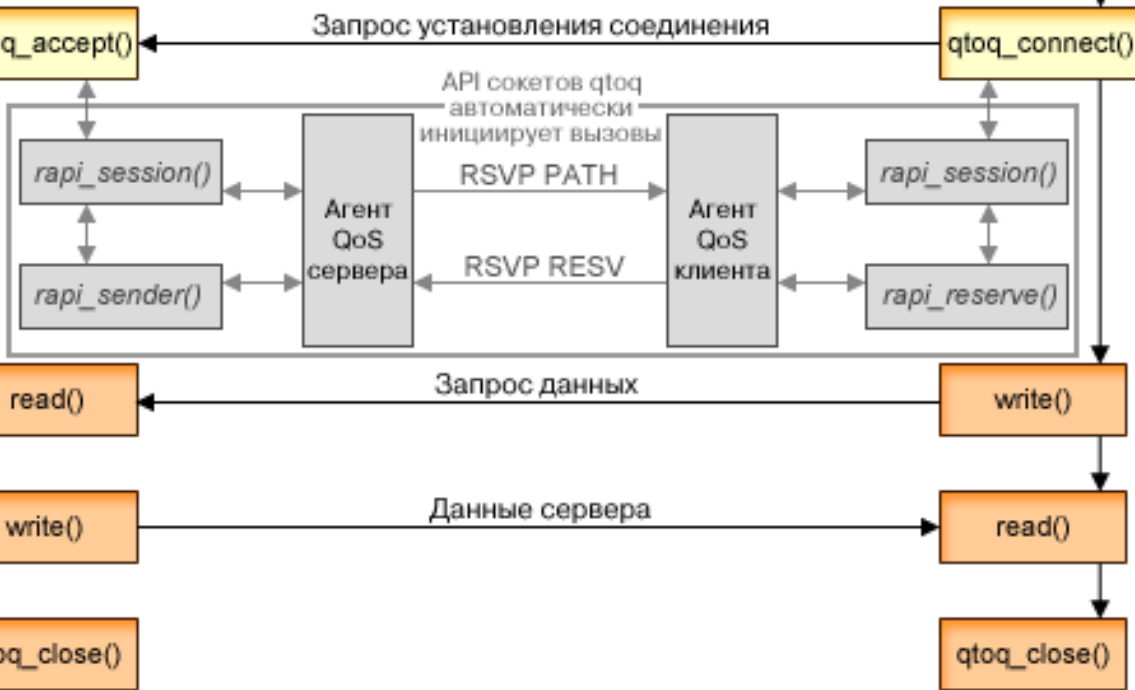
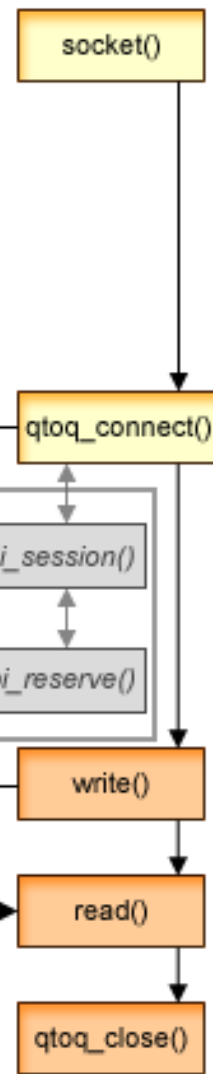
>> На приведенной ниже схеме изображена взаимосвязь функций API сокетов QoS клиента и сервера для протокола с установкой соединения, такого как Протокол управления передачей (TCP).

Когда поток данных, передаваемый с установкой соединения, требует инициализации протокола RSVP, вместе с функциями API QoS, запускающими этот протокол, вызываются дополнительные функции. В результате выполнения этих функций агенты QoS в системах клиента и сервера настраивают протокол RSVP для передачи потока данных между клиентом и сервером.

Приложение сервера



Приложение клиента



Последовательность событий qtoq: Приведенная ниже последовательность вызовов функций сокетов соответствует схеме. Кроме того, эта последовательность описывает взаимосвязь между приложениями клиента и сервера в случае, когда устанавливается соединение. Ниже указываются модификации API сокетов.

Приложение сервера

Вызов qtoq_accept() для правила "Без сигналов"

1. Приложение вызывает функцию socket(), чтобы получить дескриптор сокета.
2. Приложение задает ожидаемые соединения с помощью функции listen().
3. Приложение вызывает API qtoq_accept() и ожидает запрос на установку соединения от клиента.
4. Этот API вызывает API rapi_session(). В случае успешного выполнения последнего присваивается ИД сеанса QoS.
5. API вызывает стандартную функцию accept() для ожидания запроса на установку соединения от клиента.

6. Когда поступает запрос на установку соединения, для запрошенного правила выполняются функции управления доступом. Правило отправляется в стек TCP/IP. Если оно допустимо, то оно возвращается в вызвавшее приложение с кодом результата и ИД сеанса.
7. Приложения клиента и сервера выполняют необходимый обмен данными.
8. Приложение вызывает функцию `qtoq_close()`, чтобы закрыть сокет и выгрузить правило.
9. Сервер QoS удаляет правило из диспетчера QoS, удаляет сеанс QoS и выполняет прочие необходимые действия для освобождения ресурсов.

Вызов `qtoq_accept()` с обычной обработкой сигналов RSVP

1. Приложение вызывает функцию `socket()`, чтобы получить дескриптор сокета.
2. Приложение задает ожидаемые соединения с помощью функции `listen()`.
3. Приложение вызывает API `qtoq_accept()` и ожидает запрос на установку соединения от клиента.
4. При поступлении запроса на установку соединения вызывается API `rapi_session()`, чтобы создать для этого соединения сеанс на сервере QoS и получить ИД сеанса QoS, который будет возвращен вызвавшему приложению.
5. Вызывается API `rapi_sender()`, чтобы сервер QoS отправил сообщение PATH и ожидал сообщения RESV от клиента.
6. Вызывается API `rapi_getfd()`, чтобы получить дескриптор, применяемый приложениями при ожидании сообщений о событиях QoS.
7. Дескрипторы приема и QoS возвращаются в приложение.
8. Сервер QoS ожидает поступления сообщения RESV. При получении сообщения сервер загружает необходимое правило в диспетчере QoS и отправляет сообщение приложению, если это приложение запросило уведомление в вызове API `qtoq_accept()`.
9. Сервер QoS продолжает обновлять установленный сеанс.
10. По окончании работы с соединением приложение вызывает API `qtoq_close()`.
11. Сервер QoS удаляет правило из диспетчера QoS, удаляет сеанс QoS и выполняет прочие необходимые действия для освобождения ресурсов.

Приложение клиента

Вызов `qtoq_connect()` с обычной обработкой сигналов RSVP

1. Приложение вызывает функцию `socket()`, чтобы получить дескриптор сокета.
2. Приложение вызывает функцию `qtoq_connect()`, чтобы сообщить приложению сервера о предстоящей установке соединения.
3. Функция `qtoq_connect()` вызывает API `rapi_session()`, чтобы создать сеанс для этого соединения на сервере QoS.
4. Сервер QoS начинает ожидать поступления команды PATH через запрошенное соединение.
5. Вызывается API `rapi_getfd()`, чтобы получить дескриптор QoS, применяемый приложениями при ожидании сообщений QoS.
6. Вызывается функция `connect()`. В приложение возвращается код результата функции `connect()` и дескриптор QoS.
7. Сервер QoS ожидает поступления сообщения PATH. В ответ на полученное сообщение сервер отправляет сообщение RESV серверу QoS, расположенному в системе сервера приложений.
8. В случае, если приложение запросило уведомление, сервер отправляет приложению уведомление с помощью дескриптора QoS.
9. Сервер QoS продолжает обновлять установленный сеанс.
10. По окончании работы с соединением приложение вызывает API `qtoq_close()`.
11. Сервер QoS закрывает сеанс и выполняет все необходимые действия для освобождения ресурсов.

