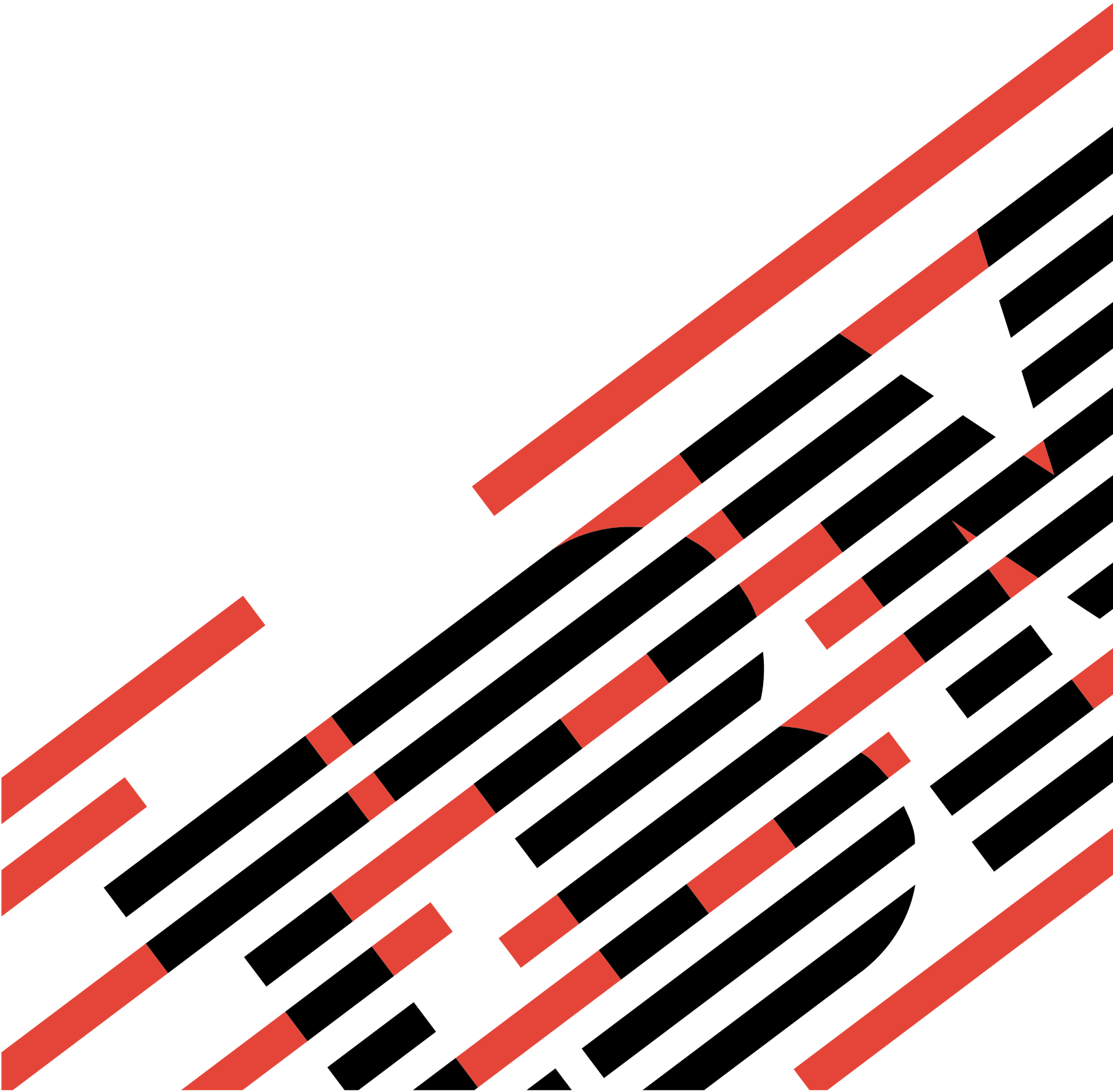
IBM

eserver

iSeries

서비스 품질



IBM

@server

iSeries

서비스 품질

목차

서비스 품질(QoS). 1
V5R2의 새로운 사항 2
이 주제 인쇄 3
QoS 시나리오 3
QoS 시나리오: 전달 전용(IP 전화 통신) 5
QoS 시나리오: 브라우저 통신량 제한 8
QoS 시나리오: 인바운드 연결 제한 11
QoS 시나리오: 예측 가능 B2B 트래픽 14
QoS 시나리오: 보안 및 예측 가능한 결과(VPN 및 QoS) 17
QoS 개념 21
연결 요구 비율 및 URI 요구 비율 21
평균 연결 비율 및 버스트 한계 23
차별화된 서비스 23
차별화된 서비스 클래스 24
코드점 및 홉별 작동 25
통신량 조절기 27
디렉토리 서버 개념 27
키워드 28
통합 서비스 29
통신량 제어 기능 31
통합 서비스 유형 31
토큰 버켓 및 대역폭 한계 32
차별화된 서비스 표시를 사용하는 통합 서비스 33
RSVP 프로토콜 및 QoS API 34
QoS API 연결 지향 기능 흐름 37
QoS API 무접속 기능 흐름 40
QoS 계획 41
권한 요구사항 41
시스템 요구사항 42
QoS 정책 순서화 42
서비스 레벨 계약 43
네트워크 하드웨어 및 소프트웨어 44
QoS 구성 44
디렉토리 서버 구성 45
마법사를 사용하여 QoS 구성 46
iSeries Navigator에서 QoS 마법사에 액세스 47
QoS 관리 48
iSeries Navigator에서 QoS 도움말에 액세스 48
QoS 정책 백업 49
기존 정책 복사 49
QoS 모니터 53
QoS 문제 해결 54
QoS 정책 저널 55

QoS 서버 작업 기록 55
서버 트랜잭션 모니터 56
현재 네트워크 통계 모니터 57
TCP 어플리케이션 추적 60
추적 출력 읽기 62
QoS 관련 정보 62

서비스 품질(QoS)

네트워크에서는 모든 통신에 같은 우선순위를 부여합니다. 중요하지 않은 브라우저 통신 처리도 중요한 비지니스 어플리케이션과 같은 것으로 간주됩니다. 회사의 최고 경영자(CEO)가 오디오/비디오 어플리케이션을 사용하여 프리젠테이션을 준비할 경우, IP 패킷 우선순위가 문제가 될 수 있습니다. 프리젠테이션이 진행되는 동안 다른 어플리케이션보다 이 어플리케이션에 더 높은 성능이 필요하기 때문입니다.

QoS는 TCP/IP 어플리케이션에 대해 네트워크 우선순위와 대역폭을 요구할 수 있게 해 주는 기능입니다. 패킷 우선순위는 멀티미디어와 같이 예측할 수 있고 믿을 수 있는 결과가 요구되는 어플리케이션을 송신할 때 매우 중요합니다.

정책 결과에 대한 계획을 시작하기 전에 QoS를 이해하는 것이 중요합니다. 다음은 QoS를 구현하기 위해 필요한 정보를 제공하는 링크입니다.

V5R2의 새로운 사항
서비스 품질 네트워킹 기능 및 Information Center 주제에 대한 변경 사항을 나열합니다.

이 주제 인쇄
전체 주제를 인쇄하십시오.

QoS 시나리오
QoS를 사용하는 이유와 방법을 알아보려면, 일부 QoS 정책 시나리오를 보십시오.

QoS 개념
QoS(서비스 품질)를 처음 사용하는 초보자의 경우에는 기본 QoS 개념과 메카니즘을 보십시오. 여기서에서는 QoS 작업 방법과 QoS 메카니즘 작업 방법 개요를 함께 제공합니다.

QoS 계획
QoS의 효율적인 사용 방법에 관해 알아보려면, 계획 어드바이저 및 네트워크 정보에 링크하십시오.

QoS 구성
차별화된 서비스 정책과 통합 서비스 정책을 새로 작성하려면 다음 프로시듀어를 수행하십시오.

QoS 관리
기존 정책을 편집하려면, 다음 프로시듀어를 수행하십시오. 다음 항목은 기타 정책 관리 기술을 삭제 및 추적하고 실제로 사용할 타스크가 있는 위치를 알려줍니다.

QoS 문제 해결
QoS 문제를 디버그하려면 문제 해결 섹션을 사용하십시오.

QoS 관련 정보
기타 유용한 QoS 소스에 링크하십시오. 여러 가지 책, 웹 사이트, RFC 및 백서가 있습니다.

V5R2의 새로운 사항

여기에서는 버전 5 릴리스 2에 새롭게 추가된 기능에 대해 설명합니다. 또한 설계 상 개선된 부분에 대해서도 설명합니다.

