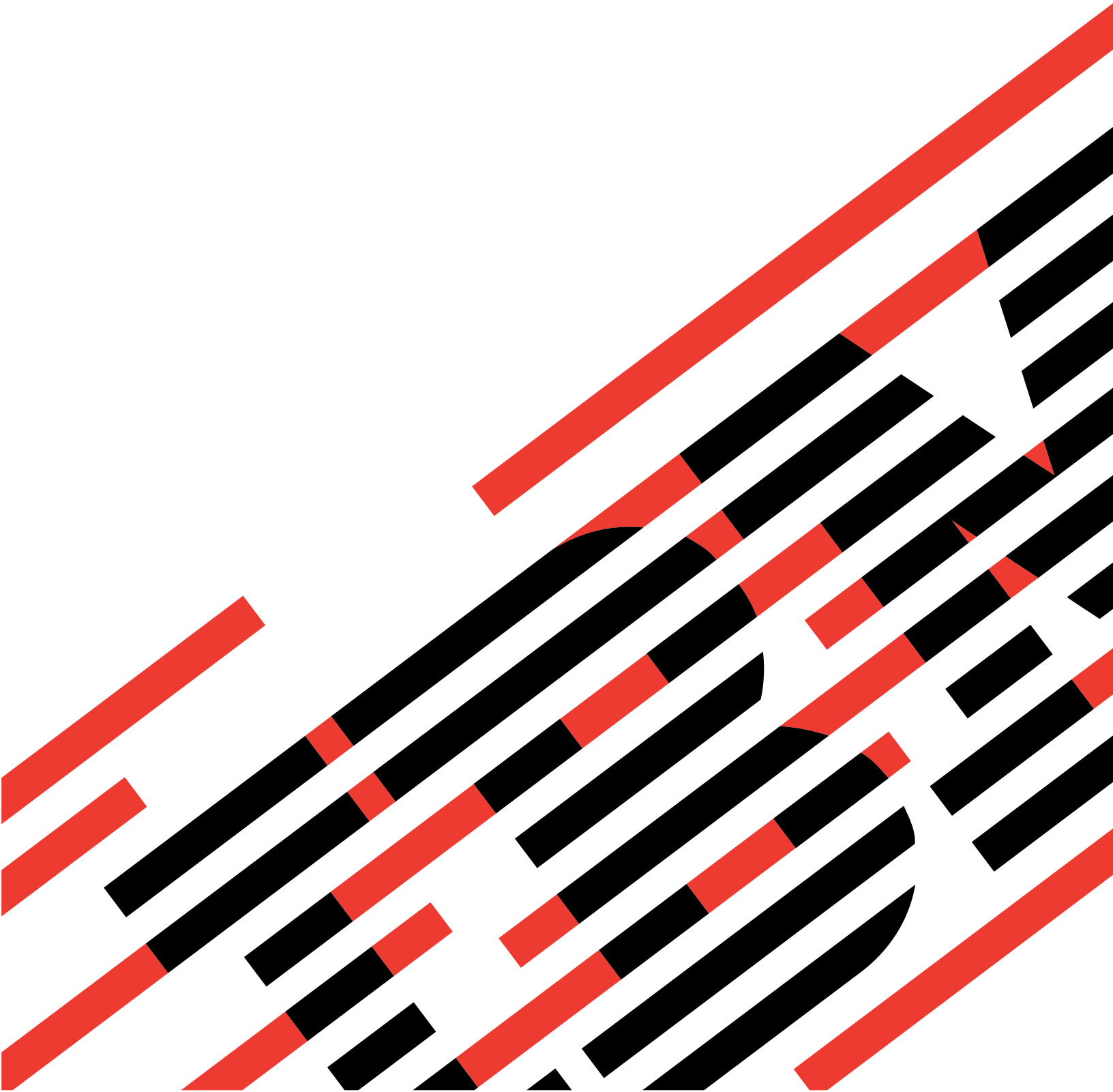
IBM

eserver

iSeries

服务质量



IBM

@server

iSeries

服务质量

目录

服务质量（QoS）

网络中的所有流量都具有同等优先级。非关键浏览器流量被认为与关键商业应用程序同样重要。如果您的首席执行官（CEO）使用音频／视频应用程序进行讲演，IP 信息包优先级就变得很重要。讲演期间，此应用程序接收比其它应用程序更高的性能，这一点至关重要。

QoS 允许您为 TCP/IP 应用程序请求网络优先级和带宽。如果您发送需要可预测且可靠的结果的应用程序（如多媒体），信息优先级对您非常重要。

在开始计划策略规则之前了解 QoS 很重要。以下链接提供实现 QoS 所需要的信息。

V5R2 有哪些新增内容?
列示服务质量联网功能的更改和信息中心主题。

打印本主题
打印本整个主题。

QoS 方案
查看某些 QoS 策略方案，以了解使用 QoS 的原因和方法。

QoS 概念
如果您不熟悉服务质量，则查看某些基本的 QoS 概念和机制。这使您对 QoS 如何工作以及 QoS 机制如何一起工作有一个大概的了解。

计划 QoS
链接至要有效使用 QoS 而需要知道的计划顾问程序和网络信息。

配置 QoS
遵循这些过程来创建新的区分服务策略和集成服务策略。

管理 QoS
遵循这些过程来编辑现有的策略。这些文章告诉您在哪里查找有关删除、跟踪和使用其它策略管理技术的实际任务。

QoS 故障诊断
使用此故障诊断部分帮助您调试 QoS 问题。

QoS 的相关信息
查找其它有用 QoS 源的链接。有许多其它书籍、Web 站点、请求注释文件（RFC）和白皮书。

V5R2 中有哪些新增内容?

本文描述为“版本 5 发行版 2”添加的新功能。它也突出该主题的某些设计改进。

新功能

- **使策略与本地接口相关联**
  可以使策略与 iSeries(TM) 上的某个特定的本地接口或某个范围内的本地接口相关联。指定本地接口使不同策略能够基于客户机信息包到达的那个接口。
- **使策略与多个客户机相关联**
  现在可以使一个策略与多个客户机相关联。这使您能够创建更灵活的策略定义。

- **入站许可策略**
  现在可以创建策略来控制尝试访问您的服务器的外部流量。有两种新的向导使您能够控制流量，该流量尝试访问您的网络中的特定 IP 地址或 URI 值。使用以上链接来了解关于两种入站策略的更多信息。
- **可以存储和打印监控器信息**
  现在可以保存和打印监控器信息。保存信息时，将可以访问该信息供将来参考。如果要打印监控器信息，现在可以指定 “导出为 HTML”。
- **在 LDAP 目录服务器中存储的策略**
  现在策略导出到具有最新 LDAP 协议版本 3 的目录服务器。使用目录服务器使您的 QoS 解决方案更易于管理。与在每个服务器上配置相同的 QoS 策略相反，您可以配置您的服务器来使用单个服务器创建的策略数据。然后将策略保存到目录服务器中。使用此链接来获取关于配置的更多详细信息。
- **调度更改**
  调度是由时间范围定义的。在过去，时间范围必须存在于同一天中。现在，时间范围可以跨任何 24 小时时间段，即使它覆盖几天。使调度与策略相关联来指定策略何时应该是活动的。这使您能够创建更灵活的策略定义。

新的设计改进

- **QoS 计划顾问程序**
  已更新 QoS 计划顾问程序，以便在配置策略之前给予您建议和先决条件。使用它使概念在组织的位置中组合在一起来帮助进行计划。
- **新的入站方案**
  添加了新的方案来显示入站策略实现示例。

如何查看新增内容或更改的内容

为了帮助您查看作了技术更改的位置，此信息使用:

- 图像来标记新增或更改的信息开始的位置。
- 图像来标记新增或更改的信息结束的位置。

要查找关于此发行版的新增或更改的其它信息，参见用户备忘录 。

打印本主题

要查看或下载 PDF 版本，选择服务质量（大约 378 KB 或 53 页）。

要在工作站上保存 PDF 以进行查看或打印:

1. 在浏览器中打开该 PDF（单击以上链接）。
2. 在浏览器的菜单中，单击**文件**。
3. 单击**另存为...**
4. 导航至要保存该 PDF 所在的目录。
5. 单击**保存**。

如果需要 Adobe Acrobat Reader 来查看或打印这些 PDF，可以从 Adobe Web 站点 下载副本。

QoS 方案

了解服务质量的最佳方法之一是在整个网络图片上查看功能如何工作。以下基本示例显示为何要使用服务质量策略。

方案: 专用传送（IP 电话）
如果需要专用传送并要请求预订，则使用集成服务策略。可以创建两种类型的集成服务策略: 保证和受控负载。在此示例中，我们使用保证服务。

方案: 限制浏览器流量
可以使用 QoS 来控制流量性能。使用区分服务策略来限制或扩展网络内应用程序的性能。

方案: 限制入站连接
如果需要控制对服务器作出的入站连接请求，使用入站许可策略。

方案: 可预测的 B2B 流量
如果需要可预测的传送并仍需要请求预订，则也使用集成服务策略。但是，此示例使用受控负载服务。

方案: 安全和可预测的结果（VPN 和 QoS）
如果正在使用虚拟专用网络（VPN），仍可以创建服务质量策略。此示例显示两种类型正一起使用。

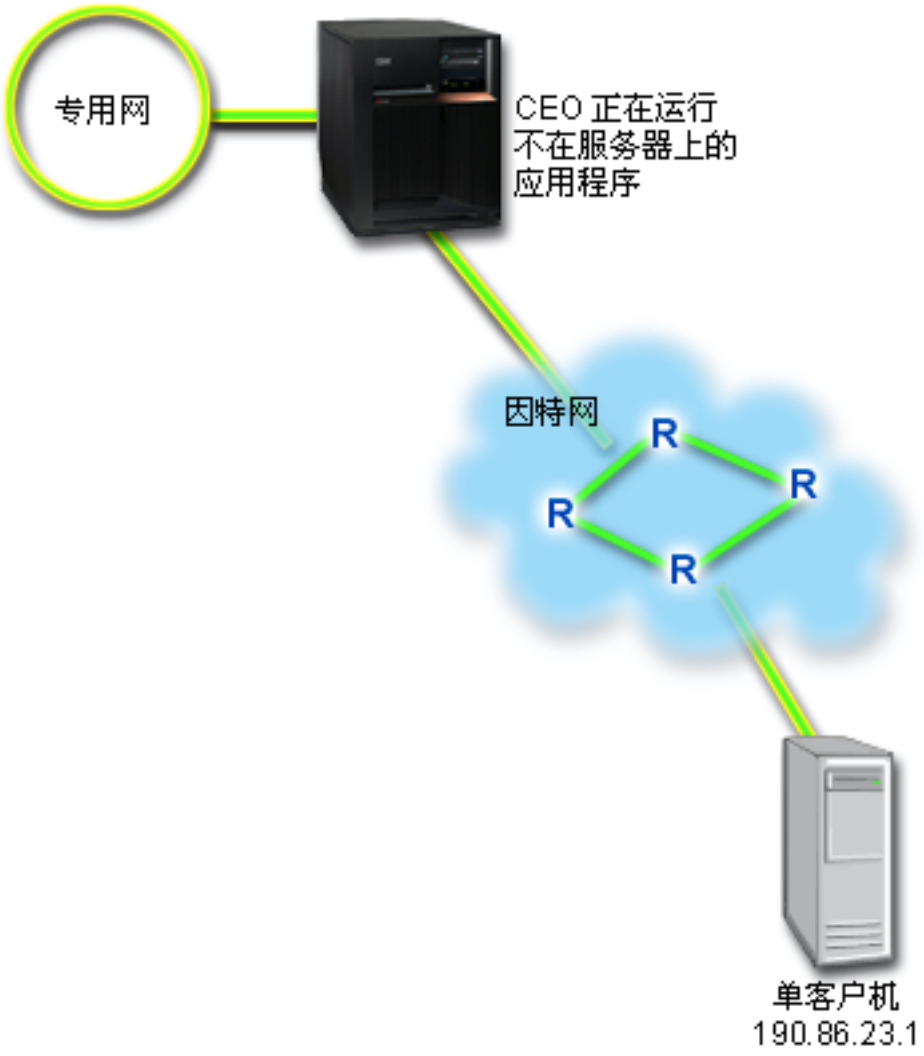
注意: IP 地址和图表是虚构的，仅用于示例的目的。

QoS 方案: 专用传送（IP 电话）

问题

公司的首席执行官（CEO）要在下午 1:00 至下午 2:00 在整个国家对客户机进行实况广播。必须保证 IP 电话将具有保证带宽，以便在广播期间不会中断。在此方案中，应用程序驻留在服务器上。下图说明了此方案中的网络设置。iSeries 服务器在 OS/400(R) V5R2 上运行。

图 1. 通过集成服务策略保证的 CEO 对客户机的讲演。



解决方案

极端敏感的应用程序需要保证连接。因为 CEO 正在使用的应用程序需要平稳且不间断的传送，所以您决定使用保证集成服务策略。保证服务控制最大入队延迟，以便延迟信息包的时间将不会超出指定的时间量。

因为要保证此连接，所以您可以使用具有有保证服务的集成服务策略。集成服务策略需要启用了 RSVP 的应用程序。因为您的服务器不具有启用了 RSVP 的应用程序，所以必须编写您自己的启用了 RSVP 的应用程序。要编写自己的应用程序，使用资源预订设置协议（RAPI）API 或 qtoq QoS 套接字 API。

集成服务策略也要求在流量所经之路径上的路由器启用了 RSVP。有关更多信息，参见集成服务概念一节。

配置

1. 在“iSeries 导航器”中打开 QoS。
    1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
    2. 右键单击**服务质量**并选择**配置**。
    3. 展开**出站带宽策略**。

4. 右键单击 **IntServ** 并选择**新建策略**。 “新建 IntServ 策略”向导出现。

2. 创建集成服务策略。

   第一步是完成集成服务策略向导。因为要保证来自首席执行官（CEO）的流量，可以将该策略称为 **CEO_guaranteed**。单个客户机在 IP 地址 **190.86.23.1** 上接收此讲演。这是仅用于示例目的的虚构数字。可以将此客户机命名为 **Branch1**。因为此流量流过端口 2427，所以可以将应用程序命名为**端口 2427**。可以将调度表命名为 **1:00-2:00**。在向导中使用下列值:

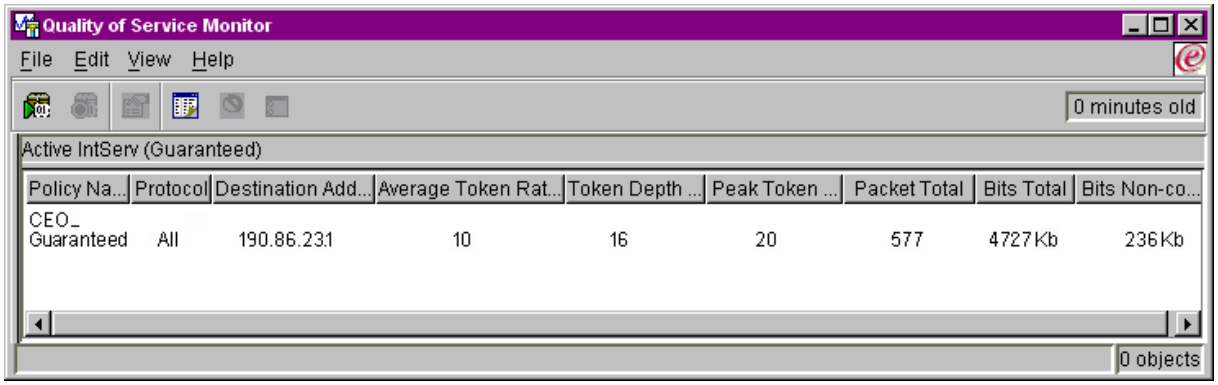
   名称 = CEO_guaranteed
   客户机 = Branch1
   应用程序 = 端口 2427（如果它是 IP 电话所流过的端口）
   本地 IP 地址 = 10.5.27.1
   协议 = TCP
   调度表 = 1:00-2:00
   令牌桶大小 = 16 千位
   带宽限制（R） = 每秒 10 兆位
   流数 = 1

   “iSeries 导航器”列示您的服务器上创建的所有集成服务策略。

4. 使用监控器来验证策略是否在起作用。
   1. 选择特定的“策略”文件夹（DiffServ、IntServ、服务器请求 —> URI 或连接速率）。
   2. 右键单击您要监控的策略并选择**监控器**。

   以下是监控器输出对话，带有注释来帮助解释结果。

   图 2. 服务质量监控器。



   最引人关注的字段是从流量中获取数据的评测字段。这些字段包括总位数、符合要求的位数和符合要求的信息包数。不符合要求的位数指示正在延迟或删除其它流量以满足此集成服务策略的需要。有关所有监控器字段的描述，参见监控器一节。