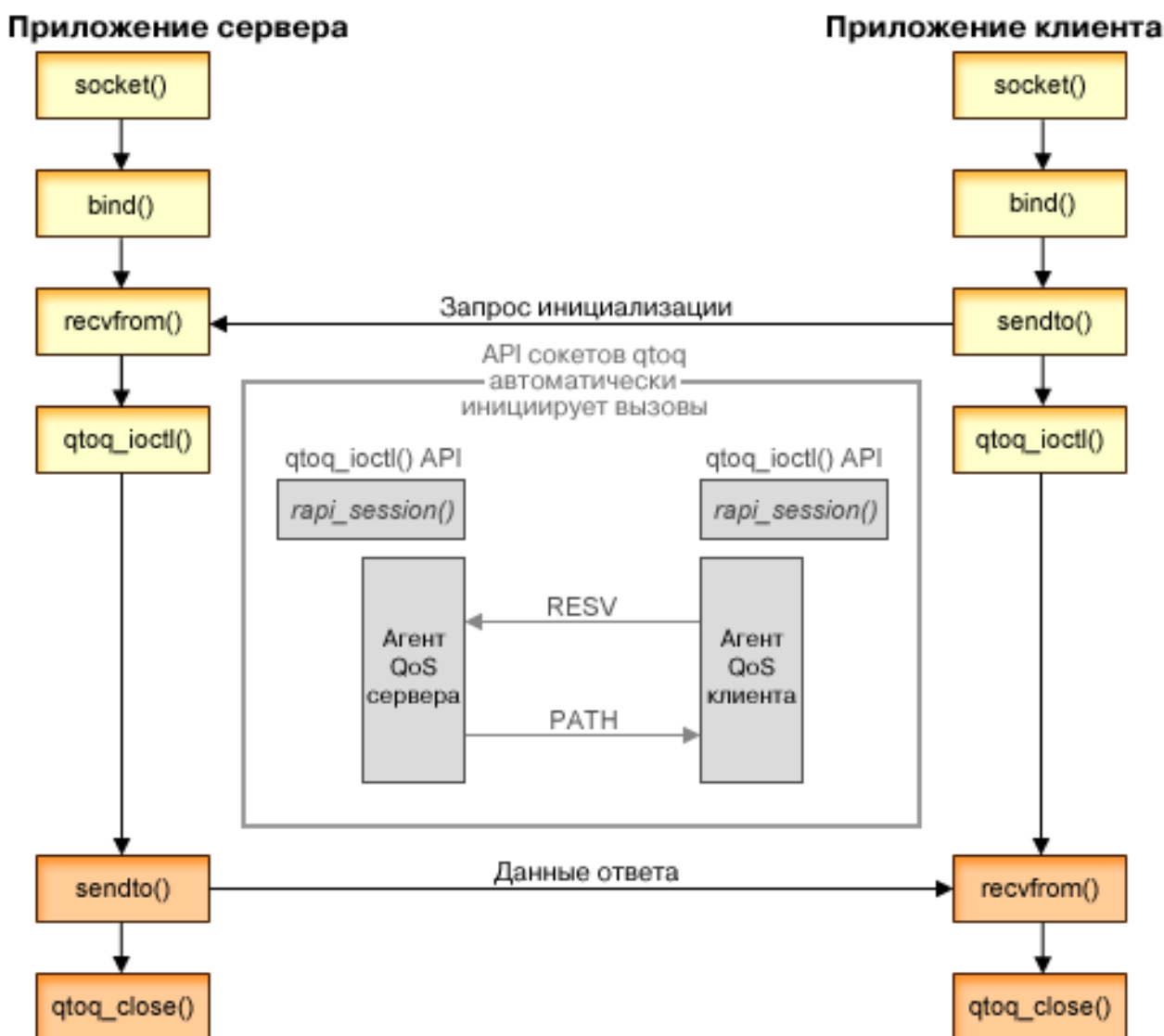
Вызов `qtoq_connect()` для правила "Без сигналов"

Такой запрос недопустим для приложения клиента, так как в данной ситуации ответ от клиента не требуется. <<

Последовательность вызовов API QoS без установки соединения

➤ В приведенных ниже примерах для клиента и сервера продемонстрированы вызовы API сокетов QoS для передачи потока данных без установки соединения.

Когда поток данных, передаваемый без установки соединения, требует инициализации протокола RSVP, то вместе с функциями API QoS, запускающими этот протокол, вызываются дополнительные функции. В результате выполнения этих функций агенты QoS в системах клиента и сервера настраивают протокол RSVP для передачи потока данных между клиентом и сервером.



Последовательность событий qtoq: Приведенная ниже последовательность вызовов функций сокетов соответствует схеме. Кроме того, эта последовательность описывает взаимосвязь между

приложениями клиента и сервера в случае, когда соединение не устанавливается. Ниже указываются модификации API сокетов.

Приложение сервера

Вызов `qtoq_ioctl()` для правила "Без сигналов"

1. На сервер QoS отправляется запрос на выполнение функций управления доступом для указанного правила.
2. В случае, если правило может быть принято, вызывается функция, отправляющая на сервер QoS запрос на загрузку этого правила.
3. Информация о результатах выполнения этой операции возвращается инициатору.
4. По окончании работы приложения с соединением API закрывает соединение путем вызова функции `qtoq_close()`.
5. Сервер QoS удаляет правило из диспетчера QoS, удаляет сеанс QoS и выполняет прочие необходимые действия для освобождения ресурсов.

Вызов `qtoq_ioctl()` с обычной обработкой сигналов RSVP

1. На сервер QoS отправляется запрос на выполнение функций управления доступом для указанного соединения.
2. Вызывается API `rapi_session()`, чтобы отправить запрос на создание сеанса для этого правила и получить ИД сеанса QoS, который возвращается инициатору.
3. Вызывается API `rapi_sender()` для инициализации отправки сообщения PATH клиенту.
4. Вызывается API `rapi_getfd()` для получения дескриптора файла, необходимого при ожидании сообщений о событиях QoS.
5. Инициатору возвращаются дескриптор `select()`, ИД сеанса QoS и код состояния.
6. Сервер QoS загружает правило при получении сообщения RESV.
7. По окончании работы с соединением приложение вызывает API `qtoq_close()`.
8. Сервер QoS удаляет правило из диспетчера QoS, удаляет сеанс QoS и выполняет прочие необходимые действия для освобождения ресурсов.

Приложение клиента

Вызов `qtoq_ioctl()` с обычной обработкой сигналов RSVP

1. Вызывается API `rapi_session()`, чтобы отправить запрос на создание сеанса для соединения. API `rapi_session()` отправляет запрос на выполнение функций управления доступом для этого соединения. Запрос на соединение отклоняется клиентом только в том случае, если для клиента существует настроенное, но в данный момент не активизированное правило. API возвращает ИД сеанса QoS, который затем возвращается в приложение.
2. Вызывается API `rapi_getfd()` для получения дескриптора файла, необходимого при ожидании сообщений о событиях QoS.
3. Функция `qtoq_ioctl()` возвращает инициатору дескриптор ожидания и ИД сеанса.
4. Сервер QoS ожидает поступления сообщения PATH. В ответ на полученное сообщение PATH сервер отправляет сообщение RESV и с помощью дескриптора сеанса уведомляет приложение о событии.
5. Сервер QoS продолжает обновлять установленный сеанс.
6. По окончании работы с соединением приложение клиента вызывает API `qtoq_close()`.

Вызов `qtoq_ioctl()` для правила "Без сигналов"

Такой запрос недопустим для приложения клиента, так как в данной ситуации ответ от клиента не требуется. <<

Планирование QoS

>> Планирование - важнейший этап реализации функции Quality of Service. Для достижения ожидаемых результатов вы должны собрать сведения о сетевом оборудовании и потоках данных в сети. В разделе Советник по планированию QoS приведены основные вопросы, на которые необходимо ответить на этапе планирования. Кроме того, перед тем как приступить к настройке QoS, ознакомьтесь со следующими разделами:

Требования к правам доступа

Содержит список всех прав доступа, необходимых для настройки QoS и сервера каталогов.

Требования к системе

В этом разделе описаны требования, предъявляемые к системе при использовании QoS.

Упорядочивание стратегий QoS

Стратегии применяются в том порядке, в котором они расположены в файле. Это относится только к стратегиям дифференцированного обслуживания и числа соединений.

Соглашения об уровне обслуживания

Соглашения об уровне обслуживания являются важной составной частью QoS. В процессе планирования QoS необходимо заключить с сетевым провайдером соглашение об уровне обслуживания.

Сетевое аппаратное и программное обеспечение

Качество обслуживания определяется самым слабым звеном цепочки. Эффект от применения QoS во многом зависит от используемого оборудования.

Производительность сети

Функцию QoS нельзя рассматривать отдельно от понятия производительности сети. Как правило, именно перегруженность сети и, как следствие, потеря пакетов служат причиной, по которой решают применять QoS. Перед настройкой стратегий рекомендуется с помощью монитора QoS измерить текущие статистические показатели потоков данных IP, связанные с производительностью. Полученные данные позволят определить "узкие места" сети. Дополнительная информация приведена в параграфе Отслеживание транзакций сервера раздела Устранение неполадок.

Советник по планированию QoS

Перед настройкой стратегий QoS ответьте на приведенные в этом разделе вопросы. Это позволит создать схему планирования, которая будет содержать рекомендуемые стратегии, учитывающие особенности установленных в системе приложений.



Требования к правам доступа

>> Стратегии Quality of Service могут содержать конфиденциальную информацию о сети. По этой причине, административные права доступа к QoS следует предоставлять только при необходимости. Ниже перечислены права доступа, которые требуются для настройки стратегий QoS и серверов каталогов LDAP. Поскольку стратегии QoS хранятся на сервере каталогов LDAP, необходимы и те, и другие права доступа.

Предоставление прав доступа, необходимых для управления сервером каталогов

Администратору QoS потребуются следующие права доступа: *ALLOBJ и *IOSYSCFG. Альтернативные права доступа рассмотрены в разделе Настройка сервера каталогов.