새로운 기능

- **로컬 인터페이스와 정책 연관**
  iSeries(TM)의 특정 로컬 인터페이스 또는 로컬 인터페이스 범위와 정책을 연관시킬 수 있습니다. 로컬 인터페이스를 지정함으로써 클라이언트 패킷이 도달한 인터페이스를 기반으로 정책이 수행될 수 있습니다.
- **여러 클라이언트와 정책 연관**
  정책을 여러 클라이언트와 연관시킬 수 있습니다. 따라서 보다 유연한 정책 정의를 작성할 수 있습니다.
- **인바운드 수락 정책**
  사용자 서버에 액세스하려고 시도하는 외부 통신을 제어하기 위한 정책을 작성할 수 있습니다. 사용자 네트워크 내의 특정 IP 주소나 URI 값에 액세스하려는 통신을 제어할 수 있도록 두 가지 새로운 마법사가 있습니다. 위의 링크를 사용하여 두 가지 인바운드 정책에 대해 더 자세히 알아 보십시오.
- **모니터 정보 저장 및 인쇄 가능**
  모니터 정보를 저장하고 인쇄할 수 있습니다. 정보를 저장할 때 차후 참조를 위해 액세스할 수 있습니다. 모니터 정보를 인쇄하려면 “HTML로 내보내기”를 지정할 수 있습니다.
- **LDAP 디렉토리 서버에 정책 저장**
  최신 LDAP 프로토콜 버전 3을 사용하여 디렉토리 서버로 정책을 내보낼 수 있습니다. 디렉토리 서버를 사용함으로써 QoS 솔루션 관리가 보다 쉬워졌습니다. 각 서버에서 동일한 QoS 정책을 구성하는 대신 하나의 서버에서 작성된 정책 자료를 사용하도록 서버를 구성할 수 있습니다. 그리고나서 정책은 디렉토리 서버에 저장됩니다. 이 링크를 사용하여 구성에 대한 자세한 내용을 참조하십시오.
- **스케줄 변경**
  스케줄은 시간 범위에 의해 정의됩니다. 이전에는 시간 범위가 동일한 날로 국한되었습니다. 이제 시간 범위가 24시간으로 확장되어 이틀에 걸쳐도 무관하게 되었습니다. 스케줄은 정책 활동 시점을 지정하기 위해 정책에 연관됩니다. 따라서 보다 유연한 정책 정의를 작성할 수 있습니다.

새로운 설계 개선 사항

- **QoS 계획 어드바이저**
  QoS 계획 어드바이저가 갱신되어 정책을 구성하기 전에 사용자에게 제안 및 전제조건을 제시합니다. 이는 조직화된 곳에서 개념을 한데 모아 계획을 세우는 데 사용하면 도움이 됩니다.
- **신규 인바운드 시나리오**
  인바운드 정책 구현의 예를 보여주기 위한 새로운 시나리오가 추가되었습니다.

새로운 사항 및 변경된 사항을 찾는 방법

기술적인 변경 사항을 찾는 데 도움이 되도록 여기에서는 다음을 사용합니다.

- 
  이미지를 사용하여 새로운 정보 또는 변경된 정보가 시작되는 위치를 표시합니다.

- «

  이미지를 사용하여 새로운 정보 또는 변경된 정보가 끝나는 위치를 표시합니다.

이 릴리스에서 새로운 사항이나 변경된 사항에 대한 다른 정보를 찾아 보려면 사용자 메모  를 참조하십시오.

이 주제 인쇄

PDF 버전을 보거나 다운로드하려면 서비스 품질(약 378KB 또는 53 페이지)을 선택하십시오.

보기 또는 인쇄하기 위해 워크스테이션에 PDF를 저장하려면 다음을 수행하십시오.

1. 브라우저에서 PDF를 여십시오(위의 링크 클릭).
2. 브라우저 메뉴에서 **파일**을 클릭하십시오.
3. **다른 이름으로 저장...**을 클릭하십시오.
4. PDF를 저장하려는 디렉토리로 이동하십시오.
5. **저장**을 클릭하십시오.

PDF를 보거나 인쇄하기 위해 Adobe Acrobat Reader가 필요한 경우, Adobe Web site  에서 다운로드할 수 있습니다.

QoS 시나리오

서비스 품질에 대한 가장 좋은 학습 방법은 귀사의 전체 네트워크 그림 안에서 그 기능이 어떻게 작동하는지를 알아 보는 것입니다. 다음은 서비스 품질 정책을 사용하는 이유에 관한 기본적인 예입니다.

»

시나리오: 전달 전용(IP 전화 통신)
전달 전용으로 필요하거나 예약을 요구하려는 경우 통합 서비스 정책을 사용합니다. 작성할 통합 서비스 정책에는 보장 서비스 및 제어를 받는 로드 서비스의 두 가지 유형이 있습니다. 이 예에서는 보장 서비스를 사용합니다.

시나리오: 브라우저 통신량 한계
통신량 성능을 제어하기 위해 QoS를 사용할 수 있습니다. 차별화된 서비스 정책을 사용하여 어플리케이션의 네트워크 내 성능을 제한하거나 확장할 수 있습니다.

시나리오: 인바운드 연결 제한
서버에 대한 인바운드 연결 요구를 제어해야 하는 경우 인바운드 수락 정책을 사용하십시오.

시나리오: 예측 가능한 B2B 통신량
예측 가능한 전달이 필요하거나 예약을 요구해야 하는 경우에도 통합 서비스 정책을 사용합니다. 그러나 이 예에서는 제어를 받는 로드 서비스를 사용합니다.

시나리오: 보안 및 예측 가능한 결과(VPN 및 QoS)
VPN(가상 사설망)을 사용하는 경우, 서비스 품질 정책을 작성할 수 있습니다. 다음 예는 함께 사용되는 두 가지를 모두 보여줍니다.

«

주: IP 주소 및 다이어그램은 가공의 것으로 단지 예제로만 사용된 것입니다.

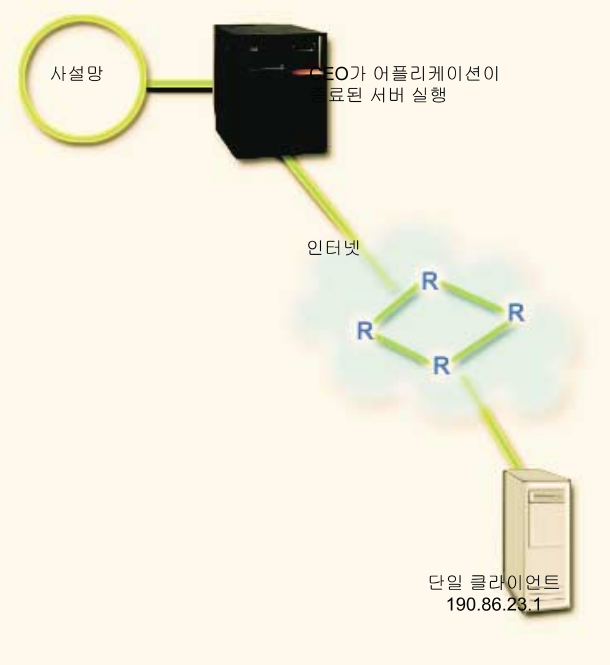
QoS 시나리오: 전달 전용(IP 전화 통신)

»

문제점

귀사의 최고 경영자(CEO)가 오후 1시부터 오후 2시 사이에 한 클라이언트에게 라이브로 방송을 내보내려고 합니다. 따라서 IP 전화 통신에 대역폭을 보장하여 방송 중에 어떤 간섭도 받지 않도록 해야 합니다. 이 시나리오에서는 어플리케이션이 서버에 상주합니다. 다음 그림은 이 시나리오에서의 네트워크 설정을 보여줍니다. iSeries 서버에서는 OS/400(R) V5R2가 실행 중입니다.

그림 1. 통합 서비스 정책으로 보장되는 클라이언트에 대한 CEO 프리젠테이션.



솔루션

매우 민감한 어플리케이션에는 보장된 연결이 필요합니다. CEO가 사용 중인 어플리케이션은 유연하고 막힘없는 전송 처리가 필요하므로 보장된 통합 서비스 정책을 사용하기로 결정합니다. 보장 서비스는 최대 대기행렬 지연을 제어하므로 패킷은 지정된 시간 이상 지연되지 않습니다.

사용자가 이와 같은 연결을 보장하고자 하기 때문에 보장 서비스를 제공하는 통합 서비스를 사용할 수 있습니다. 통합 서비스 정책에는 RSVP 작동 가능 어플리케이션이 필요합니다. 서버에는 RSVP 작동 가능 어플리케이션이 없으므로 직접 RSVP 작동 가능 어플리케이션을 작성해야 합니다. 직접 어플리케이션을 작성하려면 자원 예약 설치 프로토콜(RAPI) API 또는 qtoq QoS 소켓 API를 사용하십시오.

통합 서비스 정책의 경우 통신 경로와 함께 라우터도 RSVP 작동 가능 상태가 되어야 합니다. 자세한 정보는 통합 서비스 개념 섹션을 참조하십시오.

구성

1. iSeries Navigator에서 QoS를 여십시오.
    1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
    2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭한 후 **구성**을 선택하십시오.
    3. **아웃바운드 대역폭 정책**을 확장하십시오.
    4. **IntServ**를 마우스 오른쪽 버튼으로 클릭하고 **신규 정책**을 선택하십시오. 새로운 IntServ 정책 마법사가 표시됩니다.

2. 통합 서비스 정책을 작성하십시오.

   첫 번째 단계는 통합 서비스 정책 마법사를 완료하는 것입니다. CEO로부터의 통신을 보장하고자 하므로 이 정책을 **CEO_guaranteed**라고 할 수 있습니다. 현재 단일 클라이언트가 IP 주소, **190.86.23.1**에서 이 프리젠테이션을 수신하는 중입니다. 이것은 하나의 예로 사용한 번호입니다. 클라이언트를 **Branch1**으로 명명하십시오. 통신이 포트 2427에서 실행되므로 어플리케이션을 포트 **2427**로 명명하십시오. 그리고 스케줄을 **1:00-2:00**로 명명하십시오. 마법사에는 다음 값을 사용하십시오.