3. 修改需要调整的任何值。

   查看此策略之后，可以修改先前用此向导创建的值。
   1. 关闭监控器。
   2. 右键单击以上创建的策略名称。

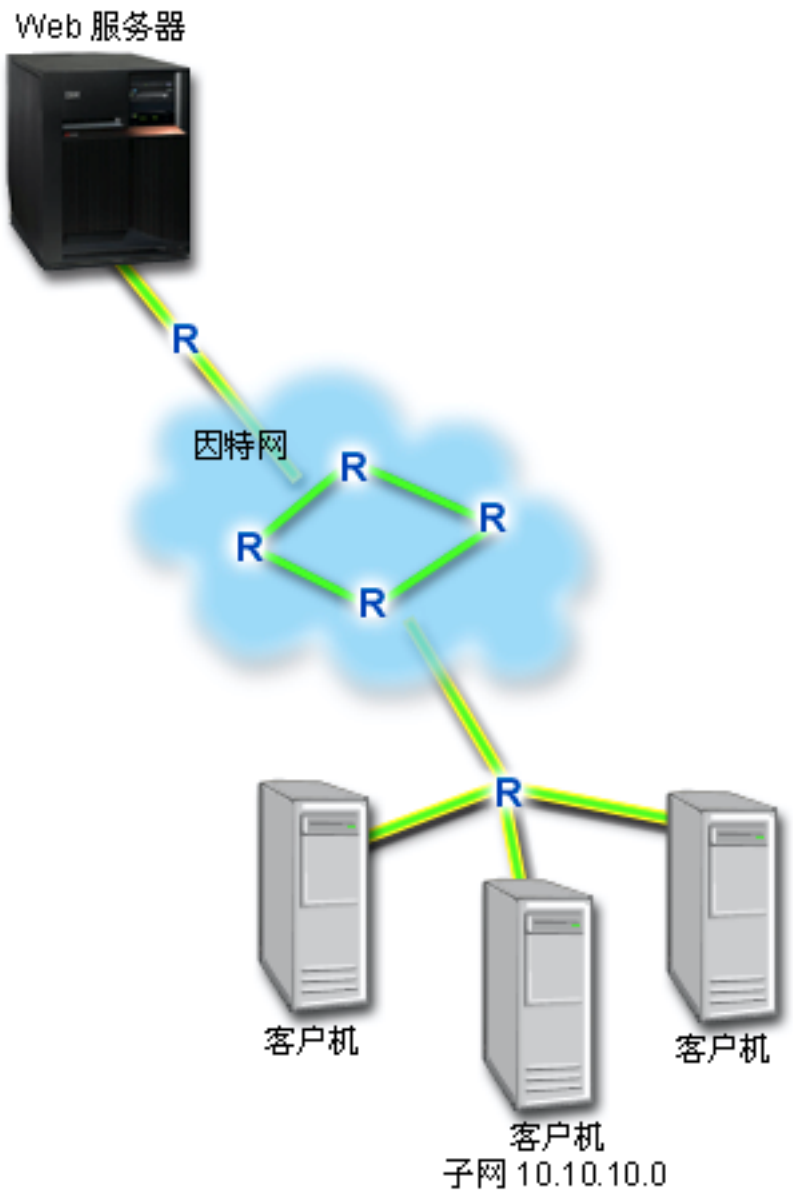
3. 选择**特性**，出现“IntServ_Guaranteed 特性”对话框。
4. 选择**流量控制**选项卡来更改控制流量流的值。这也是您编辑调度表、客户机、应用程序和流量管理的地方。

QoS 方案：限制浏览器流量

问题

公司在星期五一直有来自“以用户为中心的设计”（UCD）组的高级浏览器流量。此流量一直在妨碍会计部门，会计部门在星期五也需要记帐应用程序的良好性能。您决定限制来自 UCD 组的浏览器流量。下图说明了此方案中的网络设置。iSeries 服务器正在 OS/400(R) V5R2 上运行。

图 3. 限制客户机的浏览器流量的 Web 服务器。



解决方案

要限制网络以外的浏览器流量，可以创建区分服务策略。区分服务策略将您的流量划分为类。对此策略内的所有流量指定一个代码点。此代码点告知路由器如何处理流量。在此方案中，将对策略指定一个较低的代码点值来影响网络区分浏览器流量优先顺序的方式。

配置

1. 在“iSeries 导航器”中打开 QoS。
    1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
    2. 右键单击**服务质量**并选择**配置**。
    3. 展开**出站带宽策略**。

4. 右键单击 **DiffServ** 并选择**新建策略**。出现“新建 DiffServ 策略”向导。

2. 创建区分服务策略。

   因为要限制“以用户为中心的设计”（UCD）组的浏览器流量，所以可以将该策略称为 **UCD**。客户机使用 **10.10.10.0** 的子网地址。这是仅用于示例目的的虚构数字。Web 流量一般流经端口 80，所以可以将应用程序命名为**端口 80**。因为拥塞仅在星期五发生，可以将上午 9:00 到下午 5:00 调度表应用于此策略。可以将它命名为 **Friday9-5**。在向导中使用以下设置:

   名称 = UCD（可以是您指定的任何名称）
   客户机 = 子网 10.10.10.0
   应用程序 = 端口 80（HTTP 流量的已知端口）
   协议 = TCP
   调度表 = Fridays9-5

   通过“服务类”向导输入其余策略信息，当您继续时，该向导将自动出现。

   令牌桶大小 = 8 千位
   平均速率限制 = 每秒 10 兆位
   最大速率限制 = 每秒 20 兆位
   概要文件外流量溢出处理 = 删除信息包（重新传送）

   “iSeries 导航器”列示您的服务器上创建的所有区分服务策略。完成向导之后，策略列示在右窗格。

3. 完成新的服务类。

   完成该向导时，需要指定逐跳行为、性能限制以及概要文件外流量处理。这在服务类中定义。

   服务类实际上确定此流量从路由器接收到的性能级别。可以将服务类命名为 **Bronze**，以显示此流量接收较低的服务。“iSeries 导航器”列示您的服务器上定义的所有服务类。

   服务类名 = Bronze

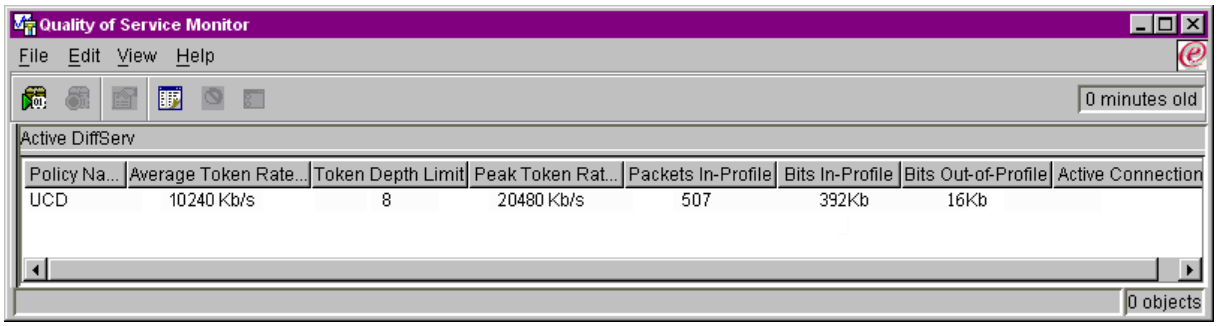
4. 使用监控器来验证策略是否在起作用。

   要验证策略的行为是否符合您在策略中配置的行为，使用监控器。

   1. 选择特定的“策略”文件夹（DiffServ、IntServ、服务器请求 —>URI 或连接速率）。
   2. 右键单击您要监控的策略并选择**监控器**。

   以下是监控器输出对话，带有注释来帮助解释结果。

   图 4. 服务质量监控器。



最引人关注的字段是从流量中获取数据的字段。确保检查总位数、概要文件内位数和概要文件内信息包数字段。概要文件外位数指示流量何时超过配置的策略值。在区分服务策略中，概要文件外数字指示正删除的位。概要文件内信息包数指示此策略控制的位数（从启动信息包的时间到当前监控器输出）。

在平均速率限制字段中所指定的值也很重要。当信息包超过此限制时，服务器将开始删除它们。因此，概要文件外位数将增加。这显示策略的行为与为它配置的行为相同。有关所有监控器字段的描述，参见监控器一节。

5. 更改不适用于此策略的任何值。

   可以修改在策略中创建的任何值。

   1. 关闭监控器。
   2. 在左窗格中选择“服务类”。
   3. 在右窗格中，右键单击以上创建的服务类名称。
   4. 选择**特性**。“CoS 特性”对话框出现，其中包含控制流量的值。修改适当的值。

«

QoS 方案: 限制入站连接

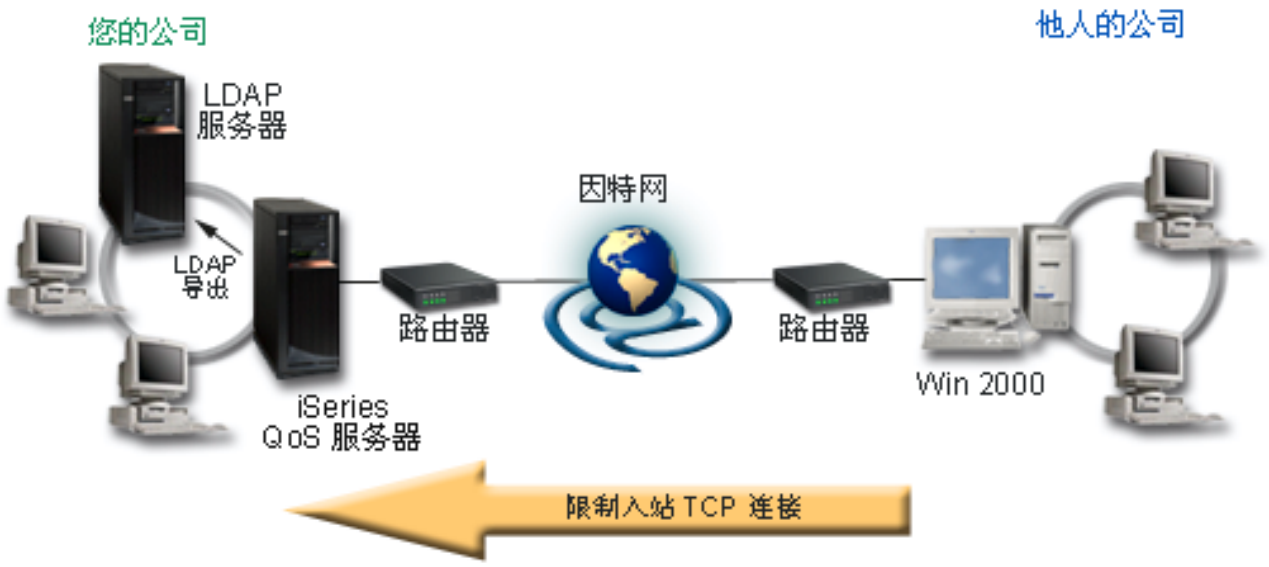
»

问题

进入网络的客户机请求正使 Web 服务器的资源过载。要求您减慢至本地接口 10.1.1.1 上的 Web 服务器（10.1.1.4）的入局 HTTP 流量的速度。根据与服务器的连接属性（例如，IP 地址），QoS 可以帮助您限制接受的入站连接尝试次数。为了达到这一点，决定实现入站许可策略，该策略将限制接受的入站连接数。

该图显示您的公司和一个客户公司。此 QoS 策略只能在一个方向上控制流量流。

图 5. 限制入站 TCP 连接。



先决条件:

- 正运行 iSeries V5R2
- 已配置并正运行 LDAP 服务器

解决方案

要配置入站策略，必须决定是将流量限制于本地接口还是特定应用程序，以及是否从特定客户机限制它。在此情况下，您需要创建一个策略，该策略限制从 Their_Company 转至您的本地接口 10.1.1.1 上端口 80（HTTP 协议）的连接尝试次数。由于您通过 IP 地址定义此限制，所以您应该创建“连接速率”策略。有两种类型的入站许可策略: “连接速率”和“服务器请求”（URI）。URI 策略限制尝试访问特定相对 URI 名称（类似于相对 URL）或您的系统中的所有 URL 的连接次数。如果需要关于 URI 策略的更多信息，参见 入站许可策略。

要创建此连接速率策略并完成以上方案，打开“iSeries 导航器”并转至 QoS 功能。

配置

1. 在“iSeries 导航器”中打开 QoS。
    1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
    2. 右键单击**服务质量**并选择**配置**。
    3. 展开**入站许可策略**。
    4. 右键单击**连接速率**并选择**新建策略**。
2. 完成“连接速率策略”向导。

    第二个步骤是完成“新建连接速率策略”向导。由于要限制来自 Their_Company 的流量，所以可以将该策略称为 **Restrict_TheirCompany**。您要限制从客户机 Their_Company 对您的本地 IP 地址 10.1.1.1 所作的请求。这是一个仅用于示例目的的虚构数字。由于此流量流经端口 80，所以可以将应用程序命名为**端口 80**。可以将调度表命名为 **Weekdays(9-5)**。在向导中使用下列值:

名称 = Restrict_TheirCompany
客户机 = Their_Company
应用程序 = 端口 80
本地 IP 地址 = 10.1.1.1
调度表 = Weekdays (9-5)
平均连接速率 = 每秒 100
连接脉冲串传输速率 = 5 个连接
优先级 = 中

“iSeries 导航器”列示在您的服务器上创建的所有连接速率策略。

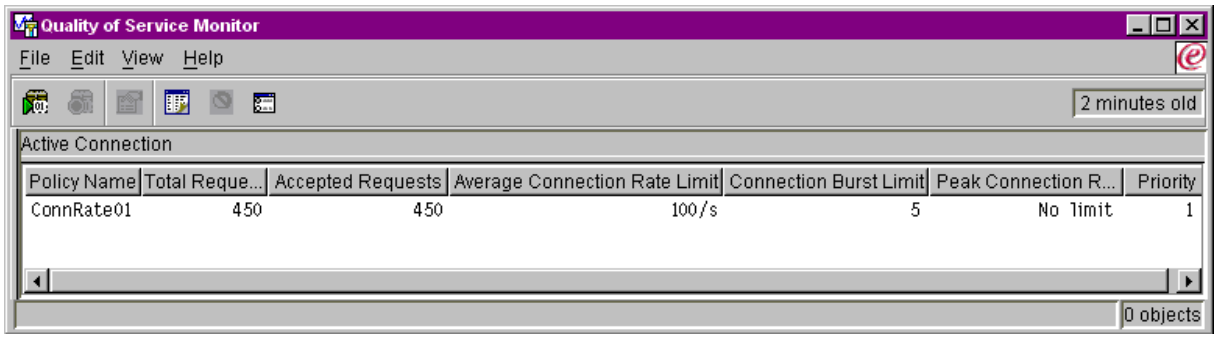
3. 监控此策略中包含的流量，以确保您看到期望的结果。

   要验证策略的行为是否与为它配置的行为相同，使用监控器。

   1. 选择特定的“策略”文件夹（DiffServ、IntServ、服务器请求 —>URI 或连接速率）。
   2. 右键单击要监控的策略并选择**监控器**。

   以下是监控器输出图，带有注释来帮助解释结果。

   图 6. 服务质量监控器。



   确保检查任何测量的字段，如接受的请求、删除的请求、总请求和连接速率。删除的请求将指示流量何时超过已配置的策略值。接受的请求指示此策略控制的位数（从启动信息包的时间到现在监控器输出）。

   指定给平均连接请求速率字段的值也很重要。当信息包超过此限制时，服务器将开始删除它们。因此，删除的请求将增加。这显示策略的行为与为它配置的行为相同。有关所有监控器字段的描述，参见监控器一节。

4. 如果需要修改任何值，在特性面板中更改它们。

   关闭监控器。**右键单击** Restrict_TheirCompany 策略并选择**特性**。这些面板允许您编辑策略的特性。这也是您编辑调度表、客户机、应用程序和流量管理的地方。

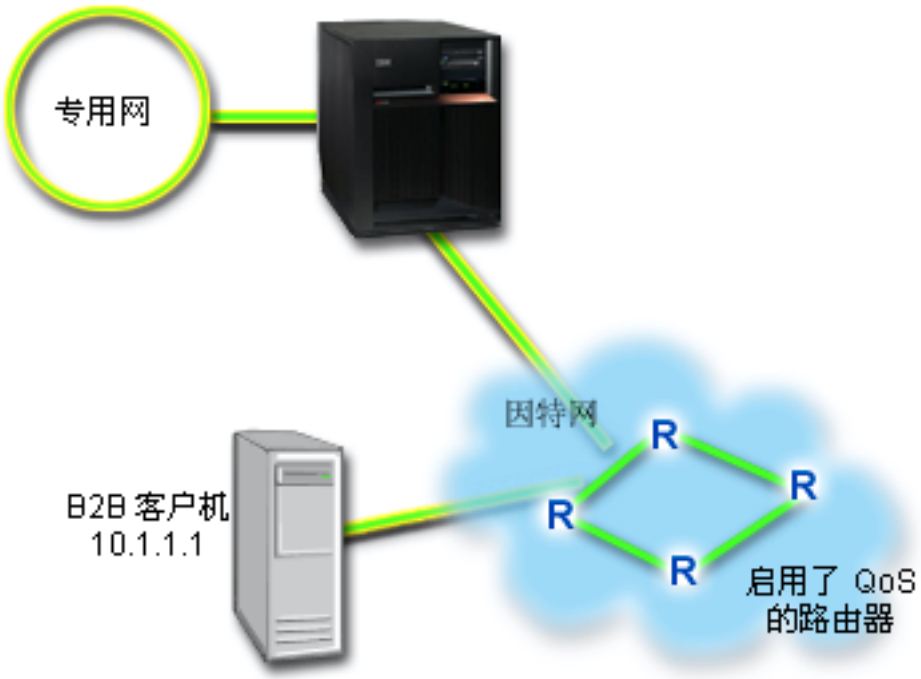
QoS 方案: 可预测的 B2B 流量

问题

销售部门报告网络流量不按预期执行的问题。公司的 iSeries 服务器驻留在需要可预测的电子商务服务的企业到企业（B2B）环境中。您需要对客户提供可预测的交易。您要在工作日的最忙期间（上午 10 点到下午 4 点）对销售单元的订购应用程序给予较高服务质量。

在下图中，销售小组在专用网内。沿流量到 B2B 客户机的路径上有启用了 RSVP 的路由器。每个 R 代表流量路径上的一个路由器。

图 7. 使用启用了 RSVP 的路由器的对于 B2B 客户机的集成服务策略。



解决方案

受控负载服务支持对拥塞网络高度敏感但容忍少量丢失和延迟的应用程序。如果应用程序使用受控负载服务，则当网络负载增加时，它的性能将不能满足要求。将为流量提供类似负载较轻条件下网络中的正常流量的服务。因为此特定应用程序容忍某些延迟，所以您决定通过受控负载服务使用集成服务策略。