Предоставление прав доступа, необходимых для запуска сервера TCP/IP

Для того чтобы предоставить права доступа к командам STRTCPSVR и ENDTCPVR, выполните следующие действия:

1. **STRTCPSVR**: В командной строке введите GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), указав вместо ADMINPROFILE имя своего профайла администратора, и нажмите **Enter**.
2. **ENDTCPSVR**: В командной строке введите GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE), указав вместо ADMINPROFILE имя своего профайла администратора, и нажмите **Enter**.

Предоставление прав доступа ко всем объектам и к конфигурации системы

Пользователям, которые будут настраивать QoS, рекомендуется предоставить права доступа системного администратора. Для того чтобы предоставить права доступа ко всем объектам и к конфигурации системы, выполните следующие действия:

1. В Навигаторе разверните значок сервера —> **Пользователи и группы**.
2. Дважды щелкните на **Все пользователи**.
3. Щелкните правой кнопкой мыши на профайле администратора и выберите **Свойства**.
4. В окне Свойства щелкните на **Возможности**.
5. На странице Возможности выберите **Доступ ко всем объектам и к конфигурации системы**.
6. Нажмите **ОК**, чтобы закрыть страницу Возможности.
7. Нажмите **ОК**, чтобы закрыть окно Свойства.



Требования к системе

Компонент Quality of Service (QoS) встроен в операционную систему. Для настройки и запуска QoS на сервере должна быть установлена операционная система OS/400^(R) версии не ниже V5R1. Кроме того, выполните следующие требования:

1. Установите компонент TCP/IP Connectivity Utilities (57xx-TC1).
2. Установите Навигатор iSeries не PC. Во время установки Client Access обязательно выберите категорию Сеть. Компонент Quality of service находится в разделе Стратегии IP Policies категории Сеть.

Примечание: Дополнительная информация о TCP/IP, сетях и IP-адресах приведена в книгах TCP/IP Tutorial and Technical Overview и V4 TCP/IP for AS/400^(R): More Cool Things Than Ever, ссылки на которые можно найти в разделе Информация, связанная с QoS.

Упорядочивание стратегий QoS

» При наличии пересекающихся стратегий дифференцированного обслуживания или числа соединений важную роль играет последовательность, в которой стратегии расположены в Навигаторе. Пересекающимися называются стратегии, в которых применяется один и тот же клиент, приложение, расписание или протокол. В меню Навигатора стратегии представлены в виде упорядоченного списка. Приоритет стратегии определяется ее положением в списке. Стратегию, которую необходимо сделать более приоритетной относительно другой стратегии, следует поместить выше в списке стратегий.

Для того чтобы определить, пересекается ли стратегия с другими стратегиями, выполните следующие действия:

1. В Навигаторе разверните значок сервера —> **Сеть** —> **Стратегии IP**.
2. Щелкните правой кнопкой мыши на **Quality of Service**.
3. Выберите пункт **Конфигурация**.

4. Выберите одну из папок стратегий.
5. Щелкните правой кнопкой мыши на стратегии, пересекающейся с другими стратегиями. Пересекающиеся стратегии помечены специальным значком.
6. Выберите **Показать пересечения**. Появится панель пересекающихся стратегий.

Для изменения порядка, в котором стратегии расположены в списке, выполните следующие действия:

- Выделите стратегию и с помощью кнопок Вверх и Вниз измените ее позицию.
- Щелкните правой кнопкой мыши на стратегии и выберите пункт **Вверх** или **Вниз**.
- Обновите сервер QoS. Для этого нажмите кнопку Обновить сервер или обратитесь за более подробными инструкциями к разделу Справка по выполнению задач QoS.



Соглашение об уровне обслуживания

Этот раздел не содержит полного описания соглашений об уровне обслуживания (SLA), а лишь затрагивает некоторые важные аспекты SLA, связанные с реализацией Quality of Service. Качество обслуживания, обеспечиваемое стратегиями и резервированием ресурсов, определяется самым слабым звеном. Это означает, что если хотя бы один узел маршрута между клиентом и сервером не поддерживает какую-либо функцию дифференцированных или интегрированных служб, то ожидаемые результаты не будут достигнуты. Если SLA не обеспечивает достаточных ресурсов, то никакие стратегии не помогут решить проблемы, связанные с перегрузкой сети.

То же относится и к соглашениям между провайдерами Internet. Все провайдеры различных доменов должны договориться о поддержке запросов Quality of Service. При этом могут возникнуть трудности, связанные с обеспечением взаимодействия.

Убедитесь в том, что вы располагаете полной информацией о текущем фактическом уровне обслуживания. В соглашениях об обработке потоков данных подробно описываются способы обработки пакетов, а именно, их удаления, маркировки, задержки и дальнейшей передачи. Основная цель применения Quality of Service - получить контроль над задержками пакетов, пропускной способностью, потерей пакетов, готовностью к работе и производительностью. Соглашения об уровне обслуживания должны обеспечивать ресурсы, необходимые для реализации стратегий. Убедитесь в наличии необходимого уровня обслуживания. В противном случае, ресурсы могут использоваться неэффективно. Например, если вы зарезервируете 500 Кбит/с для телефонной связи IP, но приложению необходимо только 20 Кбит/с, то вы понесете лишние расходы, если провайдер Internet не уведомит вас об неэффективном использовании ресурсов.

Сетевое оборудование и программное обеспечение

Эффект от применения QoS во многом зависит от используемого оборудования.

Приложения

Для применения стратегий интегрированного обслуживания необходимы приложения с поддержкой RSVP. Поскольку в настоящее время поддержка RSVP в приложениях iSeries не предусмотрена, вы должны ее включить. Для этого вы должны написать специальные программы с помощью API Протокол настройки резервирования ресурсов (RAPI) или API сокетов QoS (qtoc). Эти программы позволят приложениям использовать RSVP. Дополнительная информация приведена в разделе Протокол RSVP и API QoS.

Сетевые узлы

Маршрутизаторы, коммутаторы и серверы должны поддерживать Quality of Service. Для применения стратегий дифференцированного обслуживания сетевое оборудование должно поддерживать дифференцированные службы. Это означает, что сетевые узлы должны обеспечивать классификацию, измерение, маркировку, задержку и удаление пакетов IP. Более подробная информация об этих функциях (называемых обработчиками потоков данных) приведена в разделе Обработчики потоков данных.

Для применения стратегий интегрированного обслуживания сетевое оборудование должно поддерживать протокол RSVP. Это означает, что протокол RSVP должен поддерживаться всеми узлами сети. Более подробная информация о протоколе RSVP приведена в разделе RSVP.

Настройка QoS

Для настройки стратегий QoS вы можете воспользоваться мастерами Навигатора. Это удобно, поскольку мастера предлагают вам выполнить пошаговую процедуру настройки.

➤ После настройки стратегий вы можете отредактировать их, открыв объекты конфигурации в Навигаторе. Объекты конфигурации - это составляющие компоненты стратегии. Когда вы открываете меню Quality of Service в Навигаторе, вы видите папки клиентов, приложений, расписаний, стратегий, классов обслуживания, способов обработки на транзитных участках и URI. Эти объекты позволяют создать стратегию. Более подробная информация об этих объектах приведена в обзорной справке по Quality of Service в Навигаторе.

Настройка сервера каталогов

Инструкции по настройке сервера каталогов в QoS.

Настройка QoS с помощью мастеров

Инструкции по работе с мастерами QoS. ⏪

Включение QoS

Для того чтобы стратегии вступили в силу, их необходимо включить. Если вы настраивали стратегии с помощью мастеров, то сервер включит стратегии автоматически. Если вы изменяли стратегию путем редактирования объектов конфигурации, то вам необходимо динамически обновить сервер, чтобы стратегии стали активными. Перед включением стратегий просмотрите пересекающиеся стратегии и убедитесь в отсутствии конфликтов, которые могут стать причиной неполадок. Дополнительная информация приведена в разделе Упорядочивание стратегий QoS.

Настройка сервера каталогов

➤ Конфигурации стратегий QoS теперь хранятся на сервере каталогов LDAP. Это упрощает работу с QoS. Вместо того чтобы настраивать стратегии QoS на каждом сервере, вы можете сохранить данные конфигурации на локальном сервере каталогов, сделав их доступными для всех систем. При первой настройке функции Quality of Service на сервере запускается мастер начальной настройки. Этот мастер предложит вам настроить сервер каталогов.

Для настройки сервера каталогов вы должны располагать следующей информацией:

- Имя сервера каталогов
- Определите отличительное имя (DN), на которое будут ссылаться стратегии QoS

- Решите, следует ли применять защиту с помощью SSL на сервере каталогов LDAP
- Решите, следует ли применять ключевые слова для ускорения поиска стратегий на сервере каталогов.

Примечание: В настоящее время применение Kerberos для идентификации сервера QoS при обращении к каталогу не поддерживается.