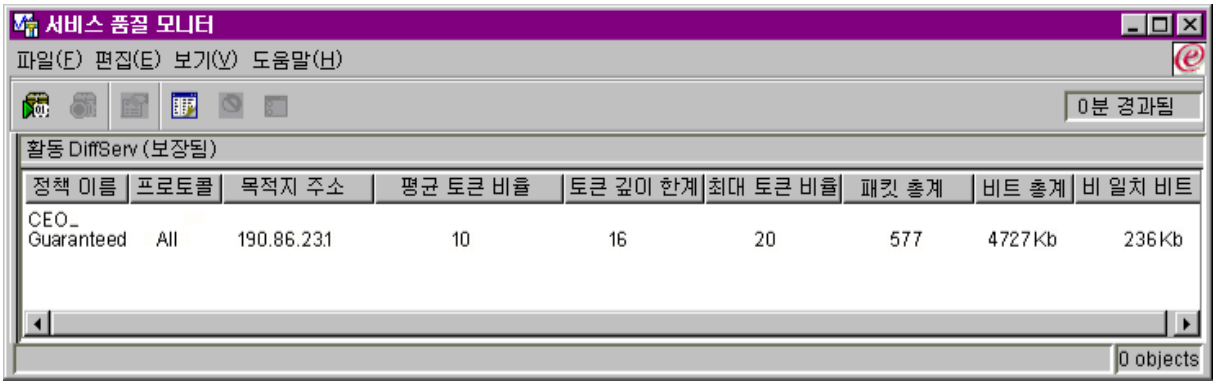
   이름 = CEO_guaranteed
   클라이언트 = Branch1
   어플리케이션 = 포트 2427(이것이 IP 전화 통신이 실행되고 있는 포트인 경우)
   로컬 **IP** 주소 = 10.5.27.1
   프로토콜 = TCP
   스케줄 = 1:00-2:00
   토큰 버켓 크기 = 16킬로비트
   대역폭 한계**(R)** = 초당 10메가비트
   흐름 수 = 1

   iSeries Navigator는 사용자 서버에서 작성된 통합 서비스 정책을 모두 나열합니다.

4. 모니터를 사용하여 정책이 작동 중인지 확인하십시오.
   1. 특정 정책 폴더를 선택하십시오(DiffServ, IntServ, 서버 요구 —> URI 또는 연결 비율).
   2. 모니터하려는 정책을 마우스 오른쪽 버튼으로 클릭하고 **모니터**를 선택하십시오.

   다음은 결과를 설명하는 주석이 있는 모니터 출력 대화상자입니다.

   그림 2. 서비스 품질 모니터



   가장 중요한 필드는 통신으로부터 자료를 얻는 측정된 필드입니다. 이러한 필드에는 총 비트 수, 적합한 비트 수 및 적합한 패킷 수 등이 있습니다. 부적합 비트 수는 이 통합 서비스 정책 요구사항을 충족시키기 위해 다른 통신이 지연되거나 드롭(drop)되는 경우 표시됩니다. 모든 모니터 필드에 대한 설명은 모니터 절을 참조하십시오.

3. 조정이 필요한 값을 모두 수정하십시오.

이 정책에 대한 모니터 결과를 본 후에는 마법사에서 이전에 작성한 값을 수정할 수 있습니다.

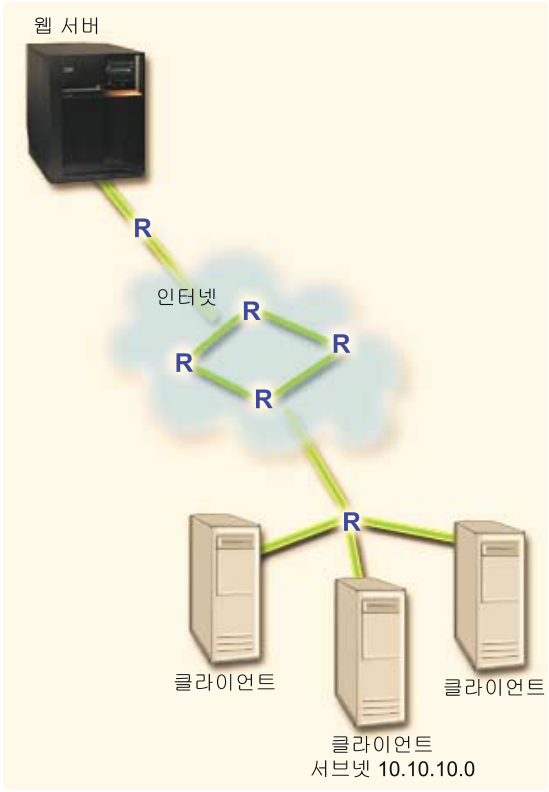
1. 모니터를 닫으십시오.
2. 위에서 작성한 정책 이름을 마우스 오른쪽 버튼으로 클릭하십시오.
3. **등록 정보**를 선택하면 IntServ_Guaranteed 등록 정보 대화 상자가 표시됩니다.
4. 통신 흐름을 제어하는 값을 변경하려면, **흐름 제어** 탭을 선택하십시오. 여기에서 스케줄, 클라이언트, 어플리케이션 및 통신 관리를 편집할 수 있습니다.

QoS 시나리오: 브라우저 통신량 제한

문제점

현재 귀사에서는 금요일마다 사용자 중심 설계(UCD) 그룹으로부터 과도한 브라우저 통신량이 발생합니다. 이로 인해 회계 부서의 업무에 차질을 빚게 되는데, 금요일은 회계 어플리케이션에 있어서 높은 성능이 요구되는 날입니다. 따라서 UCD 그룹으로부터의 브라우저 통신량을 제한하기로 결정합니다. 다음 그림은 이 시나리오에서의 네트워크 설정을 보여줍니다. iSeries 서버에서는 OS/400(R) V5R2가 실행 중입니다.

그림 3. 클라이언트로의 브라우저 통신량을 제한하는 웹 서버



솔루션

네트워크 밖으로부터의 브라우저 통신량을 제한하기 위해 차별화된 서비스 정책을 작성할 수 있습니다. 차별화된 서비스 정책은 통신량을 클래스로 나눕니다. 이 정책의 모든 통신량에 코드점이 지정됩니다. 이 코드점이 라우터에게 통신량의 처리 방법을 지시합니다. 이 시나리오에서는 네트워크가 브라우저 통신량에 우선순위를 지정하는 방법에 영향을 미치도록 낮은 코드점을 정책에 할당할 수 있습니다.

구성

1. iSeries Navigator에서 QoS를 여십시오.
    1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
    2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭한 후 **구성**을 선택하십시오.
    3. **아웃바운드 대역폭 정책**을 확장하십시오.
    4. **DiffServ**를 마우스 오른쪽 버튼으로 클릭하고 **신규 정책**을 선택하십시오. 새로운 DiffServ 정책 마법사가 표시됩니다.
2. 차별화된 서비스 정책을 작성하십시오.

    UCD 그룹에 대해 브라우저 통신량을 제한할 것이므로, **UCD** 정책을 호출해야 합니다. 클라이언트는 서브네트 주소 **10.10.10.0**을 사용합니다. 이것은 하나의 예로 사용된 번호입니다. 일반적으로 웹 통신을 포

트 80에서 실행하므로 어플리케이션을 **포트 80**으로 지정할 수 있습니다. 금요일에만 과도한 통신량이 발생하므로, 오전 9:00 - 오후 5:00 스케줄을 정책에 적용할 수 있습니다. 이름을 **Friday9-5**로 지정할 수 있습니다. 마법사에서 다음 설정을 사용하십시오.

이름 = UCD(사용자가 지정한 이름)
클라이언트 = 서브네트 10.10.10.0
어플리케이션 = 포트 80(HTTP 통신에 잘 알려진 포트)
프로토콜 = TCP
스케줄 = Fridays9-5

계속 진행하면서 자동으로 표시될 서비스 클래스 마법사로부터 나머지 정책 정보를 입력하십시오.

토큰 버켓 크기 = 8킬로비트
평균 비율 한계 = 초당 10메가비트
최고 비율 한계 = 초당 20메가비트
프로파일 외부 통신량 넘침 처리 = 패킷 드롭(다시 전송됨)

iSeries Navigator는 사용자 서버에서 작성된 차별화된 서비스 정책을 모두 나열합니다. 마법사가 완료되면 정책은 오른쪽 분할 창에 표시됩니다.

3. 새로운 서비스 클래스를 완료하십시오.

마법사를 완료하는 동안 홉별 작동, 성능 한계 및 프로파일 외부 통신량 처리를 지정할 것을 요청받습니다. 이것은 서비스 클래스에 정의되어 있습니다.

실제로 서비스 클래스가 통신량이 라우터에서 수신되는 성능 레벨을 결정합니다. 통신에서 낮은 서비스를 수신하는 것을 보여주기 위해 서비스 클래스를 **Bronze**로 지정할 수 있습니다. iSeries Navigator는 사용자 서버에서 정의된 서비스 클래스를 모두 나열합니다.

서비스 클래스 이름 = Bronze

4. 유효한 정책을 확인하려면 모니터를 사용하십시오.

정책에 사용자가 구성한대로 그 정책이 작동하는지 확인하려면, 모니터를 사용하십시오.

1. 특정 정책 폴더를 선택하십시오(DiffServ, IntServ, 서버 요구 —> URI 또는 연결 비율).
2. 모니터하려는 정책을 마우스 오른쪽 버튼으로 클릭하고 **모니터**를 선택하십시오.