集成服务策略需要启用了 RSVP 的应用程序。因为服务器不具有启用了 RSVP 的应用程序，您必须编写您自己的启用了 RSVP 的程序。要编写自己的应用程序，使用资源预订设置协议（RAPI）API 或 qtoq QoS 套接字 API。

集成服务策略还需要沿流量路径上的路由器是启用了 RSVP 的。有关更多信息，参见集成服务概念部分。

配置

1. 在 “iSeries 导航器” 中打开 QoS。
    1. 在 “iSeries 导航器” 中，展开服务器 —> **网络 —> IP 策略**。
    2. 右键单击**服务质量**并选择**配置**。
    3. 展开**出站带宽策略**。

4. 右键单击 **IntServ** 并选择**新建策略**。 “新建 IntServ 策略”向导出现。

2. 创建新的集成服务策略。

   因为要给予客户可预测的流量，所以可以将该策略称为 **B2B_CL**。单个客户机在 IP 地址 **10.1.1.1** 上接收此交易。这是一个仅用于示例目的的虚构数字。因为此流量流经 7000 和 8000 之间的各个端口，所以可以将应用程序命名为**端口 7000-8000**。因为此交易在上午 10:00 至下午 4:00 期间发生，所以可以将调度表命名为**黄金时间**。在向导中使用以下设置:

   名称 = B2B_CL
   客户机 =10.1.1.1
   应用程序 = 端口 7000-8000
   协议 = TCP
   调度表 = 黄金时间
   令牌桶大小（b） = 8 千位
   记号速率限制 = 每秒 25 兆位
   令牌桶大小（r） = 75 千位
   流数 = 5

   “iSeries 导航器”列示您的服务器上创建的所有集成服务策略。

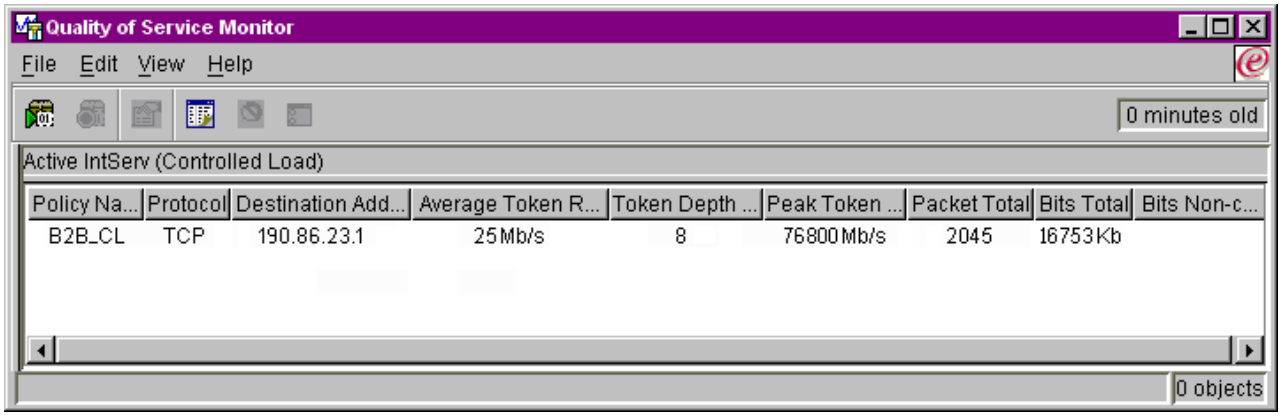
3. 使用监控器来验证策略是否在起作用。

   要验证策略是否在正确地起作用，使用监控器。

   1. 选择特定的“策略”文件夹（DiffServ、IntServ、服务器请求 —> URI 或连接速率）。
   2. 右键单击您要监控的策略并选择**监控器**。

   以下是监控器输出对话，带有注释来帮助解释结果。

图 8. 服务质量监控器。



   最引人关注的字段是从流量中获取数据的字段。确保检查总位数、符合要求的位数和符合要求的信息包字段。不符合要求的位数指示正在延迟或删除其它流量以满足此集成服务策略的需要。有关监控器字段的完整描述，参见监控器一节。

4. 修改此策略中需要调整的任何值。

   创建此策略之后，可以修改先前用此向导创建的值。

1. 关闭监控器。
2. 右键单击以上创建的策略名称。
3. 选择**特性**，出现“B2B_CL 特性”对话框。
4. 选择**流量控制**选项卡来更改控制流量流的值。

这也是您编辑调度表、客户机、应用程序和流量管理的地方。

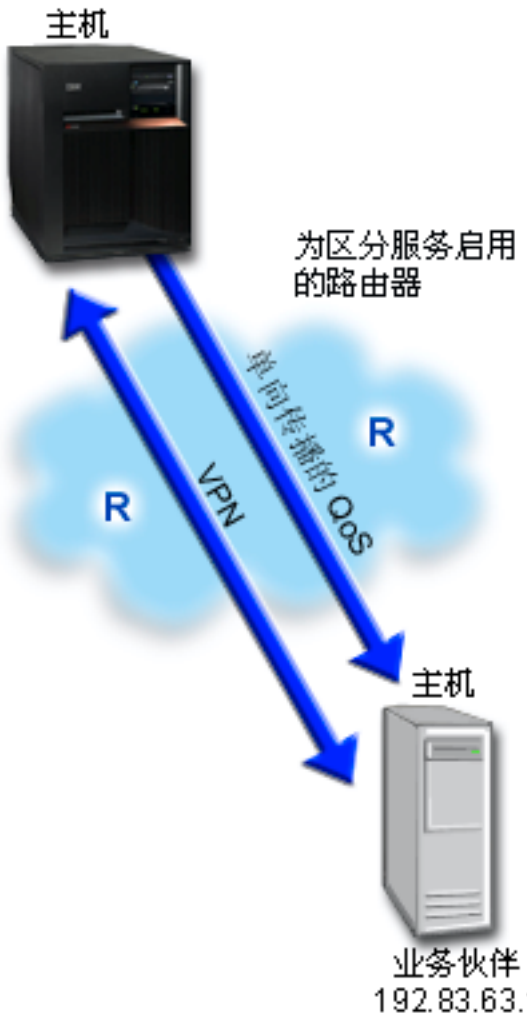
QoS 方案: 安全和可预测的结果（VPN 和 QoS）

问题

您已通过 VPN 连接业务伙伴，且想组合 VPN 和 QoS 来为任务的关键数据提供安全性和可预测的电子商务流。QoS 配置仅朝一个方向传播。因此，如果具有声频 / 视频应用程序，则需要在连接的两端为应用程序建立 QoS。

该图在主机至主机 VPN 连接中显示您的服务器和客户机。每个 R 代表流量所经之路启用了区分服务的路由器。您可以看到，QoS 策略仅朝一个方向流动。

图 9. 使用 QoS 区分服务策略的主机至主机 VPN 连接。



解决方案

使用 VPN 和 QoS 不仅建立保护，还为此连接建立优先级。首先，需要设置主机至主机 VPN 连接。参见主机至主机 VPN 连接示例，以帮助您执行 VPN 配置。一旦具有 VPN 连接的保护，就可以设置 QoS 策略。您可以创建区分服务策略。将对此策略指定一个较高的加速转发代码点值，以影响网络如何对任务的关键流量执行优先级排序。

配置

1. 设置主机至主机 VPN 连接。参见主机至主机 VPN 连接示例，以帮助您执行 VPN 配置。
2. 在“iSeries 导航器”中打开 QoS。
    1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
    2. 右键单击**服务质量**并选择**配置**。
    3. 展开**出站带宽策略**。
    4. 右键单击 **DiffServ** 并选择**新建策略**。出现“新建 DiffServ 策略”向导。

3. 创建区分服务策略。

   由于您要提高 B2B 应用程序的性能，因此您可以将该策略称为 **B2B**。客户机具有单个地址 **192.83.63.1**。这是仅用于示例目的的虚构数字。因为 B2B 流量可以使用任何端口，所以您可以将该应用程序命名为**所有端口**。因为仅在上午 9:00 到下午 5:00 之间会发生拥塞，所以可以将 9-5 调度表应用于该策略。可以将此调度表命名为**第一班**。在向导中使用以下设置:

   名称 = B2B
   客户机 = VPN 客户机
   应用程序 = 所有端口
   协议 = 全部
   调度 = 第一班

   通过“服务类”向导输入其余策略信息，当您继续时，该向导将自动出现。

   令牌桶大小 = 8 千位
   平均速率限制 = 每秒 90 兆位
   最大速率限制 = 不限制
   概要文件外流量溢出处理 = 删除信息包（重新传送）

   “iSeries 导航器”列示您的服务器上创建的所有区分服务策略。

4. 完成新的服务类。

   完成该向导时，将要求您指定服务类。服务类指定性能限制、代码点和概要文件外处理特征。在此策略中，您将要指定高优先级的加速转发代码点。因为要应用加速转发代码点，可以将服务类命名为 **EF_VPN** 来提醒自己为何选择此值。

   服务类 = EF_VPN

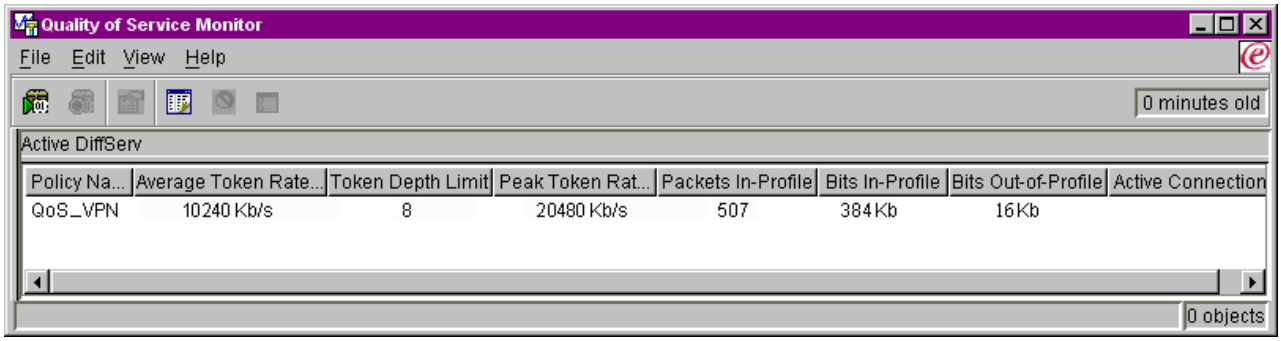
6. 使用监控器来验证策略是否在起作用。

   要验证策略的行为是否与为它配置的行为方式相同，使用监控器。

   1. 选择特定的“策略”文件夹（DiffServ、IntServ、服务器请求 —> URI 或连接速率）。
   2. 右键单击您要监控的策略并选择**监控器**。

   以下是监控器输出图，带有注释来帮助解释结果。

图 10. 服务质量监控器。



与示例 1 类似，最引人关注的字段是从流量中获取数据的字段。这些字段包括总位数、符合要求的位数和符合要求的信息包字段。不符合要求的位数指示流量何时超过配置的策略值。符合要求的信息包数表示由此策略控制的信息包的数量。您在平均速率限制字段中所指定的值很重要。当信息包超过此限制时，服务器将开始删除它们。因此，不符合要求的位数将增加。此策略和示例 1 之间的差别是使用 VPN 协议保护此处的信息包。正如您所见，QoS 的确对 VPN 连接起作用。有关所有监控器字段的描述，参见监控器一节。

5. 修改此策略中需要调整的任何值。

   也可以在创建服务类之后编辑它。

   1. 关闭监控器。
   2. 在左窗格中选择**服务类**。
   3. 在右窗格中，右键单击以上创建的服务类名称。
   4. 选择**特性**。 “CoS 特性”对话框出现，其中包含控制流量的值。修改适当的值。

QoS 概念

服务质量（QoS）术语可以在多个信息源中找到，因此，本主题将仅涉及特别适用于您的 iSeries 服务器的基础内容。

实现服务质量的最重要的部分之一是您的服务器本身。您不仅需要了解以下概念，而且还需要知道您的服务器在实现这些概念中所起的作用。iSeries 服务器只能充当客户机或服务器，而不能充当路由器。当您了解关于以下概念的更多内容并开始计划服务质量时，需要考虑此点。

要实现 QoS，为您的流量创建策略。一个策略是指定一个操作的一组规则。策略主要说明什么客户机、应用程序和调度（您指定的）应该接收特定的服务。您可以最终实现四种策略类型。策略首先分成两种类别：出站带宽和入站接纳。在出站带宽策略中，您可以创建两种服务类型：集成服务策略或区分服务策略。在“入站”接纳策略中，您也可以创建两种服务类型：新建连接请求速率策略和新建 URI 请求速率策略。

入站指控制从某些外面的源进入您的网络的连接请求的策略。出站指限制或有助于尝试离开您的网络的流量的策略。要决定需要使用哪个策略，评估您要使用 QoS 的原因。研究以下概念，以找出对于每种策略类型所适合的情况。

使用下列链接以了解更多信息:

区分服务
这是可以在您的服务器上创建的第一种类型的出站带宽策略。区分服务是 QoS 的一部分，该服务将您的流量分成几类。要实现网络中的服务质量，需要确定要如何将网络流量分类和如何处理不同的类。然后，可以创建服务类来与区分服务策略一起使用。

区分服务类
此子主题说明构成服务类的部件。当创建区分服务策略时，也必须创建服务类。

集成服务
可以创建的第二种类型的出站带宽策略是集成服务策略。集成服务提供 IP 应用程序使用 RSVP 协议请求和预定带宽的能力。集成服务策略使用 RSVP 协议来保证端到端连接。这是可以指定的最高级别的服务；但是，它也是最复杂的。当创建集成服务策略时，将指定两种服务类之一：保证服务或受控负载服务。

使用区分服务标记的集成服务
当集成服务策略可能经过混合的网络环境时，一般使用此类型的策略。混合的网络环境包含启用了 RSVP 的某些网络节点和未启用 RSVP 的某些网络节点。

RSVP 和 QoS API
此子主题描述用来进行集成服务预订的协议和 API。它也讨论使路由器启用 RSVP 的条件。

连接速率
此类型的入站策略用来控制请求允许进入（通过 IP 地址）到您的网络的流量。有两种类型的入站许可策略：连接速率和 URI。此主题描述两种类型的入站策略。

URI
此类型的入站策略用来控制请求允许进入（通过 URI）到您的网络的流量。有两种类型的入站许可策略：连接速率和 URI。此主题描述两种类型的入站策略。

目录服务器
QoS 策略现在导出到目录服务器。查看此主题来了解使用目录服务器的益处、LDAP 概念和配置以及 QoS 模式。

尝试实现 QoS 之前，应该深入研究服务质量并确保此服务将满足您的需要。有关查找附加资源的帮助，参见 QoS 的相关信息页面。 «

连接请求速率和 URI 请求速率

» 入站策略用来控制试图连接至服务器的流量。允许您定义和配置入站控制的策略有两种类型：URI 策略和连接速率策略。这两种策略类型在下面描述。

URI 请求速率策略
URI 请求速率策略是解决方案中帮助防止服务器过载的部分。此类型的策略根据应用程序级别信息应用许可控制以限制服务器接受的 URI 请求。在业界这也称为*基于报头的连接请求控制*，它使用 URI 来设置优先级。

与连接速率策略不同，URI 策略具有更多控制，因为它们检查内容而不仅仅是检查信息包报头。它们检查的内容可以包括 URI 名称或其它应用程序特定信息。对于 iSeries，使用相对 URI 名称来定义策略。例如，**/products/clothing**。下面的示例描述相对 URI。

相对 URI
相对 URI 实际上是绝对 URI（类似于旧的绝对 URL）的子集。考虑此示例:

http://www.ibm.com/software。**http://www.ibm.com/software** 段被认为是绝对 URI。**/software** 段是相对 URI。所有相对 URI 值必须以一个正斜杠（**/**）开头。以下是有效的相对 URI 示例:

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

注意: 缺省协议、主机名和端口全都从 HTTP Server 继承。另外，当您指定 URI 时，存在一个隐式通配符。例如，**/software** 将包括 software 目录中任何内容。

URI 策略被认为是入站策略，因为它们控制进入网络的流量请求。作为此入站控制的一部分，可以指定在策略接受 URI 请求之后处理 URI 请求的优先级。通过确定策略的优先级，您实际上根据每个连接的配置优先级确定队列中连接请求的优先级。

连接速率策略

连接速率策略也是解决方案中帮助防止服务器过载的部分。此类型的策略根据连接级别信息应用许可控制以限制服务器接受的连接。在业界这也称为 *TCP SYN 管制*。

连接速率管制根据您创建的策略中定义的平均每秒建立的连接数和建立的最大连接数（在任何给定的时刻）接受或拒绝新的入局连接。这些连接限制由平均速率限制和脉冲串传输限制组成，iSeries 导航器中的向导将提示您输入这些限制。当入局连接请求到达服务器时，服务器分析信息包报头信息以确定是否在策略中定义了此流量。系统根据连接限制概要文件验证此信息。如果策略未超出策略限制，则将策略置于队列中。废弃不符合策略的信息包。

与 URI 策略类似，连接速率策略被认为是入站策略，因为它们控制进入网络的流量的连接速率。作为此入站控制的一部分，可以指定在策略接受连接之后处理连接的优先级。通过确定策略的优先级，您实际上根据每个连接的配置优先级确定队列中连接请求的优先级。

URI 策略和连接速率策略要求您为每个策略中定义的流量设置连接速率限制和脉冲串传输限制。这些速率限制帮助限制尝试进入服务器的入站连接。平均连接速率指定允许进入服务器的新建连接或接受 URI 请求速率的限制。 «