Для управления сервером каталогов LDAP у вас должен быть один из следующих наборов прав доступа:

- Права доступа *ALLOBJ и *IOSYSCFG
- Права доступа *JOBCTL и права доступа к командам Остановить TCP/IP (ENDTCP), Запустить TCP/IP (STRTCP), Запустить сервер TCP/IP (STRTCPSVR) и Остановить сервер TCP/IP (ENDTCPSVR).
- Права доступа *AUDIT для настройки контроля за действиями в OS/400^(R).


Если вы работаете с Навигатором, то вам будет автоматически предоставлена Схема QoS по умолчанию. Если же вы пользуетесь другим редактором, то вам придется импортировать описанный ниже файл LDIF. Кроме того, вы должны будете импортировать этот файл, если после редактирования вы захотите восстановить исходный файл по умолчанию.

Схема QoS


Схема - это набор правил, определяющих, какие типы объектов LDAP считаются допустимыми для сервера QoS. На серверах iSeries V5R2 схема уже содержит необходимые правила для QoS. Если же применяемый сервер LDAP не является сервером iSeries, то эти правила необходимо импортировать на сервер LDAP. Для этого служит файл LDIF (LDAP Data Interchange Format - формат

обмена данными LDAP). Для загрузки файла LDIF перейдите на Web-страницу LDAP iSeries . Файл находится в разделе **Категории** → **Стратегии TCP/IP** в левой панели.

Редактирование файла LDIF

Для редактирования файлов схемы для сервера LDAP вы можете воспользоваться Средством управления каталогами (DMT) IBM^(R) SecureWay^(R). С помощью FTP вы можете загрузить файл setup.exe для DMT на свой PC. На вашем сервере файл setup.exe должен находиться в каталоге /qibm/proddata/os400/dirsrv/UserTools/Windows. Исходную схему QoS можно загрузить с Web-страницы LDAP iSeries. Пример схемы QoS приведен в разделе Принципы LDAP. На вашем сервере файл схемы находится в каталоге /QIBM/UserData/OS400/DirSrv. 

Настройка QoS с помощью мастеров

 Для настройки стратегий Quality of service применяются мастера QoS Навигатора. Ниже приведен список мастеров с информацией об их назначении:

Мастер первоначальной настройки

Этот мастер позволяет настроить конфигурацию для конкретной системы и задать информацию о сервере каталогов.

Мастера создания стратегии IntServ

Мастер создания стратегии IntServ позволяет создать стратегию интегрированного обслуживания. Эта стратегия регулирует пропускную способность сервера, управляя процессом принятия запросов RSVP. Заданные в стратегии ограничения производительности определяют, может ли сервер обеспечить пропускную способность, запрошенную приложением RSVP клиента. Для обслуживания стратегий интегрированного обслуживания, создаваемых с помощью мастера, необходимы маршрутизаторы с поддержкой RSVP.

Примечание: Перед настройкой стратегии интегрированного обслуживания необходимо создать приложения, поддерживающие протокол RSVP. Дополнительная информация приведена в разделе Протокол RSVP и API QoS.

Мастер создания стратегии DiffServ

Этот мастер позволяет разделять поток данных TCP/IP на компоненты и присваивать приоритеты каждому компоненту. Разделение потока на компоненты осуществляется с помощью стратегий. В стратегии можно задать приоритет для приложений и портов, а также время, когда стратегия будет применяться.

Мастер создания класса обслуживания DiffServ

Мастер создания класса обслуживания DiffServ позволяет задать кодовые знаки пакетов для маршрутизаторов и коммутаторов в сетях. С его помощью можно также задать ограничения на скорость передачи потока данных из сети. Классы обслуживания применяются в стратегии дифференцированного обслуживания.

Мастер создания стратегии числа соединений

Мастер создания входящей стратегии числа соединений позволяет ограничить число соединений, устанавливаемых с сервером. Ограничить доступ можно на основе адреса TCP/IP, приложения или локального интерфейса. Таким образом системный администратор управляет доступом определенных клиентов к серверу, приложениям или интерфейсам. Кроме того, применение стратегии QoS может повысить производительность сервера.

Мастер создания входящей стратегии URI

Мастер создания входящей стратегии URI позволяет ограничить число соединений, устанавливаемых с сервером. Ограничить доступ можно на основе URI, приложения или локального интерфейса. Таким образом, системный администратор управляет доступом определенных клиентов к определенным URI, приложениям или интерфейсам. Кроме того, применение стратегии QoS может повысить производительность сервера.

Примечание: Перед настройкой стратегий числа запросов URI необходимо выполнить следующие действия:

1. WRKHTTPCFG - измените экземпляр Web-сервера Apache. С помощью директивы Listen включите опцию Fast Response Cache Accelerator (FRCA).
2. STRTCPSVR SERVER(*HTTP) HTTPSrv(имя или экземпляра).
3. Создайте или измените стратегию URI с помощью функции QoS Навигатора. Порт приложения, указанный в стратегии URI должен совпадать с портом, заданным в директиве "Listen" FRCA экземпляра Web-сервера Apache.
4. STRTCPSVR SERVER(*QOS).

Порт приложения, указываемый в новых стратегиях URI должен совпадать с портом, заданным в директиве "Listen" FRCA экземпляра Web-сервера Apache. В противном случае, стратегия URI QoS будет действовать неправильно. Описание стратегий числа запросов URI приведено в разделе Число запросов на установление соединений и число запросов URI.

Выбрав необходимый тип, можно настроить стратегию с помощью соответствующего мастера из приведенного выше списка. Для того чтобы приступить к настройке стратегии, ознакомьтесь с информацией в разделе Работа с мастерами QoS в Навигаторе. <<

Работа с мастерами QoS в Навигаторе



Для запуска мастера QoS и создания новой стратегии выполните следующие действия:

1. В Навигаторе разверните значок сервера —> **Сеть** —> **Стратегии IP**.

2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
Примечание: Мастер начальной настройки автоматически запускается в следующих случаях:
 - Вы обновляете сервер. Вам потребуется настроить сервер каталогов, на котором будет храниться информация. При таком переходе к новому выпуску потери данных не происходит.
 - Вы впервые работаете с графическим пользовательским интерфейсом (GUI) QoS в данной системе.
 - Вы хотите вручную удалить всю прежнюю информацию о конфигурации и начать настройку заново. Это можно сделать только при открытом интерфейсе QoS.
3. Выполните инструкции **Мастера начальной настройки**. Если меню мастера начальной настройки не появляется, перейдите к шагу 4.
4. Выберите **Стратегии**. Щелкните правой кнопкой мыши на **IntServ**, **DiffServ**, **Число соединений** или **Запросы сервера** → **URI**.
5. Выберите **Создать стратегию**.



Управление QoS

После настройки и запуска стратегий QoS вам может потребоваться внести в них некоторые изменения. Ниже перечислены возможные операции по управлению стратегиями:

Работа со справкой QoS в Навигаторе

Вы, вероятно, заметили, что в этом разделе часто встречаются ссылки на справочную информацию по задачам QoS в Навигаторе. Если вы не знаете, как получить к ней доступ, ознакомьтесь с приведенными инструкциями.

Резервное копирование стратегий QoS

Вы можете создать резервные копии своих стратегий на случай непредвиденной утери файлов.

Копирование существующей стратегии

Вместо того чтобы создавать новую стратегию "с нуля", вы можете скопировать существующую стратегию и создать новую на ее основе.

Динамическое обновление стратегий

Вы можете динамически обновлять стратегии, не прекращая работы сервера. Пошаговые инструкции приведены в разделе *Обновление сервера QoS* справки по QoS в Навигаторе.

Изменение стратегий QoS

Вы можете изменять параметры существующих стратегий.

Изменение параметров конфигурации QoS

Вы можете изменять параметры конфигурации Quality of Service. К ним относятся параметры конфигурации сервера каталогов, ведения журнала и автоматического запуска сервера. Пошаговые инструкции приведены в разделе *Изменение свойств QoS* справки по QoS в Навигаторе.

Включение стратегий QoS

Для того чтобы стратегии вступили в силу, их необходимо включить. Не забудьте вручную проверить правильность стратегий, прежде чем включить их. Например, убедитесь, что стратегии расположены в правильном порядке. Дополнительная информация о роли, которую играет порядок стратегий, приведена в разделе *Упорядочивание стратегий QoS*. Пошаговые инструкции приведены в разделе *Включение стратегий QoS* справки по QoS в Навигаторе.

Отслеживание стратегий QoS

При настройке и изменении стратегий рекомендуется с помощью монитора QoS убедиться, что стратегии работают именно так, как предполагается.

Просмотр стратегий QoS

Просмотр пересекающихся стратегий позволяет определить возможную причину неправильных результатов. Вы можете найти и проанализировать любые существующие пересечения стратегий. Рекомендуется просматривать пересечения не только перед активизацией и тестированием стратегий, но и перед их печатью и резервным копированием. Это значительно ускорит дальнейшую отладку стратегий. Инструкции по просмотру пересекающихся стратегий приведены в разделе *Упорядочивание стратегий QoS*.