다음은 결과를 설명하는 주석이 있는 모니터 출력 대화상자입니다.

그림 4. 서비스 품질 모니터

가장 의미있는 필드는 통신으로부터 자료를 얻는 필드입니다. 반드시 총 비트 수, 프로파일 내부 비트 수 및 프로파일 내부 패킷 수 필드를 검사하십시오. 프로파일 외부 비트 수는 통신량이 구성된 정책 값을 초과할 때 표시됩니다. 차별화된 서비스 정책에서 프로파일 외부 수치는 드롭(drop)된 비트 수를 나타냅니다. 프로파일 내부 패킷은 이 정책에 의해 제어되는 비트 수를 나타냅니다(패킷이 시작된 시간부터 현재 모니터 출력 시간까지).

평균 비율 한계 필드에 지정한 값 역시 중요합니다. 패킷 수가 이 한계를 초과할 때부터 서버가 드롭을 시작합니다. 그 결과 프로파일 외부 비트 수가 증가합니다. 이것은 사용자가 구성한대로 정책이 작동하는 것을 보여줍니다. 모든 모니터 필드에 대한 설명은 모니터 절을 참조하십시오.

5. 이 정책에 적용하지 않는 값을 모두 변경하십시오.

   정책에서 작성한 값은 모두 수정할 수 있습니다.

   1. 모니터를 닫으십시오.
   2. 왼쪽 분할 창에서 서비스 클래스를 선택하십시오.
   3. 오른쪽 분할 창에서 위에서 작성한 서비스 클래스 이름을 마우스 오른쪽 버튼으로 클릭하십시오.
   4. **등록 정보**를 선택하십시오. CoS 등록 정보 대화상자에 통신을 제어하는 값이 표시됩니다. 적절한 값을 수정하십시오.

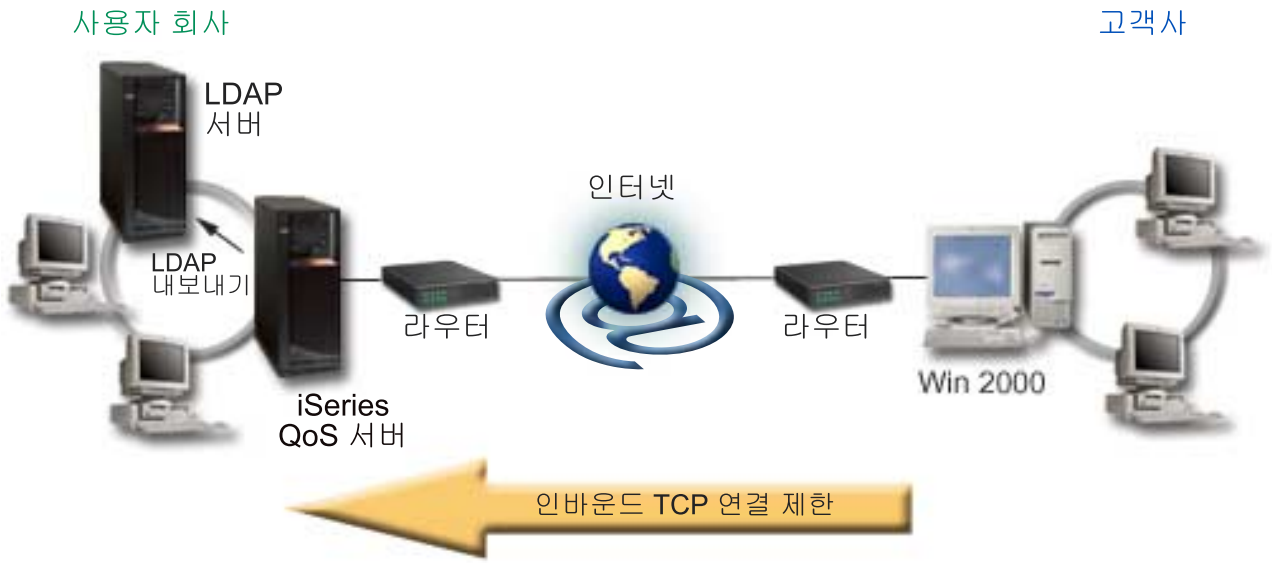
QoS 시나리오: 인바운드 연결 제한

문제점

웹 서버 자원이 네트워크로 들어가는 클라이언트 요구에 의해 과부하되는 경우입니다. 로컬 인터페이스 10.1.1.1에서 웹 서버(10.1.1.4)로 수신되는 HTTP 통신량을 지연시켜 달라는 요청을 받습니다. QoS를 사용하여 사용자 서버에 대한 연결 속성(예를 들면 IP 주소)에 근거하여 수락되는 인바운드 연결 수를 제한할 수 있습니다. 이를 위해 인바운드 수락 정책을 구현하기로 결정하고 이는 수락되는 인바운드 연결 수를 제한합니다.

일러스트레이션에서는 귀사 및 고객사를 보여줍니다. 이 QoS 정책으로만 한 방향에서 통신 흐름을 제어할 수 있습니다.

그림 5. 인바운드 TCP 연결 제한



전제조건:

- iSeries V5R2 실행
- LDAP 서버 구성 및 실행

솔루션

인바운드 정책을 구성하려면 통신을 로컬 인터페이스로 제한할 것인지 특정 어플리케이션으로 제한할 것인지를 결정하고 특정 클라이언트로부터 이를 제한할 것인지 여부도 결정해야 합니다. 이 경우 Their_Company로부터 포트 80(HTTP 프로토콜)으로 들어가는 연결 시도를 사용자의 로컬 인터페이스 10.1.1.1에서 제한하는 정책을 작성하고자 할 것입니다. IP 주소에 의해 이 한계를 정의하므로 연결 비율 정책을 작성해야 합니다. 인바운드 수락 정책에는 연결 비율 및 서버 요구(URI)의 두 가지 유형이 있습니다. URI 정책은 특정 상대 URI 이름(상대 URL과 비슷함) 또는 시스템의 모든 URL에 액세스하기 위한 연결 시도를 제한합니다. URI 정책에 대한 자세한 내용은 인바운드 수락 정책을 참조하십시오.

이 연결 비율 정책을 작성하고 위의 시나리오를 완료하려면 iSeries Navigator를 열고 QoS 기능으로 가십시오.

구성

1. iSeries Navigator에서 QoS를 여십시오.
    1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.

2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭한 후 **구성**을 선택하십시오.
3. **인바운드 수락 정책**을 확장하십시오.
4. **연결 비율**을 마우스 오른쪽 버튼으로 클릭하고 **신규 정책**을 선택하십시오.

2. 연결 비율 정책 마법사를 완료하십시오.

   두 번째 단계는 새로운 연결 비율 정책 마법사를 완료하는 것입니다. Their_Company로부터의 통신량을 제한하려고 하므로 정책 이름을 **Restrict_TheirCompany**로 지정할 수 있습니다. 사용자는 클라이언트인 Their_Company로부터 로컬 IP 주소 10.1.1.1로 수신되는 요구를 제한하고자 합니다. 이것은 하나의 예로 사용된 번호입니다. 이 통신은 포트 80에서 실행되므로 어플리케이션의 이름을 **포트 80**이라고 지정할 수 있습니다. 스케쥴 이름은 **Weekdays(9-5)**로 지정할 수 있습니다. 마법사에는 다음 값을 사용하십시오.

   이름 = Restrict_TheirCompany
   클라이언트 = Their_Company
   어플리케이션 = 포트 80
   로컬 **IP** 주소 = 10.1.1.1
   스케줄 = Weekdays(9-5)
   평균 연결 비율 = 초당 100
   연결 버스트 비율 = 5 연결
   우선순위 = 보통

   iSeries Navigator는 사용자 서버에서 작성된 연결 비율 정책을 모두 나열합니다.

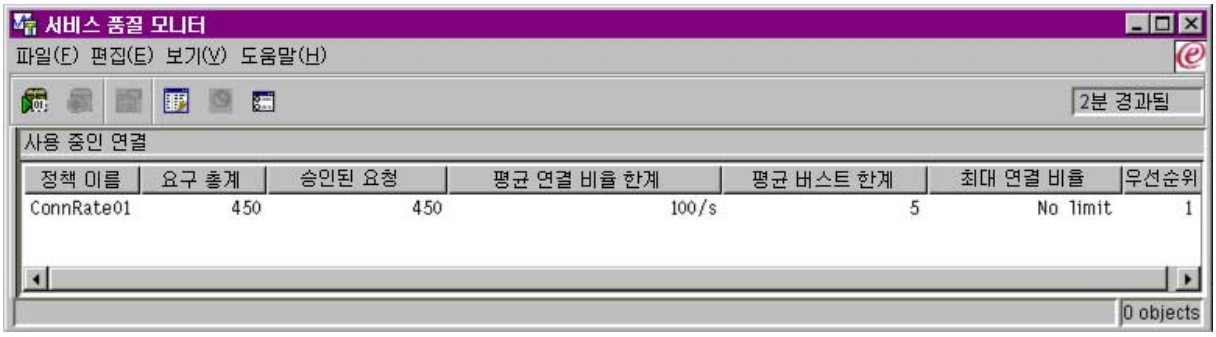
3. 이 정책에 포함된 통신을 모니터하여 원하는 결과를 얻을 수 있는지 확인하십시오.

   정책이 사용자가 구성한대로 작동하는지 확인하려면, 모니터를 사용하십시오.