平均连接速率限制和脉冲串传输限制

» 连接速率限制和脉冲串传输限制通称为速率限制。这些速率限制帮助限制尝试进入服务器的入站连接。在入站许可策略中设置速率限制（URI 和连接速率）。

连接脉冲串传输限制

突发限制大小确定保留连接的突发的缓冲区容量。连接突发进入服务器的速率可能比服务器所能处理的速率或您允许的速率大。如果突发中的连接数目超出所设置的连接脉冲串传输速率，则废弃附加的连接。

平均连接速率

平均连接速率指定允许进入服务器的新建连接或接受 URI 请求速率的限制。如果请求将导致服务器超出所设置的限制，服务器拒绝请求。平均连接请求限制是按每秒连接数测量的。

提示: 要确定要设置的限制，可能要运行监控器。有关参考，参见监控当前网络统计信息以获取将帮助您收集在服务器上传播的大多数数据的样本策略。使用这些结果，可以适当地调整限制。 «

区分服务

区分服务将您的流量划分为类。要在网络中实现服务质量，需要确定如何将网络流量分类和如何处理不同的类。

服务器使用 IP 报头中的位数来标识 IP 信息包的服务级别。路由器和交换机基于 IP 报头的 TOS 字段中的逐跳行为（PHB）信息分配它们的资源。在请求注释文件（RFC）1349 和 OS/400(R) V5R1 中重新定义了 TOS 字段。PHB 是信息包在网络节点上接收的转发行为。由称为代码点的十六进制值表示它。可以在服务器或网络的其它部件（如路由器）标记信息包。为了信息包能保留所请求的服务，必须对每个网络节点启用区分服务。即，设备必须能够执行逐跳行为。要实施 PHB 处理，网络节点必须能够使用队列调度和出站优先级管理。有关启用区分服务的意义的更多信息，参见流量调节器页面。

如果信息包经过未启用区分服务的路由器或交换机，它将丢失它的服务级别。注意：仍会处理信息包，但可能会以意外方式传送它。在 iSeries 服务器上，可以使用标准 PHB 代码点，也可以定义您自己的类。建议不要创建您自己的代码点在专用网外部使用。

与集成服务不同，区分服务流量不需要预订或对每个流进行处理。同等地处理处于相同类的所有流量。

区分服务也用于控制进出服务器的流量。这意味着 iSeries 服务器实际上使用区分服务来限制性能。限制不太关键的应用程序允许任务的关键应用程序首先退出专用网。当创建策略时，要求您在服务器上设置不同的限制。性能限制包含令牌桶大小、最大速率限制和平均速率限制。 “iSeries 导航器” 的 QoS 功能内的帮助主题提供有关这些限制的更多特定信息。

现在，您对有关使用区分服务来将流量分组有了更多的了解。如果您不知道要指定哪些代码点，查看代码点和逐跳行为。如果您仍不知道要使用哪些代码点，则反复试验。创建测试策略，监控这些策略并作出相应的调整。

区分服务类

区分服务节讨论区分服务功能如何将流量按类分组。即使通过设备实现了此功能的大部分，也应控制如何将流量分组以及流量应接收什么优先级。

当实现 QoS 时，将首先定义策略。策略确定谁、什么、何处和何时。然后您必须对策略指定服务类。服务类是单独定义的，且可以由策略重新使用。服务类由逐跳行为、流量限制和服务类中的概要文件外处理组成。

逐跳行为

服务质量使用建议的代码点来将逐跳行为指定给流量。路由器和交换机使用这些代码点来给出流量优先级。服务器不能使用这些代码点，因为它未用做路由器。应基于您的单独网络需要确定要使用哪些代码点。考虑哪些应用程序对您最重要以及应给什么策略指定较高的优先级。最重要的是要与标记一致，以便获得预期结果。这些代码点将是区分流量的不同类的关键部分。

性能限制

服务质量使用性能限制来限制通过网络的流量。通过设置令牌桶大小、最大速率限制和平均速率限制来规定这些限制。有关这些特定值的更多信息，参见令牌桶和带宽限制。

概要文件外处理

服务类的最终部分是概要文件外处理。当您指定以上的性能限制时，应设置限制流量的值。当流量超出这些限制，信息包被认为是概要文件外的。服务类中的此信息告诉服务器是删除、整形还是转发这些概要文件外信息包。如果决定要删除概要文件外信息包，则在指定的时间量之后重新传送它们。如果延迟概要文件外信息包，则将它们整形以符合您定义的处理特征。如果用 “区分服务代码点”（DSCP）重新标记概要文件外信息包，则给它们重新指定一个新代码点。当在向导中指定这些处理指示信息时，单击 “帮助” 以获取更多的特定信息。

代码点和逐跳行为

服务质量使用下列建议的代码点将逐跳行为指定给流量。应该根据个人的网络需要来确定要使用哪些代码点。只有您可以决定哪些代码点模式对您的环境有意义。您需要考虑哪些应用程序对您最重要以及应该指定哪些策略较高的优先级。最重要的事情是与您的记号相符，以便获取期望的结果。

此表显示建议的代码点。也可以创建您自己的逐跳行为。

加速转发	类选择程序	有保证转发
101110	0 类 — 000000	有保证转发，1 类，低 — 001010
	1 类 — 001000	有保证转发，1 类，中 — 001010
	2 类 — 010000	有保证转发，1 类，高 — 001010
	3 类 — 011000	有保证转发，2 类，低 — 010010
	3 类 — 100000	有保证转发，2 类，中 — 010100
	5 类 — 101000	有保证转发，2 类，高 — 010110
	6 类 — 110000	有保证转发，3 类，低 — 011010
	7 类 — 111000	有保证转发，3 类，中 — 011100
		有保证转发，3 类，高 — 011110
		有保证转发，4 类，低 — 100010
		有保证转发，4 类，中 — 100100
		有保证转发，4 类，高 — 100110

加速转发

加速转发是一种类型的区分服务逐跳行为。它主要用来提供网络上的保证服务。加速转发通过保证网络上的带宽给予流量低损失、低抖动和端到端服务。发送信息包之前进行预订。主要目的是避免延迟并及时传送信息包。

注意: 通常接收加速转发处理需要高的成本，因此不建议定期使用此逐跳行为。

类选择程序

类选择程序代码点是另一种类型的区分服务行为。有 7 个类。在类选择程序代码点值中， “0 类”给予信息包最低优先级，而 “7 类”给予信息包最高优先级。这是最普通的一组逐跳行为，因为大多数路由器已经使用类似的代码点。

有保证转发

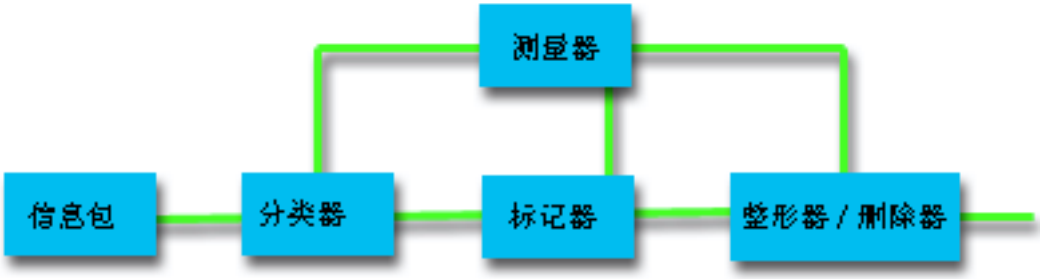
有保证转发分成四个逐跳行为类，每个类具有低、中或高删除优先级别。删除优先级别确定要删除信息包的可能性。每个类有其自己的带宽规范。 “1 类，高”给予策略最低优先级，而 “4 类，低”给予策略最高优先级。低删除级别表示在此特定类级别中此策略中的信息包具有最少的删除机会。

流量调节器

使用服务质量策略的网络设备必需能识别 QoS。这意味着网络设备（如路由器和交换机）必须具有以下性能: 分类器、测量器、标记器、整形器和删除器。这些术语的集合称为*流量调节器*。如果网络设备具有所有流量调节器，则认为它能识别 QoS。

下图显示流量调节器如何工作的逻辑表示。

图 11. 流量调节器



以下信息更详细地描述了每个流量调节器。

分类器
信息包分类器基于信息包的 IP 报头中的内容选择流量流中的信息包。iSeries 服务器定义两种类型的分类器。BA（行为聚集）专门基于区分服务代码点对信息包进行分类。MF（多字段）分类器基于一个或多个报头字段（如源地址、目标地址、区分服务字段、协议标识、源端口号和目标端口号）的组合的值选择信息包。

测量器
流量测量器评测由分类器转发的 IP 信息包是否与流量的 IP 报头概要文件一致。IP 报头中的信息由您在此流量的 QoS 策略中设置的值决定。测量器将信息发送给其它调节功能来触发某个操作。对每个信息包都触发该操作，而不管信息包是在概要文件内还是在概要文件外。

标记器
信息包标记器设置区分服务（DS）字段。它们获取区分服务代码点设置并将它们转换为字节。可以将标记器配置为将所有信息包标记为单个代码点或标记为用于选择逐跳行为的一组代码点。

整形器
整形器延迟流量流中的某些或全部信息包，以使流符合流量概要文件。整形器具有有限的缓冲区大小，如果没有足够的空间来容纳延迟的信息包，则可能会废弃信息包。

删除器
删除器废弃流量流中的某些或全部信息包。这使流符合流量概要文件。

目录服务器概念

» QoS 策略配置存储在 LDAP 目录服务器中。必须使用具有最新 LDAP 协议版本 3 的 LDAP 服务器。

使用目录服务器的益处
使用目录服务器使 QoS 解决方案更容易管理。与在所有服务器上配置 QoS 策略相反，您可以将配置数据存储在一个本地目录服务器上供许多系统共享。但是，并非必须共享数据。将目录服务器与 QoS 配合使用有其它两种方式。

1. 数据仍可以配置、存储并仅由一个系统使用。
2. 配置数据也可以驻留在一个目录服务器上，该目录服务器为其它系统保存数据，但配置数据不一定为其它系统所共享。这允许在单个位置为多个系统备份和保存数据。

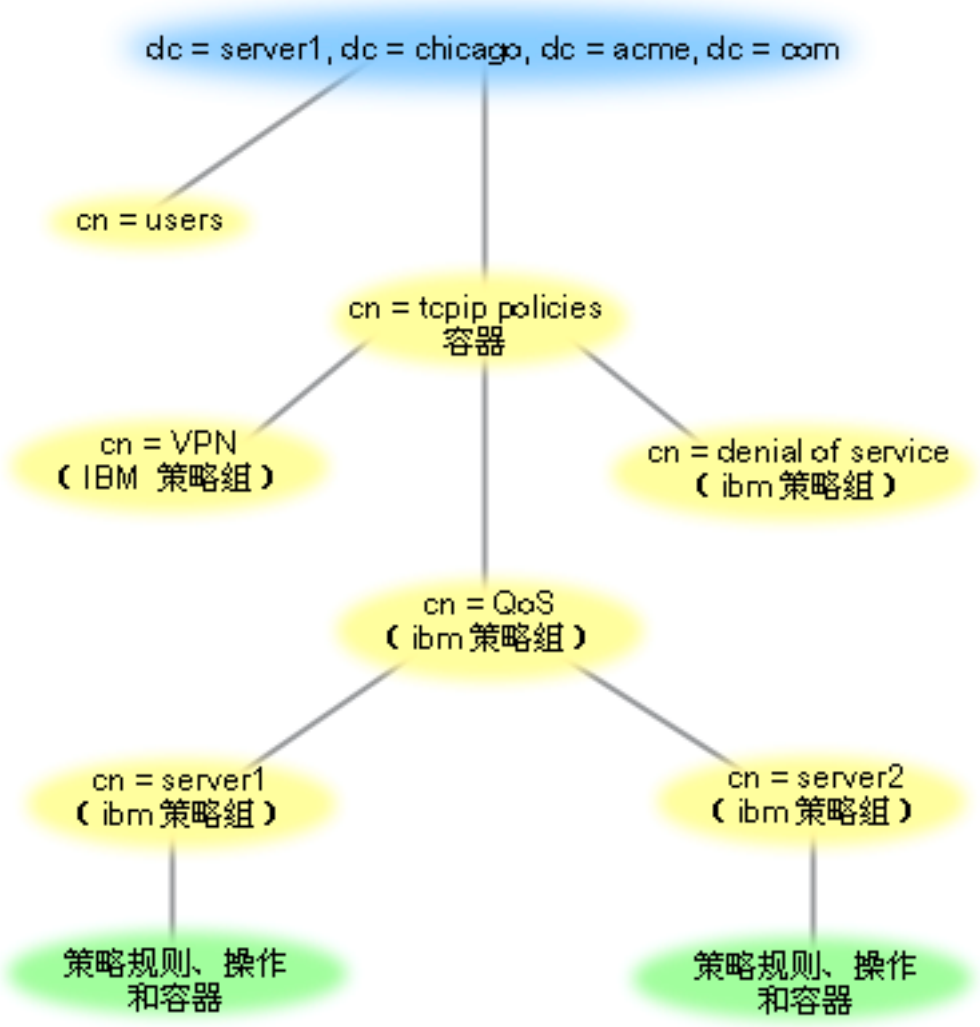
LDAP 资源

在使用 QoS 之前，应熟悉 LDAP 概念和目录结构。请查看 “iSeries 信息中心” 的目录服务（LDAP）主题中的 LDAP 基础。

QoS 树结构

如果要管理目录的组成部分，请参考**专有名称（DN）**或（如果您选择的话）关键字。在配置目录服务器时指定 DN。DN 通常由项本身的名称以及目录中该项上面的对象（从上到下）组成。服务器可以访问目录中该 DN 下面的所有对象。例如，假设 LDAP 服务器包含下面的目录结构:

图 12. 样本 QoS 目录结构



顶部的 Server1（dc=server1,dc=chicago,dc=acme,dc=com）是目录服务器所驻留的服务器。其它服务器（如 cn=QoS 或 cn=tcpip 策略）是 QoS 服务器所驻留的位置。因此在 cn=server1 上，缺省 DN 将显示为 cn=server1,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com。在 cn=server2 上，缺省 DN 将显示为 cn=server2,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com。

管理目录时，更改 DN 中的正确服务器（如 cn 或 dc）很重要。编辑 DN 时应特别小心，因为字符串通常太长，需要滚动才能显示。有关如何使用 “iSeries 导航器” 中的 “服务质量” 功能配置目录服务器的信息，参见配置目录服务器。

有关某些替代 LDAP 资源，参见 QoS 的相关信息页面。 «

关键字

»

配置目录服务器时，需要确定是否使关键字与每个 QoS 配置相关联。关键字字段是可选的，可以忽略。以下信息帮助说明关键字概念以及要使用关键字的原因。

在 “新建服务质量配置” 向导中，您将配置目录服务器。您将指定配置的服务器是主目录服务器还是辅助系统。您在其中维护所有 QoS 策略的服务器称为主系统。

关键字用来标识主系统创建的配置。虽然关键字是在主系统上创建的，但关键字事实上有利于辅助系统。它们使辅助系统能够装入和使用主系统创建的配置。下面的描述有助于说明如何在每个系统中使用关键字。

关键字和主系统
关键字与主系统创建和维护的 QoS 配置相关联。使用关键字，辅助系统可以标识主系统创建的配置。

关键字和辅助系统
辅助系统使用关键字来搜索配置。辅助系统装入并使用主系统创建的配置。配置辅助系统时，可以选择特定的关键字。根据选择的关键字，辅助系统装入与选择的关键字相关联的任何配置。这使辅助系统能够装入多个主系统创建的多个配置。

当您开始在 “iSeries 导航器” 中配置目录服务器时，使用 QoS 任务帮助以了解特定指示信息。 «

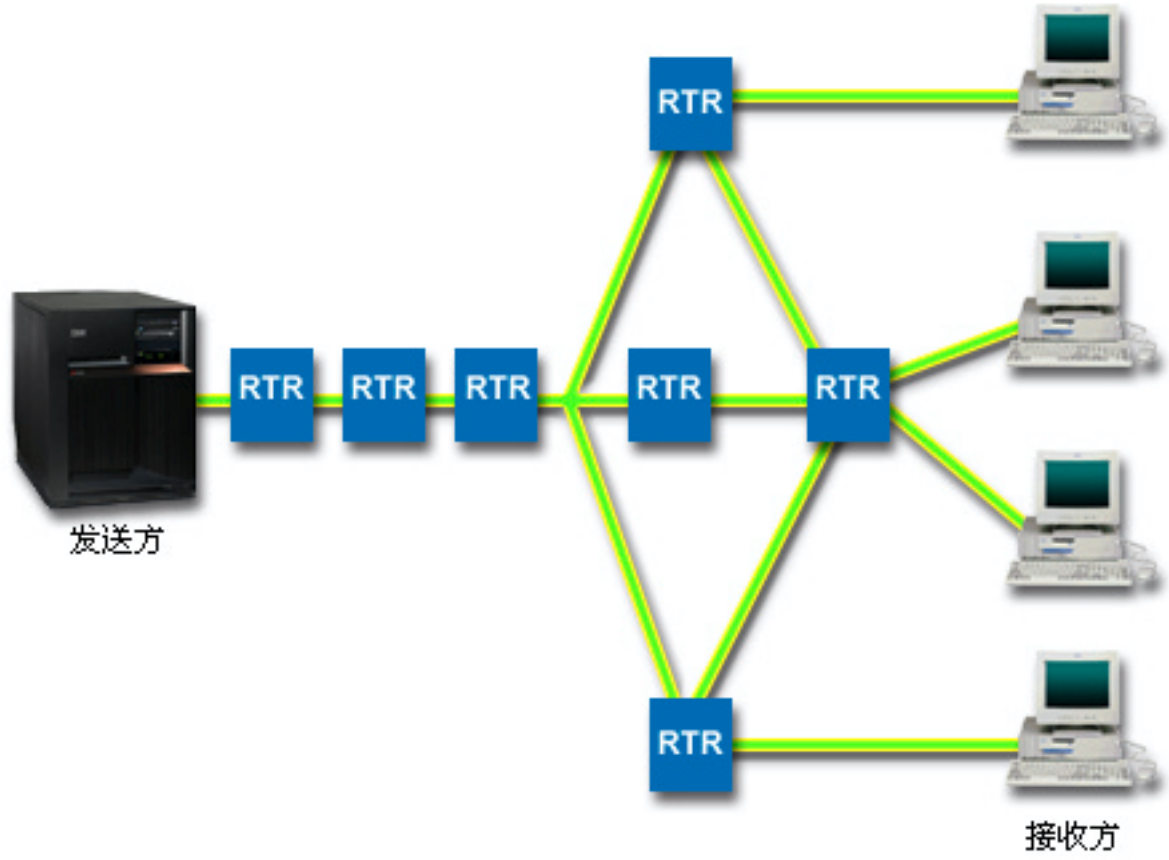
集成服务

集成服务处理流量传送时间并指定特定的流量特殊处理指示信息。采取保守的集成服务策略很重要，因为保证数据传输的费用仍相对较高。但是，过分供应资源可能费用更高。

» 在发送数据之前，集成服务预定资源供特定的策略使用。在数据传输以及网络实际同意并根据策略管理（端到端）数据传输之前，向路由器发出信号。**策略**是指定操作的一组规则。它基本上是一个许可控制列表。带宽请求以预订的方式来自客户机。如果路径中的所有路由器都同意发出请求的客户机的要求，则该请求到达服务器和 intserv 策略。如果请求未超出策略定义的限制，QoS 服务器允许进行 RSVP 连接，然后取消应用程序的带宽。执行预订时使用 “资源预订协议”（RSVP）以及 RAPI 和／或 qtoq QoS 套接字 API。有关更多信息，参见 RSVP 协议和 QoS API。 «