Работа со справкой QoS в Навигаторе

» Для просмотра справочной информации по Quality of Service выполните следующие действия в Навигаторе:

1. В Навигаторе разверните значок сервера —> **Сеть** —> **Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
3. В строке меню выберите **Справка** —> **Разделы справки**. На экране появится окно справки.




Резервное копирование стратегий QoS

» Резервное копирование файлов конфигурации рекомендуется выполнять во всех случаях. Это позволяет хранить стратегии как на вашем компьютере, так и сервере каталогов. В первую очередь необходимо сохранить следующие каталоги интегрированной файловой системы:

QIBM/UserData/OS400/QOS/ETC, QIBM/UserData/OS400/QOS/TEMP и QIBM/UserData/OS400/QOS/USR. Кроме

того, следует создать резервную копию публикующего агента сервера каталогов для сервера QoS. Публикующий агент содержит имя сервера каталогов, отличительное имя (DN) сервера QoS, порт связи с сервером каталогов и идентификационную информацию. В случае утери стратегий гораздо проще и удобнее воспользоваться резервными копиями, чем создавать стратегии заново. Ниже приведены советы общего характера относительно мер предосторожности:

1. **Воспользуйтесь программами резервного копирования и восстановления интегрированных файловых систем**
См. приведенную ниже ссылку на книгу Резервное копирование и восстановление.
2. **Напечатайте стратегии**
Распечатки - это надежное и удобное средство хранения информации. При необходимости вы всегда сможете восстановить утерянные данные.
3. **Скопируйте информацию на диск**
По сравнению с распечаткой, электронная копия обладает тем преимуществом, что в случае утери данных их не нужно вводить вручную. Достаточно скопировать резервный экземпляр на свой компьютер.
Примечание: Сервер iSeries копирует информацию на системный диск, а не на дискету. Файлы правил хранятся в каталоге QIBM/UserData/OS400/QOS/ETC, согласно отличительному имени в настроенном сервере каталогов. Для защиты данных, хранящихся на системном диске, вам рекомендуется воспользоваться соответствующими средствами защиты диска.

Если вы копируете данные на сервер iSeries, то вы должны разработать стратегию резервного копирования и восстановления. Подробная информация приведена в разделе Резервное копирование и восстановление  . <<

Копирование существующей стратегии

Некоторые стратегии могут быть очень похожи. Вместо того, чтобы создавать все стратегии с самого начала, можно создать копии одной базовой стратегии, а затем отредактировать их. В Навигаторе эта функция QoS называется *Создать стратегию на основе существующей*. Для копирования стратегий необходимо воспользоваться окном QoS в Навигаторе.

Инструкции по созданию копии существующей стратегии приведены в справочном разделе **Создание новой стратегии на основе существующей** Навигатора.

Для того чтобы стратегии вступили в силу, необходимо включить их, запустив сервер QoS или выполнив динамическое обновление сервера. Перед включением стратегий просмотрите пересекающиеся стратегии и убедитесь в отсутствии конфликтов, которые могут стать причиной неполадок. Дополнительная информация приведена в разделе Упорядочивание стратегий QoS.

Монитор QoS

» С помощью монитора QoS вы можете проанализировать поток данных IP, проходящий через сервер. Это позволит вам определить “узкие места” сети. Монитор может применяться не только для планирования QoS, но и для устранения неполадок. С помощью монитора QoS можно собирать данные о сети и, при необходимости, настраивать стратегии в соответствии с полученными сведениями.

Для запуска монитора QoS воспользуйтесь инструкциями, приведенными в справке по QoS Навигатора.

Примечание: Если во время сбора данных QoS вам потребовалось изменить конфигурацию QoS, то для обеспечения правильной работы монитора выполните следующие действия:

1. Остановите сбор данных QoS.
2. Внесите изменения в конфигурацию.
3. Перезапустите/обновите сервер QoS.

4. Запустите сбор данных QoS.

Вывод монитора

Вывод монитора зависит от типа отслеживаемой стратегии. Существуют следующие типы стратегий: DiffServ, IntServ (управляемая нагрузка), IntServ (гарантированное обслуживание), Количество соединений и URI. Поля, которые следует анализировать, зависят от типа стратегии. Наибольший интерес представляют поля со значениями, полученными в результате измерения. Следующие поля содержат измеряемые (а не заданные) значения: принятые запросы, активные соединения, службы соединений, количество соединений, отклоненные запросы, профильные пакеты, профильные биты, внепрофильные биты, общее число битов и общее число запросов.

Проанализировав приведенные выше показатели, можно выяснить, насколько поток данных в сети соответствует заданным стратегиям. Нижеследующие описания содержат более подробную информацию о полях вывода монитора для каждого типа стратегии. Примеры применения монитора для отслеживания стратегий QoS приведены в разделе Сценарии QoS.

- Стратегии дифференцированного обслуживания (См. 45)
- Стратегии интегрированного обслуживания (управляемая нагрузка) (См. 46)
- Стратегии интегрированного обслуживания (гарантированное обслуживание) (См. 47)
- Стратегии URI (См. 48)
- Стратегии количества соединений (См. 47)

Стратегии дифференцированного обслуживания

Поле	Описание
Имя стратегии	Имя, присвоенное этой стратегии.
Протокол	UDP, TCP, ALL
Средняя скорость передачи маркеров	Средняя скорость передачи маркеров, разрешенная этой стратегией для маршрутизаторов и серверов, через которые проходит поток.
Размер буфера маркеров	Максимальный размер буфера маркеров, разрешенная этой стратегией для маршрутизаторов и серверов, через которые проходит поток.
Максимальная скорость передачи маркеров	Максимальная скорость передачи для данного соединения.
Профильные пакеты	Число переданных пакетов IP, отвечающих параметрам этой стратегии.
Профильные биты	Число переданных битов, отвечающих параметрам этой стратегии.
Внепрофильные биты	Число переданных битов, не отвечающих параметрам этой стратегии.
Скорость передачи данных	Максимальное число битов, которое может быть передано по этому соединению в единицу времени.
Активные соединения	Общее число активных соединений.
Профайл потока данных	Тип обработки внепрофильных пакетов. Параметры формата: <ul style="list-style-type: none">• Изменение кодового знака• Задержка• Удаление
Общее число битов	Число битов, переданных согласно этой стратегии с момента ее запуска до момента сбора данных монитора.

Профильный кодовый знак	При добавлении к пакетам новых кодовых знаков этот кодовый знак добавляется к пакетам, отвечающим параметрам данной стратегии.
Внепрофильный кодовый знак	При добавлении к пакетам новых кодовых знаков этот кодовый знак добавляется к пакетам, не отвечающим параметрам данной стратегии.
Диапазон целевых адресов	Диапазон адресов, определяющий целевой адрес пакетов (контролируемых этой стратегией).
Общее число пакетов	Число пакетов, переданных согласно этой стратегии с момента ее запуска до момента сбора данных монитора.
Диапазон исходных портов	Диапазон исходных портов, определяющий список приложений, контролируемых этой стратегией.

Стратегии интегрированного обслуживания (управляемая нагрузка)

Поле	Описание
Имя стратегии	Имя, присвоенное этой стратегии.
Протокол	UDP или TCP
Целевой адрес	Диапазон адресов, определяющий целевой адрес пакетов (контролируемых этой стратегией).
Средняя скорость передачи маркеров	Средняя скорость передачи маркеров, разрешенная этой стратегией для маршрутизаторов и серверов, через которые проходит поток.
Размер буфера маркеров	Максимальный размер буфера маркеров, разрешенная этой стратегией для маршрутизаторов и серверов, через которые проходит поток.
Максимальная скорость передачи маркеров	Максимальная скорость передачи для данного соединения.
Общее число пакетов	Число пакетов, переданных согласно этой стратегии с момента ее запуска до момента сбора данных монитора.
Внепрофильные биты	Число переданных битов, не отвечающих параметрам этой стратегии.
Общее число битов	Число битов, переданных согласно этой стратегии с момента ее запуска до момента сбора данных монитора.
Скорость передачи данных	Максимальное число битов, которое может быть передано по этому соединению в единицу времени.
Профильные биты	Число переданных битов, отвечающих параметрам этой стратегии.
Максимальный размер пакета	Максимальный размер пакета, разрешенный этой стратегией.
Минимальная единица управления	Минимальное число битов, которое может быть удалено из набора маркеров. Например, при минимальной единице управления 100 бит пакеты меньшего размера будут удаляться только по 100 бит.
Профильные пакеты	Число переданных пакетов IP, отвечающих параметрам этой стратегии.