   1. 특정 정책 폴더를 선택하십시오(DiffServ, IntServ, 서버 요구 —> URI 또는 연결 비율).
   2. 모니터하려는 정책을 마우스 오른쪽 버튼으로 클릭하고 **모니터**를 선택하십시오.

   다음 그림은 결과를 설명하는 주석이 있는 모니터 출력 대화상자입니다.

   그림 6. 서비스 품질 모니터



수락된 요구 수, 드롭(drop)된 요구 수, 총 요구 수 및 연결 비율 등 측정된 필드를 검사하십시오. 드롭된 요구 수는 통신량이 구성된 정책 값을 초과할 때 표시됩니다. 수락된 요구 수는 이 정책에 의해 제어되는 비트 수를 나타냅니다(패킷이 시작된 시간부터 현재 모니터 출력 시간까지).

평균 연결 요구 비율 필드에 지정한 값 역시 중요합니다. 패킷 수가 이 한계를 초과할 때부터 서버가 드롭을 시작합니다. 그 결과 삭제된 요구 수가 증가합니다. 이것은 사용자가 구성한대로 정책이 작동하는 것을 보여줍니다. 모든 모니터 필드에 대한 설명은 모니터 절을 참조하십시오.

4. 수정할 값이 있는 경우 등록 정보 패널에서 변경하십시오.

모니터를 닫으십시오. Restrict_TheirCompany 정책을 **마우스 오른쪽 버튼으로 클릭하고 등록 정보**를 선택하십시오. 이 패널을 사용하여 정책 등록 정보를 편집할 수 있습니다. 여기에서 스케줄, 클라이언트, 어플리케이션 및 통신 관리도 편집할 수 있습니다.

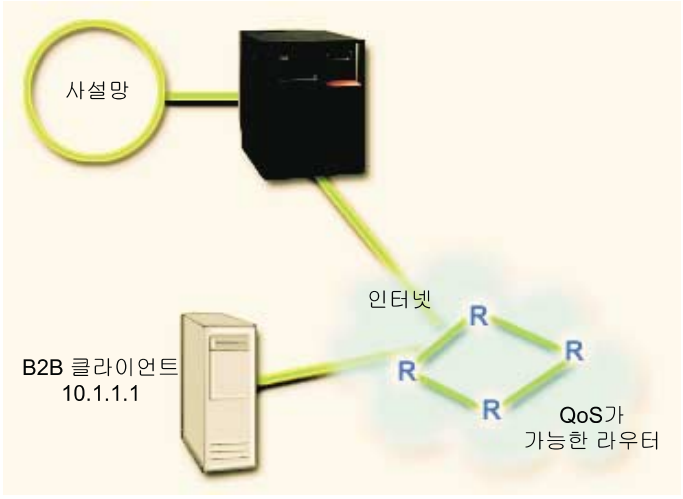
QoS 시나리오: 예측 가능 B2B 트래픽

문제점

판매 부서가 자신들이 예상한대로 네트워크 통신이 이루어지지 않는 문제점을 보고합니다. 귀사의 iSeries 서버는 예측 가능한 e-business 서비스를 필요로 하는 B2B 환경에 놓여 있습니다. 그리고 귀사는 고객들에게 예측 가능한 트랜잭션을 제공해야 합니다. 또한 하루 중 가장 바쁜 시간(오전 10시부터 오후 4시)동안 판매 팀에서 어플리케이션을 주문하는 처리에 최상의 서비스를 제공해야 합니다.

아래 일러스트레이션에서 사설망 내에 판매 팀이 존재합니다. B2B 클라이언트에 대한 통신 경로를 따라 RSVP 작동 가능 라우터가 있습니다. 각각의 R은 통신 경로를 따라 설치되어 있는 라우터를 나타냅니다.

그림 7. RSVP 작동 가능 라우터를 사용하는 B2B 클라이언트에 대한 통합 서비스 정책



솔루션

제어를 받는 로드 서비스는 혼잡한 네트워크에 매우 민감한 어플리케이션을 지원하지만 작은 양의 유실 및 지연은 허용합니다. 어플리케이션이 제어를 받는 로드 서비스를 사용하는 경우 네트워크 로드가 증가하는 것만큼 성능에 영향을 미치지는 않습니다. 가벼운 조건의 네트워크에서 처리되는 보통의 통신량과 비슷한 서비스가 제공됩니다. 특정 어플리케이션에서 발생하는 일정 수준의 지연을 무시할 수 있다면, 제어를 받는 로드 서비스를 사용하여 통합 서비스 정책을 사용하도록 하십시오.

통합 서비스 정책에는 RSVP 작동 가능 어플리케이션이 필요합니다. 서버에는 RSVP 작동 가능 어플리케이션이 없으므로 직접 RSVP 작동 가능 어플리케이션을 작성해야 합니다. 직접 어플리케이션을 작성하려면 자원 예약 설치 프로토콜(RAPI) API 또는 qtoq QoS 소켓 API를 사용하십시오.

통합 서비스 정책의 경우 통신 경로와 함께 라우터도 RSVP 작동 가능 상태가 되어야 합니다. 자세한 정보는 통합 서비스 개념 섹션을 참조하십시오.

구성

1. iSeries Navigator에서 QoS를 여십시오.
    1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
    2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭한 후 **구성**을 선택하십시오.
    3. **아웃바운드 대역폭 정책**을 확장하십시오.
    4. **IntServ**를 마우스 오른쪽 버튼으로 클릭하고 **신규 정책**을 선택하십시오. 새로운 IntServ 정책 마법사가 표시됩니다.
2. 새로운 통합 서비스 정책을 작성하십시오.

    고객들에게 예측 가능한 통신량을 제공할 것이므로, 정책을 **B2B_CL**로 명명할 수 있습니다. 단일 클라이언트가 IP 주소 **10.1.1.1**에서 트랜잭션을 수신합니다. 이것은 하나의 예로 사용된 번호입니다. 통신이

7000 - 8000 사이의 여러 포트에서 실행되면, 어플리케이션을 포트 **7000-8000**으로 명명하십시오. 이 트랜잭션이 10:00-4:00에 발생하면 **Primetime**으로 스케줄 이름을 지정할 수 있습니다. 마법사에서 다음 설정을 사용하십시오.

이름 = B2B_CL
클라이언트 =10.1.1.1
어플리케이션 = 포트 7000-8000
프로토콜 = TCP
스케줄 = Primetime
토큰 버켓 크기**(b)** = 8킬로비트
토큰 비율 한계 = 초당 25메가비트
토큰 버켓 크기**(r)** = 75킬로비트
흐름 수 = 5

iSeries Navigator는 사용자 서버에서 작성된 통합 서비스 정책을 모두 나열합니다.

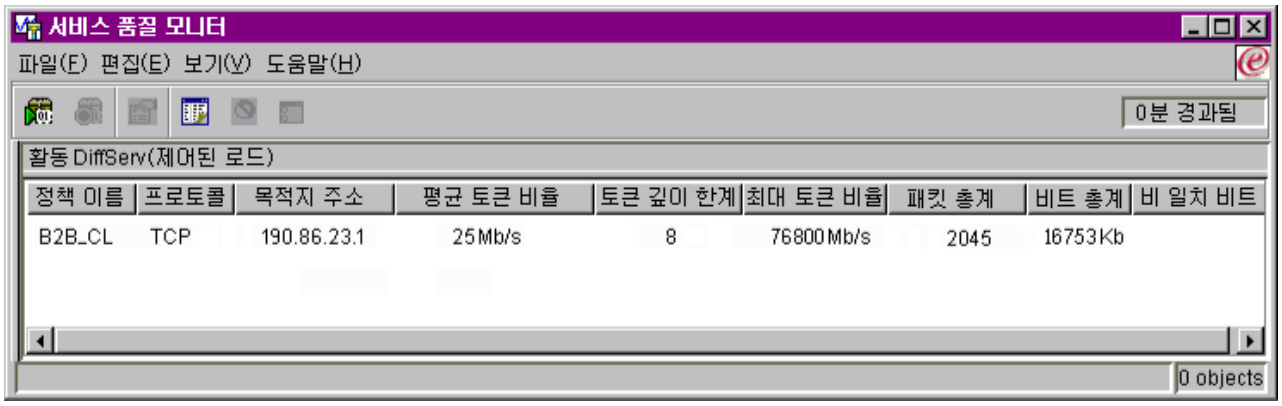
3. 유효한 정책을 확인하려면 모니터를 사용하십시오.

정책이 올바로 작동하는지 확인하려면 모니터를 사용하십시오.

1. 특정 정책 폴더를 선택하십시오(DiffServ, IntServ, 서버 요구 —> URI 또는 연결 비율).
2. 모니터하려는 정책을 마우스 오른쪽 버튼으로 클릭하고 **모니터**를 선택하십시오.

다음은 결과를 설명하는 주석이 있는 모니터 출력 대화상자입니다.

그림 8. 서비스 품질 모니터



가장 의미있는 필드는 통신으로부터 자료를 얻는 필드입니다. 반드시 총 비트 수, 적합한 비트 수 및 적합한 패킷 수 필드를 검사하십시오. 부적합 비트 수는 이 통합 서비스 정책 요구사항을 충족시키기 위해 다른 통신이 지연되거나 드롭(drop)되는 경우 표시됩니다. 모니터 필드에 대한 자세한 설명은 모니터 절을 참조하십시오.

4. 이 정책 내에서 조정이 필요한 값을 모두 수정하십시오.

정책을 작성한 후에는 마법사에서 이전에 작성된 값을 수정할 수 있습니다.