流量所经过的各个节点都必须能够使用 RSVP 协议。路由器通过以下流量控制功能提供服务质量: 信息包调度程序、信息包分类器和许可控制。实现此流量控制的能力通常称为启用了 RSVP。因此，实现集成服务策略最重要的部分是能够控制和预测网络中的资源。要获取预测结果，网络中的各个节点都应启用 RSVP。例如，根据资源而不是根据哪些路径具有能识别 RSVP 的路由器对流量进行路由选择。经过不能识别 RSVP 的路由器可能导致无法预测的性能问题。仍会建立连接，但是该路由器不能保证应用程序请求的性能。下图显示集成服务功能在逻辑上如何工作。

图 13. 客户机和服务器之间的 RSVP 路径。



服务器上启用了 RSVP 的应用程序检测到来自客户机的连接请求。服务器的应用程序作出响应，向客户机发出 PATH 命令。此命名使用 RAPI API 或 qtoq QoS 套接字 API 发出，并且包含路由器 IP 地址信息。PATH 命令包含有关服务器和沿路径的路由器上的可用资源的信息，以及服务器和客户机之间的路由信息。然后，客户机上启用了 RSVP 的应用程序将 RESV 命令沿网络路径发送回来，以发出信号通知服务器已分配网络资源。此命令根据 PATH 命令产生的路由器信息进行预订。服务器和沿路径的所有路由器预定资源供 RSVP 连接使用。当服务器接收到 RESV 命令时，应用程序开始向客户机传送数据。沿与预订相同的路由传送数据。这再次显示路由器实现此预订的能力对于策略成功的重要性。

与 HTTP 相同，集成服务并非用于短期 RSVP 连接。当然这由您决定。只有您才能决定什么最适于您的网络。考虑哪些区域和应用程序具有性能问题并需要服务质量。集成服务策略中使用的应用程序必须能够使用 RSVP 协议。服务器当前没有任何启用了 RSVP 的应用程序，因此您需要编写应用程序来使用 RSVP。有关更多详细信息，参见 RSVP 部分。

当信息包到达并试图离开网络时，服务器确定是否有用来发送信息包的资源。是否可行取决于令牌桶中的空间量。可以手工设置允许进入令牌桶的位数、任何带宽限制、记号速率限制以及服务器允许的最大连接数。这些值称为性能限制。如果入局信息包将导致存储区超过其限制，这些信息包被认为不符合要求。服务器可以使用几种不同的方式处理不符合要求的流量。它可以延迟、整形、重新传送或删除信息包。如果信息包未超出服务器的限制，则信息包符合要求且被向外发送。在集成服务中，每个连接有权使用自己的令牌桶。在区分服务中，整个子网或客户机范围共享令牌桶。

流量控制功能

流量控制功能仅适用于集成服务策略。要获取可预见的结果，需要在流量的路径上具有启用了 RSVP 的硬件。路由器必须具有一定的流量控制功能，才能使用 RSVP 协议。这通常称为启用了 RSVP 或启用了 QoS。记住，您的服务器的角色是客户机或服务器。此时它不能用作路由器。

流量控制功能包括以下:

信息包调度程序
信息包调度程序根据 IP 头中的信息管理信息包转发。信息包调度程序确保信息包传送对应于策略中设置的参数。在将信息包排队的位置实现调度程序。

信息包分类器
信息包分类器也根据 IP 头信息标识 IP 流的哪些信息包将接收一定级别的服务。每个入局信息包由分类器映射到一个特定的类。在同一类中分类的所有信息包接收相同的处理。此服务级别基于在策略中提供的信息。

许可控制
许可控制包含判定算法，路由器使用该算法来确定是否有足够的路由资源来接受新流的请求的 QoS。如果没有足够的资源，则拒绝该新流。如果接受该流，路由器指定信息包分类器和调度程序来预定请求的 QoS。许可控制发生在沿预订路径上的每个路由器中。

这并非是关于分类器和调度程序的全部讨论。要查找替代源，请查看 QoS 的相关信息页面。

集成服务类型

有两种集成服务类型：受控负载和保证服务。

受控负载

受控负载服务支持对拥塞的网络非常敏感的应用程序，如实时应用程序。应用程序还必须容许少量损失和延迟。如果应用程序使用受控负载服务，则当网络负载增加时其性能将无法满足要求。将为流量提供类似负载较轻的条件下网络中的正常流量的服务。

路由器必须确保受控负载服务接收到足够的带宽和信息包处理资源。为此，它们必须启用支持“集成服务”的 QoS。将需要检查路由器的规范以查看它们是否通过流量控制功能提供服务质量。流量控制由下列组件构成: 信息包调度程序、信息包分类器和许可控制。

保证服务

保证服务确保信息包将在指定的传送时间内到达。需要保证服务的应用程序包括使用流技术的视频和音频广播系统。保证服务控制最大入队延迟，以便信息包的延迟时间不超过指定的时间量。沿信息包路径上的每个路由器必须提供 RSVP 能力，才能确保传送。当指定令牌桶限制和带宽限制时，您正在定义您的保证服务。

令牌桶和带宽限制

令牌桶限制和带宽限制合起来称为性能限制。这些性能限制有助于保证集成和区分服务的出站带宽策略中的信息包传送。

令牌桶大小

令牌桶大小确定缓冲区容量，该容量保持数据的脉冲串传输。脉冲串传输数据是应用程序给予服务器来发送出去的信息，且发送出去的速率比信息可以退出的速率快。如果应用程序快速将足够的脉冲串传输数据发送到服务器，则缓冲区会填充满。如果应用程序发送信息的速度比它可以退出服务器的速度慢，则缓冲区腾空。当数据离开服务器的速度与它进入服务器的速度一样快时，则令牌桶大小保持不更改。一旦填充了缓冲区，QoS 就将附加数据信息包看作是在概要文件之外。在此策略中，您可以确定 QoS 如何处理在概要文件之外的流量。

记号速率限制

速率（带宽）限制指定长期数据速率或每秒允许进入一个网络的位数。从服务器请求 RSVP 的任何客户机将请求特定量的带宽（流量限制）。QoS 策略查看请求的带宽并将它与此策略的速率和流量限制进行比较。如果该请求将导致服务器超出其限制，则服务器拒绝该请求。记号速率限制仅用于集成服务策略中的许可控制。它是以 Kb/s 为单位测量的。此值可以在 10 Kb/s 到 1Gb/s 之间变化。

平均速率限制或带宽限制必须小于峰值速率限制或峰值带宽限制，以便不会用尽整个接口。例如，设想您具有一个使用 36 Kb/s 或小于 36 Kb/s 的调制解调器，您将需要这样设置平均速率限制，以便将不会利用整个接口。

提示：要确定设置什么限制，可能需要运行监控器。使用足够大的聚集记号速率限制创建策略，以便能够收集网络中的大多数数据流量。然后对此策略启动数据集合。有关收集应用程序和网络当前使用的总速率的一种方式，参见监控当前网络统计信息示例。使用这些结果，可以适当地减小限制。

有关更多信息，参见区分服务类和 集成服务主题。 

使用区分服务标记的集成服务

此策略在混合环境中最常使用。当集成服务预订经过不支持集成服务预订但支持区分服务的不同路由器时，出现混合环境。由于流量通过不同的域、服务级别协议和设备能力，您并非总能够获得所需的服务。

要帮助减轻此潜在问题，可以将区分服务标记附加至集成服务策略。如果策略经过不能使用 RSVP 协议的路由器，策略仍将保持某种优先级。您添加的标记称为逐跳行为。 

无信号

除了使用标记（如上所述）之外，还可以使用新的“无信号”功能。在集成服务策略中指定“无信号”。可以在任何集成服务策略的**特性**面板中指定无信号。

1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
2. 右键单击**服务质量**并选择**配置**。
3. 展开**出站带宽策略 —> IntServ**。
4. 右键单击以上所创建的策略名称并选择**特性**，“IntServ 特性”对话框出现。
5. 选择**流量管理**选项卡以禁用或启用信号。这里也是编辑调度表、客户机、应用程序和流量管理的地方。

选择“无信号”后，API 的“无信号”版本将允许您编写一个应用程序，该应用程序导致在服务器上装入 RSVP 规则，并且仅要求 TCP/IP 对话的服务器端应用程序启用 RSVP。该应用程序代表客户机端自动发出 RSVP 信号。这样即使客户机端不能够使用 RSVP 协议，也会为应用程序创建 RSVP 连接。

有关更多信息，参见区分服务类和 集成服务主题。

RSVP 协议和 QoS API

“资源预订协议”（RSVP）以及 RAPI API 或 qtoq QoS 套接字 API 执行集成服务预订。流量通过的每个节点必须具有使用 RSVP 协议的能力。执行集成服务策略的能力经常称为启用了 RSVP。有关使用 RSVP 协议需要哪些路由器功能的更多信息，参见流量控制功能。

RSVP 协议用来在沿着流量的路径的所有网络节点中创建 RSVP 预订。它维护此预订足够长的时间，以便提供您的策略请求的服务。该预订定义此对话中的数据将需要的处理和带宽。每个网络节点同意提供预订中定义的数据处理。

RSVP 是一种简单的协议，它仅在一个方向（从接收方）进行预订。对于更复杂的连接（如音频和视频会议），每个发送方也是接收方。在此情况下，必须为每端设置两个 RSVP 会话。

除启用了 RSVP 的路由器外，还需要具有启用了 RSVP 的应用程序来使用集成服务。由于 iSeries 服务器此时不具有任何启用了 RSVP 的应用程序，所以需要使用 RAPI API 或 qtoq QoS 套接字 API 来编写该应用程序。这将使应用程序能够使用 RSVP 协议。如果需要深入说明，有许多说明这些模型、它们的操作和消息传递的源。需要十分了解 RSVP 协议和因特网 RFC 2205 的内容。

qtoq 套接字 API

现在可以使用 qtoq QoS 套接字 API 来简化在 iSeries 系统上使用 RSVP 协议所需要的工作。qtoq 套接字 API 调用 RAPI API 并执行某些更复杂的任务。qtoq 套接字 API 不象 RAPI API 那样灵活，但使用较少的努力就可提供同样的功能。API 的“无信号”版本允许您编写以下程序:

- 将在服务器上装入 RSVP 规则的应用程序。
- 仅需要（TCP/IP 对话的）服务器端应用程序启用了 RSVP 的应用程序。

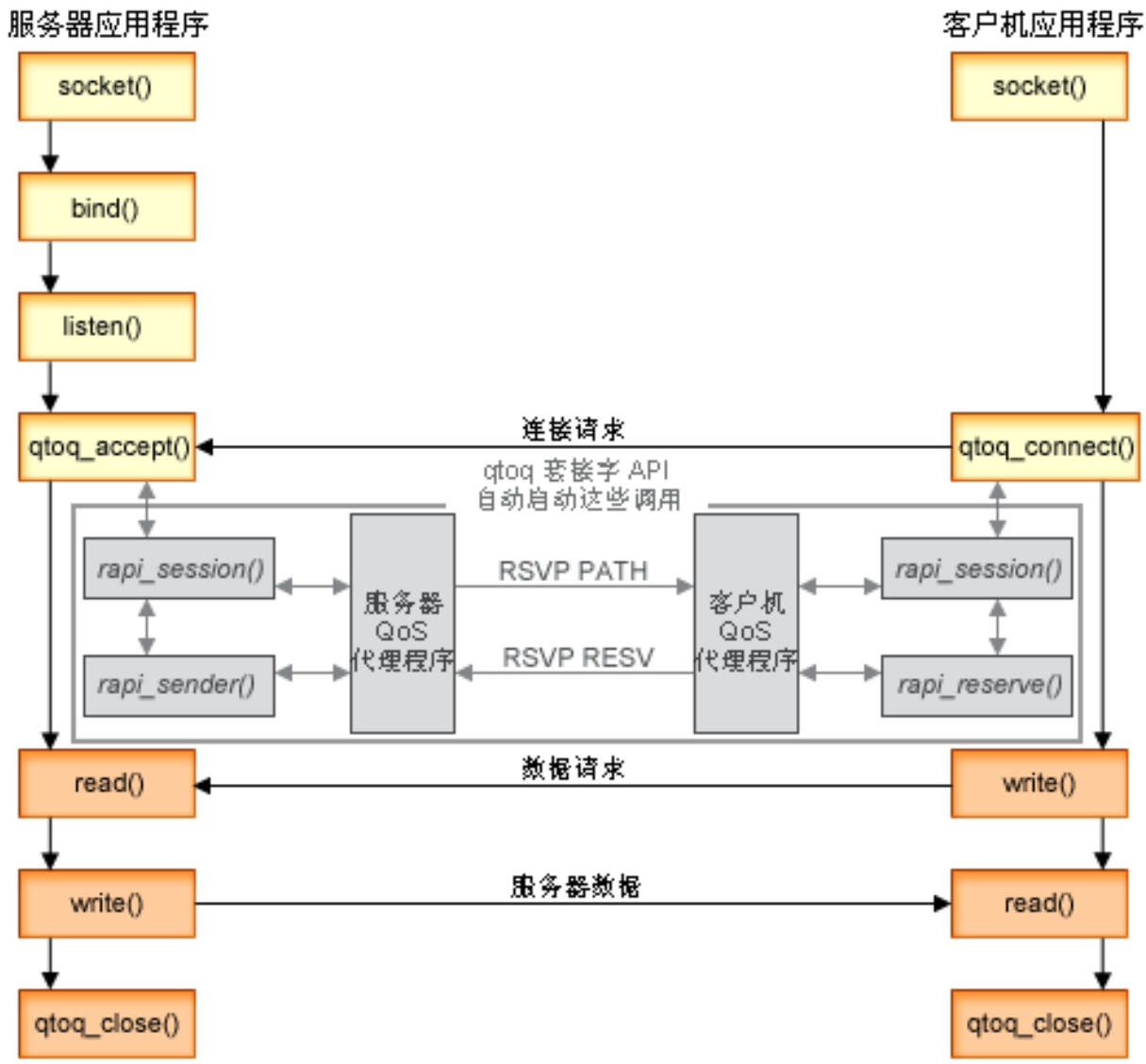
代表客户机端自动发出 RSVP 信号。

参见 QoS API 面向连接的功能流页面，或 QoS API 无连接功能流页面以获取使用面向连接或无连接的 qtoq QoS 套接字的应用程序 / 协议的典型 QoS API 流。 

QoS API 面向连接的功能流

 下图说明对于面向连接的协议（如“传输控制协议”（TCP））启用了 QoS 的 API qtoq 套接字函数的客户机 / 服务器关系。

当对于面向连接的流（该流正请求启动 RSVP）调用启用了 QoS 的 API 函数时，启动附加函数。这些函数导致客户机和服务器上的 QoS 代理程序为客户机和服务器之间的数据流设置 RSVP 协议。



事件的 qtoq 流: 下列套接字调用序列提供了图形描述。它也描述面向连接的设计中服务器和客户机应用程序之间的关系。这些是对于基本“套接字 API”的修改。

服务器端

用于标记为“无信号”的规则的 qtoq_accept()

1. 应用程序调用 socket() 函数来获取套接字描述符。
2. 应用程序调用 listen() 来指定将等待哪些连接。
3. 应用程序调用 qtoq_accept() 来等待来自客户机的连接请求。
4. API 调用 rapi_session() API 并且如果成功，将指定 QoS 会话标识。
5. API 调用标准 accept() 函数来等待客户机连接请求。
6. 当接收到连接请求时，对请求的规则执行许可控制。将规则发送至 TCP/IP 堆栈，如果有效，规则与结果和会话标识一起返回到调用应用程序。

7. 服务器和客户机的应用程序执行期望的数据传输。
8. 应用程序将调用 qtoq_close() 函数来关闭套接字并卸装规则。
9. QoS 服务器将从 QoS 管理器删除规则、删除 QoS 会话并执行需要的其它清除。

使用正常的 RSVP 信号的 qtoq_accept()