Диапазон исходных портов	Диапазон исходных портов, определяющий список приложений, контролируемых этой стратегией.
--------------------------	---

Стратегии интегрированного обслуживания (гарантированное обслуживание)

Поле	Описание
Имя стратегии	Имя, присвоенное этой стратегии.
Протокол	UDP или TCP
Целевой адрес	Диапазон адресов, определяющий целевой адрес пакетов (контролируемых этой стратегией).
Средняя скорость передачи маркеров	Средняя скорость передачи маркеров, разрешенная этой стратегией для маршрутизаторов и серверов, через которые проходит поток.
Размер буфера маркеров	Максимальный размер буфера маркеров, разрешенная этой стратегией для маршрутизаторов и серверов, через которые проходит поток.
Максимальная скорость передачи маркеров	Максимальная скорость передачи для данного соединения.
Общее число пакетов	Число пакетов, переданных согласно этой стратегии с момента ее запуска до момента сбора данных монитора.
Общее число битов	Число битов, переданных согласно этой стратегии с момента ее запуска до момента сбора данных монитора.
Внепрофильные биты	Число переданных битов, не отвечающих параметрам этой стратегии.
Гарантированная скорость передачи данных	Гарантированная скорость передачи данных в битах в секунду.
Профильные биты	Число переданных битов, отвечающих параметрам этой стратегии.
Максимальный размер пакета	Максимальный размер пакета, разрешенный этой стратегией.
Минимальная единица управления	Минимальное число битов, которое может быть удалено из набора маркеров. Например, при минимальной единице управления 100 бит пакеты меньшего размера будут удаляться только по 100 бит.
Профильные пакеты	Число переданных пакетов IP, отвечающих параметрам этой стратегии.
Отставание	Разность (в секундах) между предполагаемой и фактической задержками.
Диапазон исходных портов	Диапазон исходных портов, определяющий список приложений, контролируемых этой стратегией.

Стратегии количества соединений

Поле	Описание
Имя стратегии	Имя, присвоенное этой стратегии.
Число соединений	Число запросов на установление соединения, принимаемых в секунду.

Общее число запросов	Общее число запросов на установление соединения, переданных на данный сервер.
Принятые запросы	Общее число запросов на установление соединения, принятых данным сервером.
Отклоненные запросы	Общее число запросов, отклоненных сервером.
Среднее число соединений	Среднее число новых запросов на установление соединения, которые могут быть приняты сервером в секунду.
Максимальное число соединений	Максимальное число запросов на установление соединения, принимаемых одновременно.
Максимальное число соединений	Максимальное число сетевых соединений с сервером, устанавливаемых в секунду
Приоритет	Приоритет, присвоенный загруженным в Диспетчере QoS правилам фильтрации пакетов.
Приоритет очереди	Приоритет, присваиваемый входящим запросам на установление соединения, которые помещаются в эту очередь.
Диапазон целевых портов	Диапазон портов или порт, в который направляется поток данных на сервере.
Адрес интерфейса	IP-адрес отслеживаемого интерфейса системы.
Диапазон исходных адресов	Диапазон IP-адресов клиентов, отправляющих запросы на сервер.

Стратегии Запросы сервера - URI

Поле	Описание
Имя стратегии	Имя, присвоенное этой стратегии.
Число запросов	Число запросов, получаемых в секунду.
Общее число запросов	Общее число запросов, полученных целевым сервером.
Принятые запросы	Общее число принятых запросов.
Отклоненные запросы	Общее число отклоненных запросов.
URI	URI, контролируемый стратегией.
Среднее число принимаемых запросов	Среднее число новых запросов, которые могут быть приняты сервером в секунду.
Число принимаемых одновременно запросов	Максимальное число запросов, принимаемых одновременно.
Максимальное число запросов	Максимальное число запросов, принимаемых сервером в секунду.
Приоритет очереди	Приоритет, присваиваемый входящим запросам на установление соединения, которые помещаются в эту очередь.
Целевой порт	Порт, в который направляется поток данных на сервере.
Адрес интерфейса	IP-адрес отслеживаемого интерфейса системы.



Устранение неполадок QoS

Этот раздел содержит советы по устранению неполадок QoS.

Трассировка линии связи

Сервер поддерживает функцию трассировки для сбора данных о линии связи, такой как соединение локальной сети (LAN) или интерфейс глобальной сети (WAN). Для интерпретации всех данных трассировки необходимы специальные знания. Однако любой пользователь с помощью записей трассировки может определить, произошел ли обмен данными между двумя системами. Дополнительная информация приведена в пункте Трассировка линии связи раздела Устранение неполадок TCP/IP.

Включите поддержку QoS на сервере

В случае, если сервер QoS не запускается, прежде всего, следует проверить значение IPQOSNB с помощью команды CHGTCP. При первой настройке стратегий мастер первоначальной настройки автоматически включает поддержку QoS на сервере. Если по какой-либо причине это значение было изменено, то сервер не запускается. В командной строке введите CHGTCPA IPQOSNB(*YES).

Создайте журнал стратегий QoS

Функция Quality of service поддерживает ведение журнала. В журнале могут регистрироваться все операции, связанные с добавлением, удалением и изменением стратегий IP на сервере. Эта информация необходимо для отладки и проверки работы стратегий.

Создайте протокол стратегий QoS

При возникновении неполадок на сервере информация протоколов заданий поможет выяснить их причины.

Отслеживание транзакций сервера

Монитор QoS играет важнейшую роль в поиске и устранении неполадок QoS. Он позволяет собирать и просматривать информацию о производительности.

Выполните трассировку приложений TCP

Команда трассировки позволяет собирать данные о нескольких уровнях операций сервера. Эта информация может пригодиться при выяснении причин возникновения неполадок, связанных со стратегиями.

Упорядочивание стратегий QoS

Для правильной реализации функции Quality of service важен порядок расположения стратегий в файле.

Ведение журнала стратегий QoS

В QoS предусмотрена функция ведения журнала. Ведение журнала позволяет отслеживать различные операции над стратегиями QoS, в частности, добавление, удаление и изменение стратегий. Во время работы этой функции создается протокол операций над стратегиями. Эта информация позволяет отлаживать и проверять стратегии. Пусть, например, вы настроили применение стратегии с 9:00 до 16:00. Просмотрев протокол журнала, вы сможете узнать, действительно ли эта стратегия была добавлена в 9:00 и удалена в 16:00.

При включенной функции ведения журнала в журнале регистрируются все операции добавления, удаления и изменения стратегий. С помощью этих журналов можно создать файл на сервере iSeries. После этого информация, заносимая в журналы, позволит контролировать работу системы. На основе этих данных можно оптимизировать параметры применяемых стратегий.

Не следует заносить в журнал ненужную информацию. Ведение журнала может потребовать значительных ресурсов системы. Запустить и остановить ведение журнала можно с помощью Навигатора. Для просмотра протоколов журнала воспользуйтесь командной строкой.

Для запуска или прекращения ведения журнала выполните следующие действия:

1. В Навигаторе разверните значок сервера —> **Сеть** —> **Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.

3. Щелкните правой кнопкой мыши на пункте **QoS** и выберите **Свойства**.
4. Выберите опцию **Вести журнал**, чтобы начать ведение журнала.
5. Отмените выбор опции **Вести журнал**, чтобы прекратить ведение журнала.

Внимание: Если при выполнении описанной выше процедуры сервер работал, то необходимо перезапустить его. После включения функции ведения журнала ее можно активизировать двумя способами: перезапустить сервер или обновить сервер. В обоих случаях будет обновлено значение атрибута ведения журнала в файле `policy.conf`.

Просмотр записей журнала на экране

Для вывода записей журнала на экран выполните следующие действия:

1. Введите в командной строке сервера `iSeries: DSPJRN JRN(QUSRSYS/QQOS)`. Выберите **Опцию 5** для нужной записи журнала.

Просмотр записей журнала в файле вывода

Для работы с записями журнала в одном каталоге просмотрите файл `MODEL.OUT` в каталоге `QUSRSYS`. Скопировав записи журнала в файл вывода, можно просматривать записи с помощью `Query/400` и `SQL`. Кроме того, вы можете написать собственные программы на языке высокого уровня для обработки записей в файле вывода.

Для того чтобы скопировать записи журнала `QoS` в системный файл вывода, выполните следующие действия:

1. Скопируйте системный файл вывода `QSYS/QATOQQOS` в пользовательскую библиотеку. Это можно сделать с помощью команды Создать копию объекта (`CRTDUPOBJ`). Пример команды `CRTDUPOBJ`:
`CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(польз_библ) NEWOBJ(польз_файл)`
2. С помощью команды Показать журнал (`DSPJRN`) скопируйте записи из журнала `QUSRSYS/QQOS` в файл вывода, созданный на предыдущем шаге. При попытке скопировать `DSPJRN` в несуществующий файл вывода система создаст его, однако этот файл не будет содержать необходимых описаний полей.
 - a. `DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(польз_библ/польз_файл)`
 - b. `DSPF FILE(польз_библ/польз_файл)`

Протоколы заданий сервера QoS

При обнаружении неполадок стратегий `QoS` обязательно просмотрите протоколы заданий сервера `iSeries`. Протокол задания содержит сообщения об ошибках и другую информацию, связанную с `QoS`.