1. 모니터를 닫으십시오.
2. 위에서 작성한 정책 이름을 마우스 오른쪽 버튼으로 클릭하십시오.
3. **등록 정보**를 선택하면 B2B_CL 등록 정보 대화 상자가 표시됩니다.
4. 통신 흐름을 제어하는 값을 변경하려면, **흐름 제어** 탭을 선택하십시오.

여기에서 스케줄, 클라이언트, 어플리케이션 및 통신 관리를 편집할 수 있습니다.

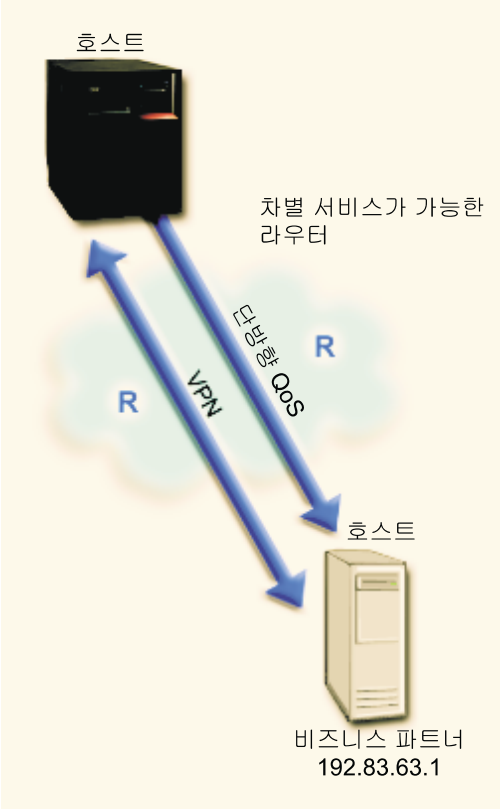
QoS 시나리오: 보안 및 예측 가능한 결과(VPN 및 QoS)

문제점

귀사의 협력업체가 VPN으로 연결되어 있고, 중요한 자료의 보안 및 예측 가능한 e-business 흐름을 위해 VPN 및 QoS를 결합하려고 합니다. QoS 구성은 한 방향으로만 진행됩니다. 따라서 오디오/비디오 어플리케이션이 있을 경우, 연결 양쪽의 어플리케이션에 QoS를 설정해야 합니다.

다음은 호스트 간 VPN 연결에서 서버와 클라이언트를 보여주는 일러스트레이션입니다. 각각의 R은 통신 경로를 따라 설치된 차별화된 서비스 작동 가능 라우터를 나타냅니다. QoS 정책은 한 방향으로만 흐릅니다.

그림 9. QoS 차별화된 서비스 정책을 사용하여 호스트 간 VPN 연결



솔루션

보호 뿐만 아니라 연결의 우선순위를 설정하기 위해 VPN와 QoS를 사용할 수 있습니다. 첫 번째로 호스트 간에 VPN 연결을 설정할 수 있습니다. VPN 구성에 대해서는 호스트 간 VPN 연결 예를 참조하십시오. VPN 연결 보호가 이루어지면, QoS 정책을 설정할 수 있습니다. 그리고 차별화된 서비스 정책을 작성할 수 있습니다. 이 정책에는 높은 긴급 이송 코드점 값을 지정하여 중요한 통신에 있어서 네트워크가 처리하는 우선순위 지정 방법에 영향을 줄 수 있습니다.

구성

1. 호스트 간 VPN 연결을 설정하십시오. VPN 구성에 대해서는 호스트 간 VPN 연결 예를 참조하십시오.
2. iSeries Navigator에서 QoS를 여십시오.
    1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
    2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭한 후 **구성**을 선택하십시오.
    3. **아웃바운드 대역폭 정책**을 확장하십시오.
    4. **DiffServ**를 마우스 오른쪽 버튼으로 클릭하고 **신규 정책**을 선택하십시오. 새로운 DiffServ 정책 마법사가 표시됩니다.
3. 차별화된 서비스 정책을 작성하십시오.

B2B 어플리케이션에 대해 성능을 향상시킬 것이므로, 정책 **B2B**를 호출할 수 있습니다. 클라이언트는 단일 주소 **192.83.63.1**을 가지고 있습니다. 이것은 하나의 예로 사용된 번호입니다. B2B 통신은 어느 포트나 사용할 수 있으므로, **모든 포트**로 어플리케이션을 명명할 수 있습니다. 오전 9:00 - 오후 5:00 사이에만 혼잡이 발생하므로, 9-5 스케줄을 정책에 적용할 수 있습니다. 이름을 **Firstshift**로 지정할 수 있습니다. 마법사에서 다음 설정을 사용하십시오.

이름 = B2B
클라이언트 = VPNClient
어플리케이션 = 모든 포트
프로토콜 = 모두
스케줄 = Firstshift

계속 진행하면서 자동으로 표시될 서비스 클래스 마법사로부터 나머지 정책 정보를 입력하십시오.

토큰 버켓 크기 = 8킬로비트
평균 비율 한계 = 초당 90메가비트
최고 비율 한계 = 제한 없음
프로파일 외부 통신량 넘침 처리 = 패킷 드롭(다시 전송됨)

iSeries Navigator는 사용자 서버에서 작성된 차별화된 서비스 정책을 모두 나열합니다.

4. 새로운 서비스 클래스를 완료하십시오.

마법사를 완료하는 동안 서비스 클래스를 지정할 것을 요청받습니다. 서비스 클래스가 성능 한계, 코드점, 프로파일 외부 처리 특성을 지정합니다. 이 정책에 높은 우선순위와 긴급 이송 코드점을 지정할 것입니다. 긴급 이송 코드점을 적용할 것이므로, 이 값을 선택한 이유를 기억하기 위해 서비스 클래스를 **EF_VPN**으로 명명할 수 있습니다.

서비스 클래스 = EF_VPN

6. 모니터를 사용하여 정책이 작동 중인지 확인하십시오.

정책이 사용자가 구성한대로 작동하는지 확인하려면, 모니터를 사용하십시오.

1. 특정 정책 폴더를 선택하십시오(DiffServ, IntServ, 서버 요구 —> URI 또는 연결 비율).
2. 모니터하려는 정책을 마우스 오른쪽 버튼으로 클릭하고 **모니터**를 선택하십시오.

다음 그림은 결과를 설명하는 주석이 있는 모니터 출력 대화상자입니다.

그림 10. 서비스 품질 모니터

예 1과 마찬가지로, 가장 관심을 끄는 필드는 통신에서 자료를 얻는 필드입니다. 이러한 필드에는 총 비트 수, 적합한 비트 수 및 적합한 패킷 수 등이 있습니다. 부적합 비트 수는 통신량이 구성된 정책 값을 초과할 때 표시됩니다. 적합한 패킷 수는 이 정책에 의해 제어되는 패킷 수를 나타냅니다. 평균 사용 비율 한계 필드에 지정한 값도 중요합니다. 패킷 수가 이 한계를 초과할 때부터 서버가 드롭을 시작합니다. 그 결과 부적합 비트 수가 증가합니다. 이 정책과 예 1의 차이점은 VPN 프로토콜을 사용하여 패킷이 보호된다는 점입니다. 이미 설명한 바와 같이 QoS는 VPN 연결에 대해 작업을 합니다. 모든 모니터 필드에 대한 설명은 모니터 절을 참조하십시오.

5. 이 정책 내에서 조정이 필요한 값을 모두 수정하십시오.

   또한 서비스 클래스를 작성한 후에는 편집할 수 있습니다.

   1. 모니터를 닫으십시오.
   2. 왼쪽 분할 창에서 **서비스 클래스**를 선택하십시오.
   3. 오른쪽 분할 창에서 위에서 작성한 서비스 클래스 이름을 마우스 오른쪽 버튼으로 클릭하십시오.
   4. **등록 정보**를 선택하십시오. CoS 등록 정보 대화상자에 통신을 제어하는 값이 표시됩니다. 적절한 값을 수정하십시오.

«

QoS 개념

»

서비스 품질(QoS)이라는 용어에 관해서는 여러 소스에서 다루고 있으므로, 이 주제에서는 귀사의 iSeries 서버에 적용되는 기본적인 사항만을 설명합니다.

서비스 품질 구현에 있어서 가장 중요한 부분 중 하나는 서버 자체입니다. 아래의 개념을 이해해야 할 뿐만 아니라, 이 개념을 구현함에 있어서 서버의 역할에 관해서도 잘 알아야 합니다. iSeries 서버는 라우터가 아니라 클라이언트나 서버로만 사용됩니다. 아래 개념에 대한 내용을 고려하여 서비스 품질(QoS) 계획을 시작하십시오.

QoS를 구현하기 위해서는 통신량에 대한 정책을 작성해야 합니다. 정책은 조치를 지정하는 규칙 세트입니다. 기본적으로 클라이언트, 어플리케이션 및 스케줄(사용자 지정)이 특정 서비스를 수신하도록 지정합니다. 기본적으로 네 가지 정책 유형을 구현할 수 있습니다. 먼저 아웃바운드 대역폭과 인바운드 수락의 두 가지 범주로 구분됩니다. 아웃바운드 대역폭 정책에서는 통합 서비스 정책과 차별화된 서비스 정책의 두 가지 서비스 유형을 작성할 수 있습니다. 인바운드 수락 정책에서는 신규 연결 요구 비율 정책과 신규 URI 요구 비율 정책의 두 가지 서비스 유형을 작성할 수 있습니다.