1. 应用程序调用 socket() 函数来获取套接字描述符。
2. 应用程序调用 listen() 来指定将等待哪些连接。
3. 应用程序调用 qtoq_accept() 来等待来自客户机的连接请求。
4. 当连接请求到达时，将调用 rapi_session() API 来为此连接创建与 QoS 服务器的会话并获取将返回至调用程序的 QoS 会话标识。
5. 将调用 rapi_sender() API 来启动来自 QoS 服务器的 PATH 消息，并通知 QoS 服务器它必须期望来自客户机的 RESV 消息。
6. 调用 rapi_getfd() API 来获取应用程序使用的等待 QoS 事件消息的描述符。
7. 将接受描述符和 QoS 描述符返回到应用程序。
8. QoS 服务器等待要接收的 RESV 消息。当接收到该消息时，它将使用 QoS 管理器装入适当的规则并且如果应用程序在 qtoq_accept() API 调用中请求了通知，则将消息发送至应用程序。
9. QoS 服务器继续为建立的会话提供刷新。
10. 当完成连接时，应用程序调用 qtoq_close()。
11. QoS 服务器将从 QoS 管理器删除规则、删除 QoS 会话并执行需要的清除。

客户机端

使用正常的 RSVP 信号的 qtoq_connect()

1. 应用程序调用 socket() 函数来获取套接字描述符。
2. 应用程序调用 qtoq_connect() 函数来通知服务器应用程序它希望建立连接。
3. qtoq_connect() 函数调用 rapi_session() API 来为此连接创建与 QoS 服务器的会话。
4. 将启动 QoS 服务器来等待来自所请求的连接的 PATH 命令。
5. 调用 rapi_getfd() 以获取 QoS 描述符，应用程序使用该描述符等待 QoS 消息。
6. 调用 connect() 函数。将 connect() 的结果和 QoS 描述符返回到应用程序。
7. QoS 服务器等待要接收的 PATH 消息。当接收到该消息时，它将使用 RESV 消息对应用程序服务器上的 QoS 服务器作出响应。
8. 如果应用程序请求了通知，QoS 服务器将通过 QoS 描述符将通知发送至应用程序。
9. QoS 服务器继续为建立的会话提供刷新。
10. 当连接完成时，应用程序调用 qtoq_close()。
11. QoS 服务器将关闭 QoS 会话并执行需要的清除。

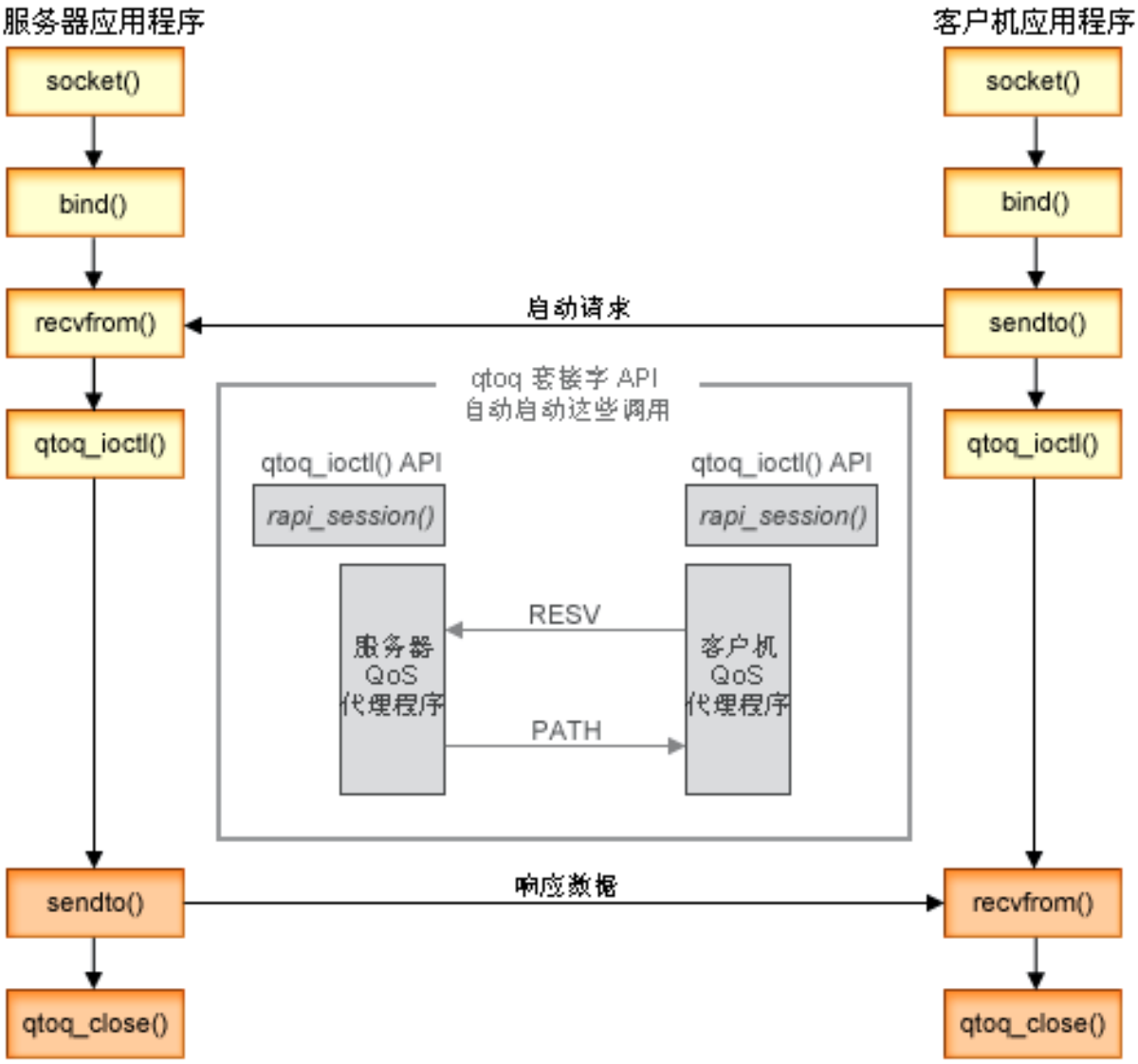
用于标记为“无信号”的规则的 qtoq_connect()

此请求对于客户机端无效，因为在此情况下不需要来自客户机的响应。 «

QoS API 无连接功能流

» 以下服务器和客户机示例说明为无连接流编写的 qtoq QoS 套接字 API。

当对于无连接流（该流正请求启动 RSVP）调用启用了 QoS 的 API 函数时，启动附加函数。这些函数导致客户机和服务器上的 QoS 代理程序为客户机和服务器之间的数据流设置 RSVP 协议。



事件的 qtoq 流：下列套接字调用序列提供了图形描述。它也描述无连接的设计中服务器和客户机应用程序之间的关系。这些是对于基本“套接字 API”的修改。

服务器端

用于标记为“无信号”的规则的 qtoq_ioctl()

1. 将消息发送至请求其对请求的规则执行许可控制的 QoS 服务器。
2. 如果规则是可接受的，它调用一个函数将消息发送至请求装入规则的 QoS 服务器。
3. 将状态返回至调用程序以指示请求的成功或故障。
4. 当应用程序完成使用连接时，它调用 qtoq_close() 函数来关闭连接。

5. QoS 服务器将从 QoS 管理器删除规则、删除 QoS 会话并执行需要的其它清除。

使用正常的 RSVP 信号的 qtoq_ioctl()

1. 将消息发送至对所请求的连接请求了许可控制的 QoS 服务器。
2. 调用 rapi_session() 来请求为规则设置会话并获取要返回至调用程序的 QoS 会话标识。
3. 调用 rapi_sender() 来启动 PATH 消息返回到客户机。
4. 调用 rapi_getfd() 来获取文件描述符以等待 QoS 事件。
5. 将描述符 select()、QoS 会话标识和状态返回至调用程序。
6. 当接收到 RESV 消息时，QoS 服务器装入规则。
7. 当完成连接时，应用程序发出 qtoq_close()。
8. QoS 服务器将从 QoS 管理器删除规则、删除 QoS 会话并执行需要的清除。

客户机端

使用正常的 RSVP 信号的 qtoq_ioctl()

1. 调用 rapi_session() 来请求为连接设置会话。rapi_session() 函数请求对连接的许可控制。仅当存在客户机的已配置的规则而此时它不活动时，才将在客户机端拒绝连接。此函数将传送的 QoS 会话标识返回到应用程序。
2. 调用 rapi_getfd() 来获取文件描述符以等待 QoS 事件。
3. qtoq_ioctl() 与等待描述符和会话标识一起返回到调用程序。
4. QoS 服务器等待要接收的 PATH 消息。当接收到路径消息时，它将使用 RESV 消息作出响应，然后通过会话描述符向应用程序发出信号表示事件已发生。
5. QoS 服务器继续为建立的会话提供刷新。
6. 当完成连接时，客户机代码调用 qtoq_close()。

用于标记为“无信号”的规则的 qtoq_ioctl()

此请求对于客户机端无效，因为在此情况下不需要来自客户机的响应。

QoS 计划

实现服务质量的最重要的步骤是计划。要接收到预期的结果，必须检查网络设备并监控网络流量。QoS 计划顾问程序引导您完成在计划阶段期间需要问您自己的基本问题。除顾问程序外，在实现 QoS 之前还应考虑以下子主题。

权限需求
列示成功配置 QoS 和目录服务器所需要的所有权限。

系统需求
列示成功操作 QoS 所需要的所有需求。

排序 QoS 策略
策略在文件中出现的顺序也是处理它们的顺序。这仅适用于区分服务策略和连接速率策略。

服务级别协议
服务级别协议是 QoS 的重要部分。必须了解 SLA 并使用网络提供程序设置 SLA 作为 QoS 计划的一部分。

网络硬件和软件
服务质量仅相当于其最弱的链路。内部设备和网络之外的其它设备的性能对 QoS 结果具有巨大的影响。

网络性能
QoS 是关于网络性能的一切。您考虑 QoS 的主要原因很可能是因为您已经经历网络拥塞和信息包丢失。在实现任何策略之前，您可能需要使用 QoS 监控器来验证您的 IP 流量的当前性能级别。这些结果将帮助您确定拥塞发生的位置。参见“故障诊断”之下的监控服务器事务主题。

QoS 计划顾问程序
在实现服务质量之前，考虑这些基本问题。您将接收到一份计划工作表，该工作表具有根据您的应用程序的能力而建议的策略。

权限需求

服务质量策略可能包含有关网络的机密信息。因此，应仅在必要时才授予 QoS 管理权限。将需要下列权限才能配置 QoS 策略或 LDAP 目录服务器。因为 QoS 策略存储在 LDAP 目录服务器中，所以需要两个权限。

授予管理目录服务器所需要的权限
QoS 管理员将需要下列权限：*ALLOBJ 权限和 *IOSYSCFG。有关替代权限的信息，参见配置目录服务器。

授予启动 TCP/IP 服务器的权限。
要授予对 STRTCPSVR 和 ENDTCPSVR 命令的对象权限，遵循下列步骤:

1. **STRTCPSVR**：在命令行上，输入 GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE)，用管理员的概要文件的名称替换 ADMINPROFILE，并按**执行**键。
2. **ENDTCPSVR**：在命令行上，输入 GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE)，用管理员的概要文件的名称替换 ADMINPROFILE，并按**执行**键。

授予全部对象访问权和系统配置权限。
建议让配置 QoS 的用户具有安全主管访问权。要授予全部对象访问权和系统配置权限，遵循下列步骤:

1. 在“iSeries 导航器”中，展开服务器 —> **用户和组**。
2. 双击**所有用户**。
3. 右键单击管理员的用户概要文件并选择**特性**。

4. 在“特性”对话框上，单击**性能**。
5. 在“性能”页面，选择**全部对象访问权和系统配置**。
6. 单击**确定**关闭“性能”页面。
7. 单击**确定**关闭“特性”页面。

系统需求

服务质量（QoS）是操作系统的一个集成部分。在继续配置和启动 QoS 之前，必须至少具有“版本 5 发行版 1”的 OS/400(R)。而且，必须完成以下需求:

1. 安装 TCP/IP 连通性实用程序（57*xx*-TC1）。
2. 在 PC 机上安装 iSeries 导航器。确保在 Client Access 安装期间安装“联网”部分。“服务质量”位于“联网”中的“IP 策略”之下。

注意: 如果需要关于 TCP/IP、联网或 IP 地址的更多信息，参考 QoS 的相关信息中的 TCP/IP Tutorial and Technical Overview 和 V4 TCP/IP for AS/400(R): More Cool Things Than Ever。

排序 QoS 策略

每当您具有两个重叠的区分服务策略或两个重叠的连接速率策略时，在“iSeries 导航器”中您的策略的物理顺序都很重要。重叠策略是使用相同的客户机、应用程序、调度表或协议的两个策略。在“iSeries 导航器”屏幕中的策略处于已排序的列表中。策略优先级取决于此列表中策略的顺序。如果要一个策略比另一个策略具有较高优先级，则较高优先级策略必须首先出现在列表中。

要确定一个策略是否与另一个策略重叠，遵循以下指示信息:

1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
2. 右键单击**服务质量**。
3. 选择**配置**。
4. 选择特定的“策略”文件夹。
5. 右键单击具有相关联的重叠策略的策略名称。在重叠策略前面有一个图标以指示重叠。
6. 选择**显示重叠**。重叠面板将出现。

要更改屏幕中的策略顺序，使用下列步骤:

- 突出显示策略并使用屏幕上的向上和向下箭头来更改策略顺序。
- 右键单击策略名称并选择**向上移动**或**向下移动**。
- 更新 QoS 服务器。可以使用工具栏中的“更新”服务器按钮或查看 QoS 任务帮助以获取更多详细的指示信息。

服务级别协议

本节不是关于服务级别协议（SLA）提供程序的教育信息，但它指出 SLA 中可能影响服务质量实现的某些重要方面。您的策略和预订仅与最弱的链路一样。这表示，如果客户机和服务器之间任何一个位置的一个节点无法执行“区分服务”或“集成服务”主题中讨论的任何一个流量处理特征，则您的策略将不会象您计划的那样来处理。如果您的 SLA 未提供您足够的资源，则即使最好的策略也将不会有助于解决您的网络的拥塞问题。

这也涉及跨 ISP 的协议。在各个域中，每个 ISP 必须同意支持服务质量请求。互操作性可能会导致某些提问。

确保了解您实际上正在接收的服务级别。流量调节协议明确提出如何处理已删除、标记、整形或重新传送的流量。提供服务质量的关键原因涉及控制等待时间、抖动、带宽、信息包损失、可用性和吞吐量。您的服务协议必须能够给予您的策略它们请求的服务。验证您是否正在接收需要的服务量。如果不是的话，可能会浪费您的资源。例如，如果您请求预定 500kbps 用于 IP 电话，但您的应用程序只需要 20kbps，则您可能支付额外费用而未从您的 ISP 接收到任何通知。

网络硬件和软件

内部设备和网络外的其它设备的性能对 QoS 结果有巨大影响。

应用程序

集成服务策略需要启用了 RSVP 的应用程序。因为 iSeries 应用程序当前未启用 RSVP，所以必须启用它们来使用 RSVP 协议。要启用应用程序，需要使用“资源预订设置协议”（RAPI）API 或 qtoq QoS 套接字 API 来编写特殊程序。这些程序将允许您的应用程序使用 RSVP。有关更多信息，参见 RSVP 协议和 QoS API。

网络节点

路由器、交换机甚至是您自己的服务器必须具有使用服务质量的能力。要使用区分服务策略，设备必须启用区分服务。这意味着网络节点必须能够分类、测量、标记、整形和删除 IP 信息包。有关流量调节器的更详细的信息（分类、测量、标记、整形和删除），参见流量调节器主题。

要使用集成服务策略，设备必须启用 RSVP。这意味着网络节点必须也能支持 RSVP 协议。有关 RSVP 协议的更详细的信息，参见 RSVP 主题。

配置 QoS

使用“iSeries 导航器”内的向导创建 QoS 策略。此向导可以非常卓越地指导您完成配置。

» 配置策略之后，可以使用“iSeries 导航器”中的配置对象来编辑策略配置。配置对象是构成策略的不同部分。当在“iSeries 导航器”中打开服务质量时，有标记为客户机、应用程序、调度表、策略、服务类、逐跳行为和 URI 的文件夹。这些对象允许您创建策略。有关对象的更详细的信息，可以参见 iSeries 导航器中的“服务质量概述帮助”。

配置目录服务器

使用它以获取有关如何在 QoS 内配置目录服务器的信息。

使用向导配置 QoS

使用它以获取有关如何访问 QoS 向导的指示信息。 «

启用 QoS

必须启用策略，它们才能生效。如果使用过向导，服务器将自动为您启用策略。如果使用配置对象更改过策略，则在策略变为活动之前，将需要 动态更新服务器。在启用之前，确保查找可能导致问题的重叠策略。有关更多信息，参见排序 QoS 策略。

配置目录服务器

» QoS 策略配置现在存储在 LDAP 目录服务器上。这使 QoS 解决方案更易于管理。可以将配置数据存储在一个本地目录服务器上以便许多系统共享，而不是在所有服务器上配置 QoS 策略。当第一次在服务器上配置服务质量时，出现“初始配置”向导。此向导将提示您配置目录服务器。

要配置目录服务器，您将需要决定或了解下列信息:

- 目录服务器名称

- 确定引用 QoS 策略的专有名称（DN）
- 确定是否要将 SSL 安全性用于 LDAP 目录服务器
- 确定是否要使用关键字来改进在目录服务器上对策略的搜索。

注意: 当前情况下，不能将 Kerberos 配置为 QoS 服务器将用来访问目录的认证方法。

要管理 LDAP 目录服务器，必须设置下列权限集的一种:

- *ALLOBJ 权限和 *IOSYSCFG 权限
- 对“结束 TCP/IP”（ENDTCP）、“启动 TCP/IP”（STRTCP）、“启动 TCP/IP 服务器”（STRTCPSVR）和“结束 TCP/IP 服务器”（ENDTCPSVR）命令的 *JOBCTL 权限和对象权限。
- 配置 OS/400(R) 安全性审计的 *AUDIT 权限。

如果正在使用“iSeries 导航器”，您将已具有对缺省“QoS 模式”的访问权。但是，如果正在使用“iSeries 导航器”以外的编辑器，您将需要导入以下所描述的 LDIF 文件。如果在编辑之后，要重新装入原始的缺省文件，也可以导入此文件。

QoS 模式

存在称为模式的一组规则，用于指定哪些类型的 LDAP 对象对于 QoS 服务器有效。V5R2 iSeries 服务器上的模式包含 QoS 的必要规则。但是，如果使用的 LDAP 服务器不是 iSeries 服务器，必须将这些规则导入到 LDAP 服务器。这通过 LDIF（LDAP 数据交换格式）文件完成。使用 iSeries LDAP Web 页面 来下载 LDIF 文件。您将在左窗格中的**类别 —> TCP/IP 策略**下找到此文件。

编辑 LDIF 文件

可以使用 IBM(R) SecureWay(R) 目录管理工具（DMT）来编辑 LDAP 服务器的模式文件。也可以将 DMT 的 setup.exe 文件 FTP 到您的 PC。Setup.exe 文件应该位于服务器上的 /qibm/proddata/os400/dirsrv/UserTools/Windows 中。可以从 iSeries LDAP Web 页面获取原始 QoS 模式。有关样本 QoS 模式，参见 LDAP 概念。模式文件位于服务器上的 /QIBM/UserData/OS400/DirSrv 中。 «

使用向导配置 QoS

» 要配置服务质量策略，必须使用位于“iSeries 导航器”中的 QoS 向导。此处是向导及其功能列表:

初始配置向导

此向导使您能够设置系统特定的配置和目录服务器信息。

新建 IntServ 策略向导

“新建 IntServ 策略”向导使您能够创建集成服务策略。此策略接纳或拒绝 RSVP 请求，这间接控制了服务器带宽。策略性能限制（您设置的）决定服务器是否可以处理来自客户机的 RSVP 应用程序的请求的带宽。您将需要 RSVP 就绪的路由器和应用程序来实现此向导中创建的集成服务策略。

> **注意**: 在设置集成服务策略之前，您必须编写自己的应用程序来使用 RSVP 协议。有关更多信息，参见 RSVP 协议和 QoS API。

新建 DiffServ 策略向导

此向导使您能区分优先级并将优先级指定给 TCP/IP 流量。您将能够通过创建策略来区分流量。在策略中，您可以将优先级指定给应用程序和端口，并指定此策略何时应该是活动的。

新建 DiffServ 服务类向导

使用区分服务类向导来设置网络中路由器和交换机使用的信息包标记。它也将性能限制指定给离开您的网络的流量。您可将服务类与 DiffServ 策略一起使用。

新建连接速率向导

使用“入站连接速率”向导来限制与服务器建立的连接。可以按 TCP/IP 地址、应用程序或本地接口来限制访问。这使系统管理员能够控制特定客户机对您的服务器的访问或对服务器应用程序或接口的访问。而且，您可以提高服务器性能。

新建 URI 向导

使用“入站 URI”向导来限制与服务器产生的连接。可以限制通过 URI、应用程序或您的 iSeries 服务器上的本地接口的访问。这使系统管理员能够控制对特定 URI、应用程序或您的服务器上的接口的访问。而且，您可以提高服务器性能。

注意: 设置 URI 请求速率策略之前，必须执行下列步骤:

1. `WRKHTTPCFG` — 修改您的 Apache Web 服务器实例。通过带有“快速响应高速缓存加速键”（FRCA）选项的 Listen 伪指令启用端口。
2. `STRTCPSVR SERVER(*HTTP) HTTPSRV`（实例的名称）。
3. 在“iSeries 导航器”中使用 QoS 创建或修改 URI 策略。确保 URI 策略中定义的应用程序端口与“Apache Web 服务器”实例中定义的 FRCA“Listen 伪指令”匹配。
4. `STRTCPSVR SERVER(*QOS)`。

新建 URI 策略中指定的应用程序端口必须与“Apache Web 服务器”配置中为 FRCA 启用的“Listen”伪指令匹配。如果端口值不匹配，QoS URI 策略将不象期望的那样起作用。有关 URI 请求速率策略的描述，参见连接请求速率和 URI 请求速率。

一旦您决定要创建哪种类型的策略，就可以在以上列示的适当向导中配置策略。参见在“iSeries 导航器”中访问 QoS 向导来启动配置策略。 

访问“iSeries 导航器”内的 QoS 向导

要访问 QoS 向导并创建新的策略，遵循下列步骤:

1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
2. 右键单击**服务质量**并选择**配置**。
   注意: “初始配置”向导在下列情况下出现:
   - 正在将服务器升级到新的发行版。将需要配置要在其中存储信息的目录服务器。在此转换期间未丢失数据。
   - 这是第一次在此系统上使用 QoS 图形用户界面（GUI）。
   - 要手工除去任何先前的配置信息并启动。仅当已打开 QoS 界面时才会出现此向导。
3. 完成“**初始配置**”**向导**。如果“初始配置”向导未出现，则跳至步骤 4。
4. 选择**策略**。右键单击 **IntServ**、**DiffServ**、**连接速率**或**服务器请求 —> URI**。
5. 选择**新建策略**。

管理 QoS

一旦激活并运行 QoS 策略，将可能需要进行更新。可以通过执行下列任务来管理策略:

在 iSeries 导航器中访问 QoS 任务帮助
您可能会注意到此主题经常引用“iSeries 导航器”中的 QoS 任务帮助。如果不知道如何到达那儿，则查看以下指示信息。

备份 QoS 策略
可以备份策略来避免丢失文件。

复制现有的策略
可以复制可能与要创建的策略类似的现有策略。

动态更新策略
可以在服务器运行时动态更新策略。使用“iSeries 导航器”的 QoS 任务帮助中的*更新 QoS 服务器*来获取循序渐进的指示信息。

编辑 QoS 策略
可以更改现有策略中的参数。

编辑 QoS 配置特性
可以更改服务质量配置的特性。这些特性包含目录服务器配置、日志记录和自动启动服务器的设置。使用“iSeries 导航器”的 QoS 任务帮助中的*编辑 QoS 特性*来获取循序渐进的指示信息。

启用 QoS 策略
必须启用策略，它们才能生效。记住在启用策略之前手工检查可能的错误。例如，确保策略的顺序正确。如果需要有关策略顺序的更多信息，参见排序 QoS 策略。否则，使用“iSeries 导航器”的 QoS 任务帮助中的*启用 QoS 策略*来获取循序渐进的指示信息。

监控 QoS 策略
当管理策略时，可能要分析 QoS 监控器来验证策略是否正如您所愿的那样工作。

查看 QoS 策略
通过查看重叠策略，可以确定何处可能有与您的期望所不同的结果。可以在可能导致问题的策略之间检查任何可见的重叠。您将不仅要在激活和测试之前，而且还要在打印和备份之前查看这些重叠。这是在测试之前使错误最小化或除去错误的有用方法。要查看重叠策略，参见排序 QoS 策略。

在“iSeries 导航器”中访问 QoS 帮助

» 要访问服务质量帮助，必须使用“iSeries 导航器”:

1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
2. 右键单击**服务质量**并选择**配置**。
3. 从菜单栏选择**帮助 —> 帮助主题**。任务帮助窗口出现在屏幕上。

«

备份 QoS 策略

» 备份配置文件始终是一个好主意。策略存储在本地或存储在目录服务器中。必须特别备份下列集成文件系统目录: `QIBM/UserData/OS400/QOS/ETC`、`QIBM/UserData/OS400/QOS/TEMP` 和 `QIBM/UserData/OS400/QOS/USR`。还应该备份 QoS 服务器的目录服务器发布代理程序。发布代理程序包含目录服务器名称、QoS 服务器的专有

名称（DN）、用于访问目录服务器的端口和认证信息。万一丢失信息，您的备份可以节省从暂存区重新创建策略所花费的时间和工作。有几个一般技巧可以用来确保使用一种容易的方法来替换丢失的文件:

1. **使用集成文件系统备份与恢复程序**
   使用以下的 Backup and Recovery 一书的链接。
2. **打印策略**
   可以将打印输出存储在最安全的地方并在必要时重新输入信息。
3. **将信息复制到磁盘**
   复制比打印输出优越的是: 不必手工重新输入且信息以电子方式存在。它为您提供了简单的方法将信息从一个联机源传送到另一个联机源。

   注意: iSeries 服务器将信息复制到系统磁盘，而不是复制到软盘。规则文件以专有名称存在于您配置的目录服务器中的 `QIBM/UserData/OS400/QOS/ETC` 中，而不是在 PC 上。您可能要将磁盘保护方法用作备份方法来保护存储在系统磁盘上的数据。

当使用 iSeries 服务器时，必须计划备份与恢复策略。有关更详细的信息，查看 Backup and Recovery  。

复制现有的策略

可以发现有几个彼此非常相似的策略。不是从零开始创建所有这些策略，而是可以复制原始策略，然后编辑策略中与原始策略不同的部分。在 “iSeries 导航器” 中，此 QoS 功能称为*基于模板新建*。必须使用 “iSeries 导航器” 来访问 QoS 对话框以使您能够继续复制策略。

要创建现有策略的副本，遵循 “iSeries 导航器” 帮助中**基于现有策略创建新的策略**中的步骤。

必须通过启动 QoS 服务器或执行动态服务器更新来启用策略之后，策略才能生效。在启用之前，确保查找可能导致问题的重叠策略。有关更多信息，参见排序 QoS 策略。

监控 QoS

可以使用监控器分析流经服务器的 IP 流量。这有助于确定网络中发生拥塞的位置。监控器不仅在 QoS 计划期间有用，而且作为故障诊断工具也很有帮助。QoS 监控器可以帮助您继续监控网络，以便可以在需要时调整策略。

要运行 QoS 监控器，参见 “iSeries 导航器” QoS 帮助中的指示信息。

注意: 如果打开了 QoS 数据集合，并且计划更改 QoS 配置，则必须执行以下步骤以确保监控器收集准确数据。

1. 停止 QoS 数据集合。
2. 更改配置。
3. 重新启动 / 更新 QoS 服务器。
4. 启动 QoS 数据集合。

监控器输出

接收的输出信息取决于正在监控的策略的类型。记住策略的类型: DiffServ、IntServ（受控负载）、IntServ（保证）、连接速率以及 URI。要评估的字段取决于策略类型。最引人关注的值是显示评测的值。评测以下字段而不是评测给定的定义: 接受的请求数、活动的连接数、连接服务、连接速率、删除的请求数、概要文件内信息包数、概要文件内位数、不符合要求的位数、概要文件外位数、总位数、总信息包数以及总请求数。

通过阅读以上评测字段中的信息，可以对网络流量符合策略的程度有一个清楚的了解。有关每个策略类型的监控器输出字段的更详细信息，参见下面的描述。（仅供参考）参见任何 QoS 方案，了解有关如何使用监控器和 QoS 策略的样本。

- 区分服务策略
- 集成服务（受控负载）策略
- 集成服务（保证）策略
- URI 策略
- 连接速率策略

区分服务策略

字段	描述
策略名称	为此策略指定的名称。
协议	UDP、TCP 和 ALL
平均记号速率限制	沿流路径的每个路由器和服务器中此策略允许的平均记号速率。
记号深度限制	沿流路径的每个路由器和服务器中此策略允许的最大记号缓冲区大小。
最大记号速率限制	此连接允许的最大速率。
概要文件内信息包数	已传送的符合此策略参数的 IP 信息包数。
概要文件内位数	已传送的符合此策略参数的位数。
概要文件外位数	已传送的超过策略参数的位数。
位速率	此连接允许的评测位数。
活动连接数	活动连接总数。
流量概要文件	概要文件外信息包中使用的信息包调节类型。格式可能包括: • 重新标记 • 整形 • 删除
总位数	从启动此策略的时间到监控集合的时间，此策略使用的已传送的位数。
概要文件内代码点	如果使用新代码点重新标记信息包，则这是 IP 信息包在符合此策略的参数时将使用的代码点。
概要文件外代码点	如果使用新代码点标记信息包，则这是 IP 信息包在超过策略的参数时将使用的代码点。
目标地址范围	确定受此策略控制的信息包的目标点的地址范围。
总信息包数	从启动此策略的时间到监控集合的时间，由此策略传送的信息包数。
源端口范围	确定哪些应用程序受此策略控制的源端口范围。

集成服务（受控负载）策略

字段	描述
策略名称	为此策略指定的名称。

协议	UDP 或 TCP
目标地址	确定受此策略控制的信息包的目标点的地址范围。
平均记号速率限制	沿连接路径的每个路由器和服务器中此策略允许的平均记号速率。
记号深度限制	沿连接路径的每个路由器和服务器中此策略允许的最大记号缓冲区大小。
最大记号速率限制	此连接允许的最大速率。
总信息包数	从启动此策略的时间到监控集合的时间，由此策略传送的信息包数。
不符合要求的位数	已传送的超过策略参数的位数。
总位数	从启动此策略的时间到监控集合的时间，此策略使用的已传送的位数。
位速率	此连接允许的评测位数。
符合要求的位数	已传送的符合此策略参数的位数。
最大信息包大小	受此策略控制的最大允许信息包大小。
最小管制单元	将从令牌桶中除去的最小位数。 例如，如果最小管制单元为 100 位，则仍将按 100 位除去 100 位以下的信息包。
符合要求的信息包数	已传送的符合此策略参数的 IP 信息包数。
源端口范围	确定哪些应用程序受此策略控制的源端口范围。

集成服务（保证）策略

字段	描述
策略名称	为此策略指定的名称。
协议	UDP 或 TCP
目标地址	确定受此策略控制的信息包的目标点的地址范围。
平均记号速率限制	沿连接路径的每个路由器和服务器中此策略允许的最大记号速率。
记号深度限制	沿连接路径的每个路由器和服务器中此策略允许的最大记号缓冲区大小。
最大记号速率限制	此连接允许的最大速率。
总信息包数	从启动此策略的时间到监控集合的时间，以此策略传送的信息包数。
总位数	从启动此策略的时间到监控集合的时间，此策略使用的已传送的位数。
不符合要求的位数	已传送的超过策略参数的位数。
保证速率	以位／秒计的保证速率。
符合要求的位数	已传送的符合此策略参数的位数。
最大信息包大小	受此策略控制的最大允许信息包大小。
最小管制单元	将从令牌桶中除去的最小位数。 例如，如果最小管制单元为 100 位，则仍将以 100 位除去 100 位以下的信息包。
符合要求的信息包数	已传送的符合此策略参数的 IP 信息包数。

缓冲期	期望的延迟与获得的延迟之间的差（以秒计）。
源端口范围	确定哪些应用程序受此策略控制的源端口范围。

连接速率策略

字段	描述
策略名称	为此策略指定的名称。
连接速率	每秒接受的连接请求数。
总请求数	对此服务器作出的连接请求总数。
接受的请求数	此服务器接受的连接请求总数。
删除的请求数	此服务器删除的请求总数。
平均连接速率限制	每秒允许的平均容许新连接请求数。
连接脉冲串传输限制	同时接受的最大新连接请求数。
最大连接速率限制	服务器从网络接受连接的最大容许速率。
优先级	为 “QoS 管理器” 中装入的每个规则指定的优先级。
队列优先级	为置于收听队列中的入局连接指定的优先级。
目标端口范围	服务器上为流量指定的端口范围或端口。
接口地址	所监控的系统接口的 IP 地址。
源地址范围	向服务器发送请求的客户机的 IP 地址范围。

服务器请求 — URI 策略

字段	描述
策略名称	为此策略指定的名称。
请求速率	每秒接收的请求数。
总请求数	目标服务器接收的总请求数。
接受的请求数	接受的总请求数。
删除的请求数	删除的总请求数。
URI	所管制的 URI 的标识。
平均请求速率限制	每秒允许的平均容许新请求数。
请求突发限制	同时接受的最大新请求数。
最大请求突发限制	服务器从网络接受请求的最大容许速率。
队列优先级	为置于收听队列中的入局连接指定的优先级。
目标端口	服务器上为流量指定的端口。
接口地址	所监控的系统接口的 IP 地址。

QoS 故障诊断

此子主题为 QoS 问题提供故障诊断建议。

通信跟踪
服务器提供通信跟踪来收集通信线路（如局域网（LAN）或广域网（WAN）接口）上的数据。一般用户可能不了解跟踪数据的整个内容。但是，您可以使用跟踪项来确定两个点之间的数据交换实际上是否发生。有关更多信息，参见“TCP/IP 故障诊断”主题中的通信跟踪。

在服务器上启用 QoS
如果 QoS 服务器未启动，首先要使用 CHGTCP 命令检查 IPQOSENB 的值。当第一次配置策略时，“初始配置”向导自动在服务器上启用 QoS。如果由于任何原因而更改此值，则服务器将不启动。从命令行界面，输入 CHGTCPA IPQOSENB(*YES)。

将 QoS 策略记入日志
服务质量功能包括日志记录功能部件。可以使用日志记录来记录服务器上添加、除去或修改的 IP 策略。这使您能够调试、抽样检查策略和验证策略是否如计划的那样工作。