Только одно задание `QoS`, `QT0QSRVR`, выполняется в подсистеме `QSYSWRK`. Навигатор позволяет просмотреть предыдущий и текущий протоколы задания сервера `QoS`.

Для просмотра протокола выполните следующие действия:

1. Откройте **Сеть** и щелкните на **Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Quality of Service**.
3. Выберите **Средства диагностики** → **Протокол сервера QoS**.

Появится окно работы с заданием.

Ниже приведен список наиболее важных заданий с кратким описанием их предназначения:

QTCP

Это базовое задание, запускающее все интерфейсы TCP/IP. При возникновении общих неполадок TCP/IP просмотрите сообщения в протоколе задания QTCP/IP.

QTOQSRVR

Это базовое задание QoS, протокол которого содержит информацию о QoS. Для просмотра протокола QTOQSRVR запустите команду WRKSPLF QTCP (Работа с буферным файлом).

Для поиска в буферном файле сообщений об ошибках выполните следующие действия:

1. Введите в командной строке **WRKSPLF QTCP** и нажмите **Enter**.
2. Будет показано окно Работа со всеми буферными файлами. В столбце Пользовательские данные найдите значение QTOQSRVR для просмотра сообщений об ошибках, связанных непосредственно с сервером QoS.
3. Выберите **Опцию 5** в нужной строке. Прочтите информацию и запишите ИД сообщения с описанием причины неполадки. Например, TCP920C.
4. Дважды нажмите клавишу **F3** для возврата в главное меню.
5. Введите в командной строке **WRKMSGF** и нажмите **Enter**.
6. В меню Работа с файлом сообщений введите следующую информацию и нажмите **Enter**.
Файл сообщений: QTCPMSG
Библиотека: *LIBL
7. В меню Работа с файлом сообщений выберите **опцию 5** для просмотра нужного файла сообщений и нажмите **Enter**.
8. В меню Показать описания сообщений введите следующую информацию:
Перейти к: Введите записанный на шаге 3 ИД сообщения и нажмите **Enter**. Например, TCP920C.
9. Выберите **Опцию 5** для нужного ИД сообщения и нажмите **Enter**.
10. В меню Выбрать сведения о сообщении для просмотра выберите 30 (Все вышеуказанные) и нажмите **Enter**.
11. Будет показано подробное описание сообщения.

Отслеживание транзакций сервера

Монитор QoS может применяться на этапе планирования и на этапе устранения неполадок QoS.

С помощью монитора QoS вы можете проанализировать поток данных IP, проходящий через сервер. Это позволит вам определить “узкие места” сети. С помощью монитора QoS можно собирать данные о сети и, при необходимости, настраивать стратегии в соответствии с полученными сведениями.

Планирование и обеспечение производительности

Одной из самых сложных задач в реализации QoS является определение оптимальных ограничений для стратегий. Здесь нельзя дать конкретные рекомендации, так как к разным сетям предъявляются разные требования. Для того чтобы найти оптимальные значения параметров, воспользуйтесь монитором перед настройкой стратегий для конкретной сети.

Попробуйте создать стратегию дифференцированного обслуживания, не выбирая измерение показателей, чтобы выяснить, как меняется поток данных в сети. Включите эту стратегию и запустите монитор. С помощью данных, собранных монитором, можно настроить параметры стратегии в соответствии с требованиями, предъявляемыми к сети. В примере отслеживания стратегии продемонстрирован сбор сведений о потоке данных.

Устранение неполадок, связанных с производительностью

Монитор может также применяться при устранении неполадок. С помощью данных, собранных

монитором, можно определить, соблюдаются ли заданные в стратегии ограничения. Примеры вывода монитора приведены в разделе Сценарии QoS. Описание всех полей монитора приведено в разделе Монитор.

Сбор текущих статистических показателей сети



Ситуация

В программах-мастерах необходимо указывать ограничения производительности. Для этих параметров не предусмотрено рекомендуемых значений, поскольку ограничения определяются конкретными требованиями, предъявляемыми к сети. Для настройки этих ограничений необходима информация о производительности сети. Как правило, к моменту настройки стратегий Quality of Service вы уже располагаете такой информацией и можете сформулировать требования к сети. Для определения точных значений ограничений, например скорости передачи наборов маркеров, вы можете собрать данные обо всех потоках данных на сервере.

Действия

Создайте наиболее широкую стратегию дифференцированного обслуживания, не содержащую никаких ограничений (максимальных значений) и применимую ко всем интерфейсам и IP-адресам. С помощью монитора QoS соберите данные по этой стратегии.

Шаг 1: Откройте QoS в Навигаторе.

1. В Навигаторе разверните значок сервера —> **Сеть**—> **Стратегии IP**
2. Щелкните правой кнопкой мыши на пункте **Quality of Service** и выберите **Конфигурация**.
3. Откройте **Стратегии исходящих соединений**.
4. Щелкните правой кнопкой мыши на пункте **DiffServ** и выберите **Создать стратегию**. Будет запущен Мастер создания стратегии DiffServ.

Шаг 2: Создайте стратегию дифференцированного обслуживания

Так как вы будете собирать информацию о большей части данных, поступающих в сеть, назовите стратегию **Network**. В качестве остальных значений укажите все IP-адреса, все порты, все локальные IP-адреса и все периоды сбора (если это необходимо). Задайте в окнах диалога мастера следующие параметры:

Имя = Network (можно присвоить любое имя)

Клиент = All IP addresses

Приложение = All ports

Протокол = All protocols

Расписание = All times

Навигатор содержит список всех стратегий дифференцированного обслуживания, созданных на сервере.

Шаг 3: Создайте новый класс обслуживания

При заполнении форм мастера потребуется указать способ обработки на транзитных участках, ограничения производительности и способ обработки внепрофильных потоков данных. Все эти параметры определяются в классе обслуживания. Задайте достаточно большие значения, чтобы обеспечить максимально возможный поток данных.

Класс обслуживания фактически определяет скорость передачи потока данных, обеспечиваемую маршрутизатором. Для этого класса обслуживания можно задать имя **Без ограничений**, чтобы отразить максимальный уровень обслуживания. Навигатор содержит список всех классов обслуживания, определенных на сервере.

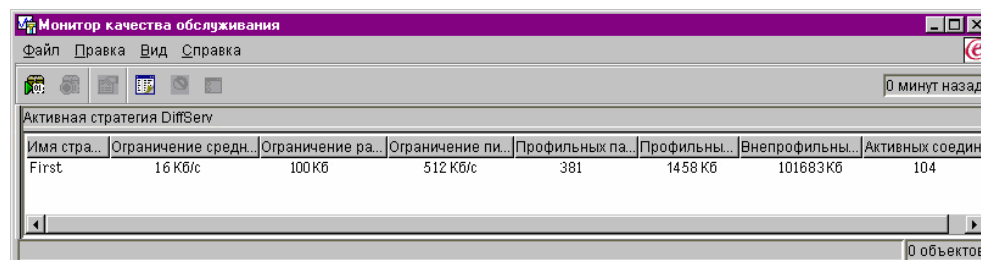
Шаг 4: Соберите данные о стратегии

Для того чтобы убедиться, что поток данных обрабатывается согласно заданной стратегии, запустите монитор.

1. Выберите одну из папок Стратегии (DiffServ, IntServ, Запросы сервера—>URI или Число соединений).
2. Щелкните правой кнопкой мыши на стратегии, о которой необходимо собрать данные, и выберите пункт **Отслеживать**.

Ниже приведен пример возможного вывода монитора для определенной выше стратегии.

Рисунок 14. Монитор Quality of Service.



The screenshot shows a window titled "Монитор качества обслуживания" (Quality of Service Monitor). The active strategy is "DiffServ". The table below displays the following data:

Имя стра..	Ограничение средн..	Ограничение ра..	Ограничение пи..	Профильных па..	Профильны..	Внепрофильны..	Активных соедин
First	16 КБ/с	100КБ	512 КБ/с	381	1458 КБ	101683КБ	104

Найдите поля, в которых указывается собранная информация о потоке данных. Просмотрите значения следующих полей: общее число бит, число профильных бит, число профильных пакетов и число внепрофильных бит. Значение в поле Число внепрофильных бит указывает на случаи, когда параметры потока данных превышают значения, определенные в стратегии. В стратегии дифференцированного обслуживания параметр внепрофильных данных указывает число удаляемых байт. Число профильных пакетов указывает, сколько байт было обработано с помощью этой стратегии (начиная с момента отправки пакета и до момента создания данного вывода монитора).

Важную роль играет также значение, заданное в поле Средняя скорость передачи маркеров. При превышении этого ограничения сервер начинает удалять пакеты. В результате, растет число внепрофильных бит. Это означает, что стратегия работает в соответствии с заданными параметрами. Для изменения числа внепрофильных бит скорректируйте ограничения производительности. Описание всех полей монитора приведено в разделе Монитор.

Шаг 5: Измените значения, если это необходимо

После сбора данных можно изменить любые из заданных ранее значений. Щелкните на имени класса обслуживания, созданного в стратегии. Выберите пункт **Свойства** и настройте значения, управляющие потоком данных, в окне диалога Свойства QoS.