인바운드란 외부 소스로부터 사용자 네트워크로 들어오는 연결 요구를 제어하는 정책을 말합니다. 아웃바운드란 네트워크를 떠나려고 하는 통신을 제한하거나 지원하는 정책을 말합니다. 사용해야 할 정책을 결정하기 위해 QoS를 사용하는 이유를 조사하십시오. 각 정책 유형에 적합한 상황이 어떤 것인지 아래 개념을 검토하십시오.

자세한 정보는 다음 링크를 사용하십시오.

차별화된 서비스
이것은 서버에서 작성할 수 있는 첫 번째 유형의 아웃바운드 대역폭입니다. 차별화된 서비스는 통신량을 클래스로 분류한 QoS 부분입니다. 네트워크에 서비스 품질(QoS)을 구현하려면, 네트워크 통신량을 분류하기 위한 방법과 서로 다른 클래스를 처리하기 위한 방법을 판별해야 합니다. 그리고나서 차별화된 서비스 정책을 사용하여 서비스 클래스를 작성할 수 있습니다.

차별화된 서비스 클래스
다음에 나오는 하위 주제에서 서비스 클래스를 구성하는 부분들을 설명합니다. 차별화된 서비스 정책을 작성할 경우 서비스 클래스도 작성해야 합니다.

통합 서비스
사용자가 작성할 수 있는 아웃바운드 대역폭 정책의 두 번째 유형은 통합 서비스 정책입니다. 통합 서비스는 IP 어플리케이션이 RSVP 프로토콜을 사용하여 대역폭을 요구하고 예약할 수 있는 기능을 제공합니다. 통합 서비스 정책은 완전한 연결을 보장하기 위해 RSVP 프로토콜을 사용합니다. 이것이 지정할 수 있는 가장 높은 레벨의 서비스이고 또한 가장 복잡한 서비스입니다. 통합 서비스 정책을 작성할 때 보장 서비스 또는 제어를 받는 로드 서비스의 두 가지 서비스 클래스 중 하나를 지정할 수 있습니다.

차별화된 서비스 표시를 사용한 통합 서비스
일반적으로 이 정책 유형은 통합 서비스 정책이 혼합 네트워크 환경에 있을 때 사용됩니다. 혼합 네트워크 환경에는 RSVP 작동 가능 네트워크 노드와 RSVP 작동 불가능 네트워크 노드가 있습니다.

RSVP 및 QoS API
여기에서는 통합 서비스 예약에 사용되는 프로토콜 및 API를 설명합니다. 또한 라우터 RSVP를 작동 가능하게 만드는 것에 대해서도 설명합니다.

연결 비율
이 유형의 인바운드 정책은 사용자 네트워크에 대해 (IP 주소에 의한) 수락을 요구하는 통신을 제어하는 데 사용됩니다. 인바운드 수락 정책에는 연결 비율 및 URI의 두 가지 유형이 있습니다. 여기에서는 두 가지 유형의 인바운드 정책 모두에 대해 설명합니다.

URI
이 유형의 인바운드 정책은 사용자 네트워크에 대해 (URI에 의한) 수락을 요구하는 통신을 제어하는 데 사용됩니다. 인바운드 수락 정책에는 연결 비율 및 URI의 두 가지 유형이 있습니다. 여기에서는 두 가지 유형의 인바운드 정책 모두에 대해 설명합니다.

디렉토리 서버
QoS 정책을 디렉토리로 서버로 내보낼 수 있습니다. 여기에서는 디렉토리 서버를 사용할 때의 장점, LDAP 개념 및 구성 및 QoS 스키마에 대해 알아 보십시오.

QoS 구현을 시도하기 전에, 서비스 품질(QoS)을 자세히 조사하여 서비스가 사용자의 요구사항을 만족하는지 확인하십시오. 추가 자원 탐색에 대한 도움말은 QoS 관련 정보 페이지를 참조하십시오.

연결 요구 비율 및 URI 요구 비율

인바운드 정책은 사용자 서버에 연결하려는 통신을 제어하는 데 사용됩니다. 사용자가 인바운드 제어를 정의하고 구성할 수 있도록 하는 두 가지 유형의 정책 즉, URI 정책 및 연결 비율 정책이 있습니다. 두 가지 정책 유형은 아래에서 설명됩니다.

URI 요구 비율 정책

URI 연결 비율 정책은 서버를 과부하로부터 보호하는 데 도움이 되는 솔루션의 일부입니다. 이러한 유형의 정책은 서버에 의해 수락되는 URI 요구를 제한하기 위해 어플리케이션 레벨 정보에 기초하여 수락 제어를 적용합니다. 이는 URI를 사용하여 우선순위를 설정하므로 *헤더에 기초한 연결 요구 제어*라고도 합니다.

연결 비율 정책과 달리 URI 정책은 패킷 헤더만 검사하는 것이 아니라 내용을 검사하므로 더 많은 제어를 갖습니다. 검사하는 내용에는 URI 이름이나 기타 어플리케이션 특정 정보가 포함될 수 있습니다. iSeries의 경우 상대 URI 이름을 사용하여 정책을 정의합니다. 예를 들면 **/products/clothing**과 같습니다. 다음은 상대 URI를 설명하는 예입니다.

상대 URI

상대 URI는 실제로 절대 URI(이전의 절대 URL과 유사함)의 서브세트입니다. http://www.ibm.com/software를 예로 들어 생각해 보십시오. The **http://www.ibm.com/software** 세그먼트는 절대 URI로 간주됩니다. **/software** 세그먼트는 상대 URI입니다. 모든 상대 URI 값은 하나의 슬래시(**/**)로 시작되어야 합니다. 다음은 올바른 상대 URI의 예입니다.

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

주: 디폴트 프로토콜, 호스트 이름 및 포트는 모두 HTTP 서버로부터 상속됩니다. 또한 URI를 지정할 때 내재적 와일드카드가 있습니다. 예를 들면 **/software**에는 소프트웨어 디렉토리에 있는 모든 것이 포함됩니다.

URI 정책은 네트워크로 들어오는 통신 요구를 제어하므로 인바운드 정책으로 간주됩니다. 이 인바운드 제어의 일부로 URI 요구가 정책에 의해 수락된 후 처리되는 우선순위를 지정할 수 있습니다. 우선순위 정책에 의해 각 연결에 대해 구성된 우선순위에 기초하여 실제로 대기행렬의 연결 요구에 대해 우선순위를 설정합니다.

연결 비율 정책

연결 비율 정책은 서버를 과부하로부터 보호하는 데 도움이 되는 솔루션의 일부입니다. 이러한 유형의 정책은 서버에 의해 수락되는 연결을 제한하기 위해 연결 레벨 정보에 기초하여 수락 제어를 적용합니다. 이는 *TCP SYN 방침 적용(policing)*이라고도 합니다.

연결 비율 방침 적용(policing)은 사용자가 작성한 정책에 정의된 초당 설정된 평균 연결 수 및 설정된 최대 연결 수(임의의 시점에서)를 기초로 새로 수신되는 연결을 수락하거나 거부합니다. 이 연결 한계는 평균 비율 및 버스트 한계로 구성되며 이는 iSeries Navigator에서 사용자에게 입력을 프롬트합니다. 수신 연결 요구가 서버에 도달하면 서버는 패킷 헤더 정보를 분석하여 이것이 정책에 정의된 통신인지 여부를 판별합니다. 시스템은 연결 한계 프로파일에서 이 정보를 확인합니다. 정책이 정책 한계 내에 있다면 대기행렬로 들어갑니다. 정책과 일치하지 않는 패킷은 삭제됩니다.

URI 정책과 유사하게 연결 비율 정책도 사용자 네트워크로 들어오는 통신의 연결 비율을 제어하므로 인바운드 정책으로 간주됩니다. 이 인바운드 제어의 일부로 연결이 정책에 의해 수락된 후 연결이 처리될 우선순위를 지정할 수 있습니다. 정책 우선순위를 설정함으로써 실제로 각 연결에 대하여 구성된 우선순위에 기초하여 실제로 대기행렬의 연결 요구에 대해 우선순위를 설정합니다.

URI 정책 및 연결 비율 정책에서는 각 정책에 정의된 통신에 대하여 연결 비율 및 버스트 한계를 설정해야 합니다. 이 비율 한계는 서버로 들어오려는 인바운드 연결을 제한하는 데 도움이 됩니다. 평균 연결 비율에서는 서버로 들어오는 것이 허용된 새롭게 설정된 연결 한계 또는 수락된 URI 요구 비율을 지정합니다.

평균 연결 비율 및 버스트 한계

연결 비율 및 버스트 한계는 함께 비율 한계라고도 합니다. 이 비율 한계는 서버로 들어오려는 인바운드 연결을 제한하는 데 도움이 됩니다. 비율 한계는 인바운드 수락 정책인 URI 및 연결 비율 내에서 설정됩니다.

연결 버스트 한계
버스트 한계 크기는 연결 버스트를 수용하는 버퍼 용량을 결정합니다. 연결 버스트는 처리할 수 있는 것보다 더 빠른 비율로 서버에 들어갈 수 있고 사용자가 이를 허용하고자 할 수도 있습니다. 버스트의 연결 수가 설정한 연결 버스트 비율을 초과하는 경우 추가된 연결은 삭제됩니다.