记录 QoS 策略
当遇到服务器问题时，可能需要分析作业记录。

监控服务器事务
QoS 监控器应该是查找和更正 QoS 问题的首要位置。它记录并使您能够查看 QoS 性能信息。

跟踪 TCP 应用程序
使用跟踪命令来记录几个级别的服务器操作。当尝试确定 QoS 策略问题时，这可能很有帮助。

排序 QoS 策略
文件中策略的顺序对于成功实现服务质量很重要。

将 QoS 策略记入日志

QoS 包括日志记录功能。日志记录允许您跟踪 QoS 策略操作，如添加、除去或修改策略的时间。只要将日志记录设置为“打开”，它就创建策略操作的记录。这有助于您调试和抽查策略工作不如意的方面。例如，将策略设置为从上午 9:00 至下午 4:00 运行。可以检查日志记录，查看实际上该策略是否在上午 9:00 添加并且在下午 4:00 除去。

如果打开了日志记录，则每当添加、除去或修改策略时，均会生成日志项。通过使用这些日志，在 iSeries 服务器上创建一个常规文件。然后可以使用系统日志中记录的信息来确定正在如何使用系统。这可以帮助您决定更改策略的各个方面。

可以选择要记入日志的内容。日志记录可能是系统资源的沉重负载。要启动或停止日志记录，使用“iSeries 导航器”。要查看日志记录，必须使用基于字符的界面。

要启动或停止日志记录，请执行以下操作:

1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
2. 右键单击**服务质量**并选择**配置**。
3. 右键单击 **QoS** 并选择**特性**。
4. 选择**运行日志记录**框打开日志记录。
5. 取消选择**运行日志记录**框关闭日志记录。

注意: 如果在完成以上步骤之前已启动服务器，则必须停止并重新启动服务器。一旦已打开日志记录，有两种方式激活它。可以停止并重新启动服务器或执行服务器更新。这两种方式都重新读取 policy.conf 文件并查找日志记录属性。

在监控器上查看日志项

要在屏幕上查看这些日志项，请执行以下操作:

1. 在 iSeries 服务器的命令提示符处输入: `DSPJRN JRN(QUSRSYS/QQOS)`。在您要查看的日志项上选择**选项 5**。

通过输出文件查看日志项

如果要查看格式化到一个文件夹中的日志项，查看 QUSRSYS 目录中的 MODEL.OUT 文件。通过将日志项复制到输出文件，可以使用 Query/400 或 SQL 等查询实用程序方便地查看这些项。还可以编写自己的 HLL 程序来处理输出文件中的项。

要将 QoS 日志项复制到系统提供的输出文件:

1. 在用户库中创建系统提供的输出文件 QSYS/QATOQQOS 的副本。可以使用“创建重复对象”（CRTDUPOBJ）命令执行此操作。以下是 CRTDUPOBJ 命令的一个示例:

   ```
   CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(userlib) NEWOBj(userfile)
   ```

2. 使用“显示日志”（DSPJRN）命令将 QUSRSYS/QQOS 日志中的项复制到先前步骤创建的输出文件。如果试图将 DSPJRN 复制到不存在的输出文件，系统会为您创建一个文件，但此文件不包含适当的字段描述。

   a. `DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(userlib/userfile)`

   b. `DSPF FILE(userlib/userfile)`

记录 QoS 服务器作业

当您遇到 QoS 策略问题时，应总是分析 iSeries 服务器作业记录。作业记录包含错误消息以及与 QoS 相关的其它信息。

只有一个 QoS 作业 QTOQSRVR 在子系统 QSYSWRK 中运行。可以使用“iSeries 导航器”查看旧的和当前的 QoS 服务器作业记录。

要查看记录，请执行以下操作:

1. 展开**网络**并单击 **IP 策略**。
2. 右键单击**服务质量**。
3. 选择**诊断工具 —> QoS 服务器记录**。

这将打开一个窗口，允许您使用作业。

以下列表显示最重要的作业名称以及有关作业用途的简要说明:

QTCP
此作业是基本作业，它启动所有 TCP/IP 接口。如果遇到 TCP/IP 的基本问题，则分析 QTCPIP 作业记录。

QTOQSRVR
此作业是基本 QoS 作业，它提供特定于 QoS 的记录信息。运行（处理假脱机文件）WRKSPLF QTCP 并查找 QTOQSRVR 记录。

要检查工作假脱机文件是否有错误，执行以下任务:

1. 从命令行界面输入 **WRKSPLF QTCP** 并按执行键。
2. 显示“使用所有假脱机文件”窗口。在“用户数据”列中，查找 QTOQSRVR 以查找特定于 QoS 服务器的错误。
3. 在要显示的行上选择**选项 5**。通读此信息并记录说明问题的“消息标识”。例如，TCP920C。
4. 按两次 **F3** 键返回主菜单。
5. 从命令行界面输入 **WRKMSGF** 并按**执行**键。
6. 在“使用消息文件”屏幕上，输入以下信息并按**执行**键。
   消息文件: QTCPMSG
   库: *LIBL
7. 在“使用消息文件”屏幕上，选择**选项 5** 以显示要查看的消息文件，然后按**执行**键。
8. 在“显示消息描述”屏幕上，输入以下信息:
   定位至: 输入以上步骤 3 中的消息标识并按执行键。例如，TCP920C。
9. 在所需消息标识上选择**选项 5**，然后按**执行**键。
10. 在“选择要显示的消息详细信息”中，选择 30（以上所有消息）并按**执行**键。
11. 显示消息的详细描述。

监控服务器事务

QoS 监控器可以在 QoS 的计划阶段和故障诊断阶段对您有所帮助。

您可以使用监控器分析流经服务器的 IP 流量。这有助于确定网络中发生拥塞的位置。QoS 监控器可以帮助继续监控网络，以便您可以在需要时调整策略。

计划和维护性能

实现 QoS 最困难的部分之一是确定要在策略中设置什么性能限制。这方面没有特定建议，因为网络各不相同。为帮助确定适合于您的值，在开始任何特定于业务的策略之前，您可能需要使用监控器。

尝试创建区分服务策略而不选择测量方法来标识当前网络流量行为。启用此策略并启动监控器。监控器的结果可以帮助您根据特定需要来调整策略。参见将标识当前流量行为的样本监控策略。

性能问题故障诊断

还可以使用监控器来对问题进行故障诊断。使用监控器输出，可以确定系统是否遵循您为策略指定的参数。有关监控器输出的某些示例，访问 QoS 方案，或查看监控中的所有监控器字段。

监控当前的网络统计信息

问题

向导要求您设置性能限制。这些值是不能建议使用的值，因为它们基于单独网络需求。要设置这些限制，确实需要了解当前网络性能。由于正在尝试配置服务质量策略，您可能已经相当了解当前网络需求。要确定令牌桶速率等精确速率限制，可能需要监控服务器上的所有流量，以便可以更好地确定设置什么样的速率限制。

解决方案

创建十分广泛的区分服务策略。它不包含约束（无最大值），并且适用于所有接口和所有 IP 地址。使用 QoS 监控器记录有关此策略的数据。

步骤 1: 在“iSeries 导航器”中打开 QoS。

1. 在“iSeries 导航器”中，展开服务器 —> **网络 —> IP 策略**。
2. 右键单击**服务质量**并选择**配置**。
3. 展开**出站带宽策略**。
4. 右键单击 **DiffServ** 并选择**新建策略**。 “新建 DiffServ 策略”向导出现。

步骤 2: 创建区分服务策略

由于要收集进入网络的大多数流量，所以可以将该策略称为**网络**。使用所有 IP 地址、所有端口、所有本地 IP 地址以及所有时间（如果适当）。在向导中使用以下设置:

名称 = 网络（可以是您指定的任何名称）
客户机 = 所有 IP 地址
应用程序 = 所有端口
协议 = 所有协议
调度表 = 所有时间

“iSeries 导航器”列示服务器上创建的所有区分服务策略。

步骤 3: 完成新的服务类

完成该向导时，需要指定逐跳行为、性能限制以及概要文件外流量处理。这在服务类中定义。选择非常大的值以允许尽可能多的流量流。

服务类实际上确定此流量从路由器接收到的性能级别。可以指定**无限制**服务类，以显示此流量接收更高级的服务。 “iSeries 导航器”列示服务器上定义的所有服务类。

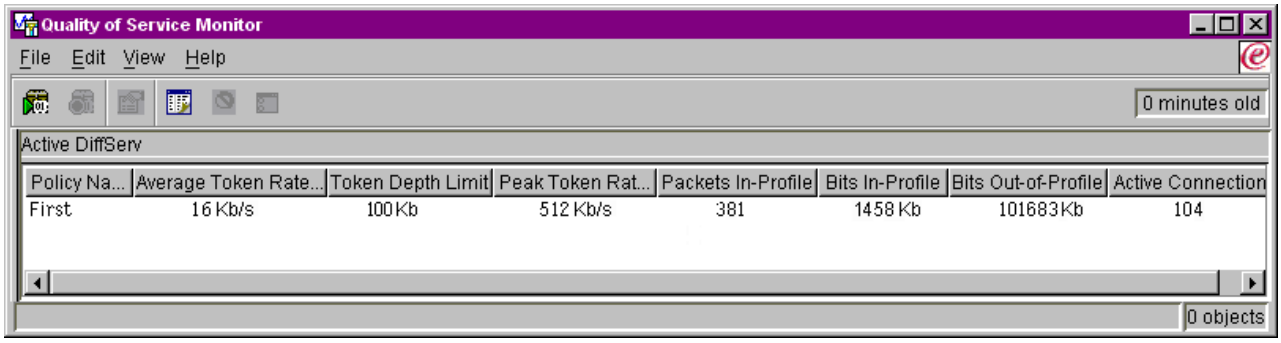
步骤 4: 监控策略

要验证流量的行为是否符合您在策略中配置的行为，使用监控器。

1. 选择特定的“策略”文件夹（DiffServ、IntServ、服务器请求 —> URI 或连接速率）。
2. 右键单击要监控的策略并选择**监控器**。

下面是以上设置的策略的可能监控器输出列表。

图 14. 服务质量监控器。



查找从流量获取数据的字段。确保检查总位数、概要文件内位数、概要文件内信息包数以及概要文件外位数等字段。概要文件外位数指示流量何时超过配置的策略值。在区分服务策略中，概要文件外数字指示删除的字节数。概要文件内信息包数指示此策略控制的字节数（从启动信息包的时间到当前监控器输出）。

在平均记号速率限制字段中所指定的值也很重要。当信息包超过此限制时，服务器将开始删除它们。因此，概要文件外位数将增加。这显示策略的行为与您为它配置的行为相同。要更改概要文件外位数，需要调整性能限制。有关所有监控器字段的描述，参见监控器一节。

步骤 5: 需要时修改值

监控之后，可以修改先前选择的任何值。右键单击在此策略中创建的服务类名称。当选择**特性**时，“CoS 特性”对话框出现，其中包含控制流量的值。

步骤 6: 再次监控策略

在查看结果之后，使用“猜测与检查”方法查找适合您的网络需要的最佳限制。 

跟踪 TCP 应用程序

使用 QoS 跟踪来使用跟踪功能以及查看当前跟踪缓冲区。要在服务器上运行跟踪，输入 TRCTCPAPP。此处是要完成的跟踪选择的一个样本:

```
TCP/IP 应用程序...........> *QOS
跟踪选项设置.................> *ON
最大跟踪存储量...............> *APP
跟踪已满操作.................> *WRAP
自变量列表...................> 'lvl=4'
QoS 跟踪类型.................> *ALL
```

下表介绍在跟踪中可能要使用的参数。如果设置不出现在基于字符的界面中，则必须以命令方式输入它们。例如，TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i')。

设置	选项
TCP/IP 应用程序	QOS
跟踪选项设置	*ON、*OFF、*END 和 *CHK
最大跟踪存储量（MAXSTG）	1-16000，*APP
跟踪已满操作（TRCFULL）	*WRAP，*STOPTRC
自变量列表（ARGLIST）	级别: 'lvl=1'、'lvl=2'、'lvl=3' 和 'lvl=4' 内容: 'c=a'、'c=i'、'c=d'、'c=m'、'c=r' 和 'c=s'
QoS 跟踪类型	*ALL

如果需要帮助解释跟踪输出，参见阅读跟踪输出。跟踪输出页面包含带有注释的样本输出以帮助您解释其含义。

最大跟踪存储量

1-16000

这是跟踪数据的最大存储大小。当达到此大小时，跟踪停止或回绕。缺省大小是 4MB。要指定缺省大小，选择 *APP。

***APP**
这是缺省选项。它告诉应用程序使用其缺省跟踪大小。QoS 服务器的缺省跟踪大小是 4MB。

跟踪已满操作

***WRAP**
当跟踪达到最大磁盘空间（跟踪缓冲区大小）时，回绕跟踪信息。回绕将使系统能够覆盖文件中最早的信息，以便您继续记录跟踪信息。如果不选择回绕，则当磁盘已满时，跟踪操作停止。

***STOPTRC**
当系统达到最大磁盘空间时，停止收集信息。

自变量列表

指定将记录哪些错误级别和内容。在 TRCTCPAPP 命令中允许使用两个自变量：跟踪级别和跟踪内容。当指定跟踪级别和跟踪内容时，确保所有属性都包含在一组引号中。例如，`TRCTCPAPP 'l=1 c=a'`

注意：记录级别是具有包含性的。这表示当选择一个记录级别时，也选择了所有先前的记录级别。例如，如果选择级别 3，则自动包括级别 1 和 2。 **跟踪级别**

级别 1：系统错误（SYSERR）
记录系统操作中发生的错误。如果此错误发生，QoS 服务器不能继续。例如，如果用尽系统内存或系统不能与 TCP/IP 通信，则系统错误可能发生。

级别 2：对象之间的错误（OBJERR）
记录 QoS 服务器代码中发生的错误。例如，因为服务器操作遇到某些意外的结果，对象错误可能发生。这通常是应该报告来维护的严重情况。

级别 3：特定事件（EVENT）
记录发生的任何 QoS 操作。例如，事件记录将记录命令和请求。结果与 QoS 日志记录功能类似。

级别 4：跟踪消息（TRACE）
跟踪传送至 QoS 服务器和从 QoS 服务器传送的所有数据。例如，可以使用此高级别跟踪记录您认为将有助于调试问题的任何数据。此信息有助于确定问题发生的位置和如何重现问题。

跟踪内容

注意：仅指定一种内容类型。如果不指定跟踪什么内容，则（缺省情况下）将跟踪所有内容。

Content = All ('c=a')
跟踪 QoS 服务器的所有功能。这是缺省值。使用此值开始查找问题。

Content = Intserv ('c=i')
仅跟踪 IntServ 操作。如果确定问题与 IntServ 有关，则使用此值。

Content = Diffserv ('c=d')
仅跟踪 DiffServ 操作。如果确定问题与 DiffServ 有关，则使用此值。

Content = Monitor ('c=m')
仅跟踪监控器操作。

Content = Rate ('c=r')
跟踪入站连接速率事件。

Content = Server ('c=s')
跟踪除监控器操作以外的任何内容。这可能很有用，因为监控器跟踪生成许多信息，而这些信息会不必要地搞乱跟踪输出。

有关 TRCTCPAPP 命令的更多完整信息，参见 CL 命令主题中 TRCTCPAPP（跟踪 TCP/IP 应用程序）命令描述。

阅读跟踪输出

这并非是关于如何阅读跟踪输出的全部讨论。但是，它在跟踪信息中突出了要查找的关键事件。

在**集成服务策略**中，要查找的最重要的事件是：是否因为未找到 RSVP 连接的策略而拒绝了 RSVP 连接。以下是一个成功消息示例:

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Found action name vreStnl_kraMoNlCvreStnl for
flow[sess=x.x.x.x:y:z:s, source=x.x.x.x:y]
```

以下是一个失败的集成服务连接消息示例:

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Unable to find action name for flow [sess=x.x.x.x:y]
```

对于**区分服务策略**，最重要的消息显示服务器装入了策略规则还是在策略配置文件中发生了错误。

示例:

```
01/11 14:07:52 [376,57] TRCE :......KernelAddPolicyRule: Installing rule = timed_42ring.
01/11 14:07:52 [376,57] EVNT :.......create_tcp_resv: No value in config file for
DiffServInProfilePeakRate, defaulted to 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
```

也可能会有显示策略配置文件中的标记不正确的消息。此处是一些样本消息:

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Unknown attribute %s in ServicePolicy-Ignoring. 12/15
11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Unknown attribute %s in Priority Mapping-Ignoring.
```

注意: % 符号是表示不可识别的标记的变量。

QoS 的相关信息

有许多关于工业中服务质量的其它信息源。查看最新的 RFC、白皮书、Redbooks(TM) 和其它源来接收关于 QoS 的一般信息。此处是一些要考虑的源:

非 IBM 源

RFC 1349
此 RFC 讨论 IP 信息包头中 TOS 字段的新定义。

RFC 2205
此 RFC 包括“资源预订协议”（RSVP）的定义。

RFC 2210
此 RFC 包括具有 IETF“集成服务”的 RSVP 的使用。

RFC 2474
此 RFC 包括“区分服务字段”（DS 字段）的定义。

RFC 2475
此 RFC 包括区分服务的体系结构。

IBM(R) 红皮书

TCP/IP More Cool Things than Ever
此手册提供样本方案，这些方案演示具有示例配置的公共解决方案。此手册中的信息帮助您计划、安装、定制、配置 iSeries 服务器上的 TCP/IP 以及对其进行故障诊断。它虽然尚未明确地包括“服务质量”，但是，它包括所有 LDAP 目录服务器信息。

TCP/IP Tutorial and Technical Overview
此手册提供协议和应用程序的“传输控制协议／网际协议”（TCP/IP）套件的介绍和参考。将在第 22 章的 *Part 3. Advanced concepts and new technologies* 中找到“服务质量”。

相关的 iSeries 信息中心主题

目录服务（LDAP）
查看此主题来获取目录服务器基本内容、配置、管理和故障诊断。目录服务主题还将给予您配置目录服务器的附加资源。

中国印刷