Шаг 6: Повторите сбор данных о стратегии

Проверив результаты, опытным путем найдите оптимальные ограничения для вашей сети. <<

Трассировка приложений TCP

Трассировка QoS позволяет работать с функциями трассировки и просматривать текущее содержимое буфера трассировки. Для запуска трассировки сервера введите команду TRTSCPAPP. Ниже приведен пример выбранных параметров трассировки:

```
Приложение TCP/IP.....> *QOS
Опция трассировки.....> *ON
Буфер трассировки.....> *APP
Действие при заполнении.....> *WRAP
Список аргументов.....> 'lv1=4'
Тип трассировки QoS.....> *ALL
```

Приведенная ниже таблица содержит возможные значения параметров трассировки. Если параметр не показан в списке, то его следует указывать непосредственно в команде. Например, TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i').

Параметры	Возможные значения
Приложение TCP/IP	QOS
Опция трассировки	*ON, *OFF, *END, *CHK
Буфер трассировки (См. 54) (MAXSTG)	1-16000, *APP
Действие при заполнении (См. 54) (TRCFULL)	*WRAP, *STOPTRC
Список аргументов (См. 54) (ARGLIST)	Уровни: 'l=1', 'l=2', 'l=3', 'l=4' Содержимое: 'c=a', 'c=i', 'c=d', 'c=m', 'c=r', 'c=s'
Тип трассировки QoS	*ALL

Интерпретация результатов трассировки рассмотрена в разделе Чтение вывода трассировки. На странице вывода трассировки приведен пример вывода с комментариями.

Буфер трассировки

1-16000

Максимальный объем памяти для данных трассировки. При достижении этого размера происходит либо прекращение трассировки, либо возврат к началу буфера. Размер по умолчанию - 4 Мб. Размер по умолчанию задается значением *APP.

*APP

Это значение по умолчанию. Если оно указано, то приложение применяет размер буфера трассировки по умолчанию. Для сервера QoS это значение составляет 4 Мб.

Действие при заполнении

*WRAP

При достижении максимального размера буфера запись вывода трассировки продолжается с начала буфера. Система продолжает запись информации трассировки, заменяя старые записи на новые. Если это значение не выбрано, то при заполнении буфера трассировка прекращается.

*STOPTRC

При заполнении буфера трассировка прекращается.

Список аргументов

Задает уровни регистрируемых ошибок и информацию, заносимую в протокол. Для команды TRCTCPAPP может быть задано два аргумента: уровень и содержимое трассировки. Все атрибуты этих параметров должны быть заключены в одну пару кавычек. Например, TRCTCPAPP 'l=1 c=a'

Примечание: Уровни трассировки вложены друг в друга. Это означает, что выбор какого-либо уровня автоматически означает выбор и всех предыдущих уровней. Например, при выборе уровня 3 автоматически будут выбраны также уровни 1 и 2. **Уровни трассировки**

Уровень 1: Системные ошибки (SYSERR)

В протокол будут заноситься системные ошибки. При возникновении таких ошибок сервер QoS не может продолжать работу. Примерами системных ошибок могут служить нехватка системной памяти или нарушение взаимодействия с TCP/IP.

Уровень 2: Ошибки объектов (OBJERR)

В протокол будут заноситься ошибки, связанные с кодом сервера QoS. Например, к ошибкам объектов относится случай, когда сервер получает непредвиденный результат выполнения какой-либо операции. Обычно это серьезная ошибка, о которой следует сообщить в сервисный центр.

Уровень 3: Определенные события (EVENT)

В протокол будут заноситься все операции QoS. Например, в протокол событий будут заноситься команды и запросы. На этом уровне выдается примерно такая же информация, что и при ведении протокола QoS.

Уровень 4: Трассировка сообщений (TRACE)

Трассируются все данные, передаваемые на сервер QoS и от него. Этот уровень трассировки позволяет получить все данные, которые могут пригодиться при устранении неполадок. Эта информация позволяет определить, где произошла ошибка и как ее можно воспроизвести.

Содержимое трассировки

Примечание: Можно указать только один тип содержимого. Если тип содержимого не указан, то по умолчанию отслеживаются все типы содержимого.

Content = All ('c=a')

Трассируются данные обо всех функциях сервера QoS. Это значение по умолчанию. Оно обычно применяется для первоначального поиска причины неполадки.

Content = Intserv ('c=i')

Трассируются только данные об операциях IntServ. Это значение применяется в случае, когда известно, что неполадка связана с функциями IntServ.

Content = Diffserv ('c=d')

Трассируются только данные об операциях DiffServ. Это значение применяется в случае, когда известно, что неполадка связана с функциями DiffServ.

Content = Monitor ('c=m')

Трассируются только данные об операциях монитора.

Content = Rate ('c=r')

Трассируются только события, связанные с числом поступающих запросов на установление соединения.

Content = Server ('c=s')

Трассируются все данные, кроме информации об операциях монитора. Информация об операциях монитора обычно очень объемна и может затруднить интерпретацию остальных данных трассировки.

Более подробная информация о команде TRCTCPAPP приведена в Описании команды TRCTCPAPP (Трассировать приложение TCP/IP) в разделе Команды CL.

Чтение вывода трассировки

Этот раздел не содержит описания всех аспектов чтения вывода трассировки. Здесь рассмотрены лишь ключевые события, на которые следует обратить внимание в информации трассировки.

Для **стратегии интегрированных служб** наиболее важное событие - это отказ в установлении соединения RSVP из-за отсутствия соответствующей стратегии. Пример сообщения об успешном выполнении операции:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Найдено имя действия vreStn1_kraMoN1CvreStn1 для потока[сеанс=x.x.x.x:y:z:s, источник=x.x.x.x:y]
```

Пример сообщения об отказе в установлении соединения интегрированных служб:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Невозможно найти имя действия для потока [сеанс=x.x.x.x:y]
```

Для **стратегии дифференцированных служб** наиболее важны сообщения о загрузке сервером правила стратегии и сообщения об ошибках в файле конфигурации стратегии.

Пример:

```
01/11 14:07:52 [376,57] TRCE :.....KernelAddPolicyRule: Установка правила = timed_42ring.  
01/11 14:07:52 [376,57] EVNT :.....create_tcp_resv: Отсутствует значение  
DiffServInProfilePeakRate в файле конфигурации, по умолчанию принято 100000 00.  
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: Create resv - bRate: 537395 5722SS1 V5R1M0  
010525 TRCTCPAPP Output RS004 Date-01/11/01 Time-14:08:03 Page-6  
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: bDepth: 32768  
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: peakR: 10000000  
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: m: 128  
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: M: 41452  
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: mark(TOS): a0  
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: flags: 15  
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: flowspe.form = 1, QOS_FORMAT_DS = 1
```

Кроме того, сообщения могут указывать на неправильные теги в файле конфигурации стратегии. Ниже приведены примеры таких сообщений:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Неизвестный атрибут %s в ServicePolicy-  
Игнорируется. 12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Неизвестный атрибут %s в Priority  
Mapping-Игнорируется.
```

Примечание: Символ % обозначает переменную, содержащую нераспознанный тег.

Связанная информация по QoS

Помимо данного, существует множество других источников информации о функции Quality of Service. В частности, общие сведения о QoS можно получить из последних документов RFC, официальных информационных документов, руководств по выполнению задач (Redbooks^(TM)) и т.п. Ниже приведены некоторые рекомендуемые источники:

Публикации других фирм

RFC 1349 

В этом документе RFC рассмотрено новое определение поля TOS в заголовке IP-пакета.

RFC 2205 

Этот документ RFC содержит определение протокола RSVP.

RFC 2210 

Этот документ RFC содержит информацию о применении протокола RSVP с интегрированными службами IETF.


RFC 2474 

Этот документ RFC содержит определение поля Дифференцированные службы (поле DS).

RFC 2475 

В этом документе RFC рассмотрена архитектура дифференцированных служб.

Руководства по выполнению задач фирмы IBM^(R)

TCP/IP More Cool Things than Ever 

Это руководство содержит примеры сценариев и возможных конфигураций. Здесь приведена информация о планировании, установке и настройке TCP/IP на сервере iSeries, а также об устранении неполадок. Несмотря на отсутствие отдельного раздела, посвященного Quality of Service, здесь приводятся сведения о сервере каталогов LDAP.

TCP/IP Tutorial and Technical Overview 

Это руководство содержит общую и справочную информацию о комплексе протоколов и приложений TCP/IP. Информация о Quality of Service приведена в разделе *Part 3. Advanced concepts and new technologies* главы 22.

Связанные разделы iSeries Information Center

Службы каталогов (LDAP)

Этот раздел содержит общую информацию о сервере каталогов, а также сведения о настройке, управлении и устранении неполадок. Раздел Службы каталогов также содержит ссылки на дополнительные источники информации о настройке сервера каталогов.



Напечатано в Дании