평균 연결 비율
평균 연결 비율에서는 서버로 들어오는 것이 허용된 새롭게 설정된 연결 한계 또는 수락된 URI 요구 비율을 지정합니다. 어떤 요구로 인해 사용자가 설정한 한계를 서버가 초과하는 경우 서버는 그 요구를 거부합니다. 평균 연결 요구 한계는 초당 연결 수로 측정됩니다.

힌트: 어떤 한계를 설정할 것인지 결정하기 위해 모니터를 실행하고자 할 수 있습니다. 서버 전체에서 대부분의 자료를 수집하는 데 도움이 되는 샘플 정책에 대해서는 현재 네트워크 통계 모니터를 참조하십시오. 이 결과를 사용하여 한계를 적절하게 조정할 수 있습니다.

차별화된 서비스

차별화된 서비스는 통신량을 클래스로 나눕니다. 네트워크에 서비스 품질(QoS)을 구현하려면, 네트워크 통신량을 분류하기 위한 방법과 서로 다른 클래스를 처리하기 위한 방법을 판별해야 합니다.

서버는 IP 패킷의 서비스 레벨을 식별하기 위해 IP 헤더에 있는 비트를 사용합니다. 라우터와 스위치는 IP 헤더 TOS 필드에 홉별 작동(PHB) 정보를 기초로 자원을 할당합니다. TOS 필드는 RFC(request for comment) 1349 및 OS/400(R) V5R1에서 다시 정의되었습니다. PHB는 네트워크 노드에서 패킷이 수신하는 이송 방식입니다. PHB는 코드점으로 알려진 16진 값으로 표시됩니다. 패킷을 서버로 표시하거나 라우터와 같은 네트워크의 기타 부분으로 표시할 수 있습니다. 패킷이 요구된 서비스를 보유하기 위해서는 모든 네트워크 노드에서

차별화된 서비스가 가능해야 합니다. 즉, 장비가 홉별 작동을 실현시킬 수 있어야 합니다. PHB를 시행하기 위해서는 네트워크 노드가 대기행렬 스케줄 및 아웃바운드 우선순위 관리를 사용할 수 있어야 합니다. 차별화된 서비스 작동 가능화에 대한 자세한 정보는 통신량 조절기 페이지를 참조하십시오.

패킷이 차별화된 서비스가 작동되지 않는 라우터나 스위치를 통과하면, 서비스 레벨을 유실합니다. 계속해서 패킷을 처리하되 예기치 않은 전달 결과가 발생할 수 있습니다. iSeries 서버에서 표준 PHB 코드점을 사용하거나 사용자 소유의 클래스를 정의할 수 있습니다. 사설망 밖에서 사용하기 위해 사용자 자신의 코드점을 작성하는 것은 권장되지 않습니다.

통합 서비스와는 달리, 차별화된 서비스 통신에는 예약이나 흐름별 처리가 필요없습니다. 같은 클래스의 모든 통신을 동등하게 취급합니다.

또한 서버 안이나 밖으로 이루어지는 통신을 제어하기 위해 차별화된 서비스를 사용할 수 있습니다. 이것은 iSeries 서버가 성능을 제한하기 위해 차별화된 서비스를 사용하는 것을 의미합니다. 별로 중요하지 않은 어플리케이션의에 한계를 지정하면 중요한 어플리케이션이 먼저 사설망으로 나갈 수 있습니다. 정책을 작성할 때, 시스템이 사용자의 서버에 다양한 한계를 설정할 것을 요청합니다. 성능 한계에는 버켓 크기, 최고 비율 한계, 평균 비율 한계가 포함됩니다. iSeries Navigator의 QoS 기능 도움말 주제를 통해 이러한 한계에 대한 자세한 정보를 알 수 있습니다.

지금까지는 통신량을 그룹화하기 위해 차별화된 서비스를 사용하는 방법에 대해 알아보았습니다. 어떤 코드점을 할당해야 할지 확실히 알지 못하면, 코드점 및 홉별 작동을 검토하십시오. 사용할 코드점이 어느 것인지 아직 확실히 알지 못하더라도 여러 번 시도하다보면 잘 알게 될 것입니다. 테스트 정책을 작성한 후 이 정책들을 모니터하여 알맞게 조정하십시오.

차별화된 서비스 클래스

차별화된 서비스 섹션에서는 차별화된 서비스 기능을 클래스로 그룹화하는 방법에 대해 논의합니다. 대부분이 장비를 통해 이루어지지만 사용자가 통신량의 그룹화 방법과 통신량에서의 우선순위를 제어합니다.

QoS를 구현할 때, 첫 번째로 정책을 정의합니다. 정책은 언제, 어디서, 누가, 무엇을 하는지 결정하는 것입니다. 그리고나서 정책에 서비스 클래스를 할당해야 합니다. 서비스 클래스는 별도로 정의되며, 정책에서 다시 사용될 수 있습니다. 서비스 클래스는 홉별 작동, 통신량 한계, 프로파일 외부 처리로 구성됩니다.

홉별 작동

서비스 품질은 통신에 홉별 작동을 지정하기 위해 권장 코드점을 사용합니다. 라우터와 스위치는 이 코드점을 사용하여 통신 우선순위 레벨를 제공합니다. 서버는 라우터의 역할을 하지 않기 때문에 코드점을 사용할 수 없습니다. 사용자별 네트워크 환경을 기초로 어떤 코드점을 사용해야 할 것인지 판별해야 합니다. 가장 중요한 어플리케이션과 높은 우선순위를 지정해야 할 정책을 고려해 보십시오. 가장 중요한 것은 사용자가 지정한 사항에 일관성을 유지시킴으로써 예상한 결과를 얻을 수 있도록 하는 것입니다. 이 코드점이 통신에 있어서 클래스 간을 차별화하는 핵심 부분입니다.

성능 한계

서비스 품질은 네트워크에서 통신량을 제한하기 위해 성능 한계를 사용합니다. 이러한 한계는 토큰 버켓 크기, 최고 사용 한계 및 평균 사용 한계를 설정합니다. 이들 특정 값에 대한 자세한 내용은 토큰 버켓 및 대역폭 한계를 참조하십시오.

프로파일 외부 처리

서비스 클래스의 마지막 부분은 프로파일 외부 처리입니다. 위의 성능 한계를 지정할 때 사용자가 통신량을 제한하기 위한 값을 설정합니다. 통신량이 한계를 초과하면, 패킷은 프로파일 외부에 있는 것으로 간주됩니다. 서비스 클래스에 있는 이 정보가 프로파일 외부 패킷의 드롭, 셰이프 또는 재전송 여부를 서버에게 알립니다. 프로파일 외부 패킷을 드롭하기로 결정하면, 지정된 시간 이후에 재전송됩니다. 프로파일 외부 패킷을 지연시키면, 정의된 처리 특성에 맞게 정리가 이루어집니다(shape). 프로파일 외부 패킷을 차별화된 서비스 코드점(DSCP)으로 다시 표시하면, 새로운 코드점이 재지정됩니다. 마법사에서 이와 같은 처리 지침을 지시할 경우, 도움말을 클릭하여 자세한 정보를 참조하십시오.

코드점 및 홉별 작동

서비스 품질(QoS)은 통신에 홉별 작동을 지정하기 위해 다음과 같은 권장 코드점을 사용합니다. 사용자별 네트워크 환경을 기초로 어떤 코드점을 사용해야 할 것인지 판별해야 합니다. 사용자만이 자신의 환경에 맞는 코드점 구조를 결정할 수 있습니다. 사용자에게 가장 중요한 어플리케이션이 어느 것이고 더 높은 우선순위를 지정해야 하는 정책이 어느 것인지 고려해야 합니다. 가장 중요한 것은 사용자가 지정한 사항에 일관성을 유지시킴으로써 예상한 결과를 얻을 수 있도록 하는 것입니다.

다음 표에 권장 코드점이 나옵니다. 권장 코드점 대신 자신만의 홉별 작동을 작성할 수도 있습니다.

긴급 이송(25 페이지 참조)	클래스 선택기(26 페이지 참조)	확실한 이송(26 페이지 참조)
101110	클래스 0 - 000000	확실한 이송, 클래스 1, 저 - 001010
	클래스 1 - 001000	확실한 이송, 클래스 1, 중 - 001100
	클래스 2 - 010000	확실한 이송, 클래스 1, 고 - 001110
	클래스 3 - 011000	확실한 이송, 클래스 2, 저 - 010010
	클래스 4 - 100000	확실한 이송, 클래스 2, 중 - 010100
	클래스 5 - 101000	확실한 이송, 클래스 2, 고 - 010110
	클래스 6 - 110000	확실한 이송, 클래스 3, 저 - 011010
	클래스 7 - 111000	확실한 이송, 클래스 3, 중 - 011100
		확실한 이송, 클래스 3, 고 - 011110
		확실한 이송, 클래스 4, 저 - 100010
		확실한 이송, 클래스 4, 중 - 100100
		확실한 이송, 클래스 4, 고 - 100110

긴급 이송

긴급 이송은 차별화된 서비스인 홉별 작동의 한 유형입니다. 이것은 주로 네트워크에서 보장된 서비스를 제공

하는 데 사용됩니다. 긴급 이송은 네트워크 간의 대역폭을 보장함으로써 낮은 유실률, 낮은 지터율, 지점 간 서비스를 제공합니다. 예약은 패킷을 송신하기 전에 이루어집니다. 기본 목적은 지연을 막고 적시에 패킷을 전달하는 것입니다.

주: 일반적으로 긴급 이송은 많은 비용을 요하는 처리이므로, 정기적으로 홉별 작동을 사용하는 것은 권장되지 않습니다.

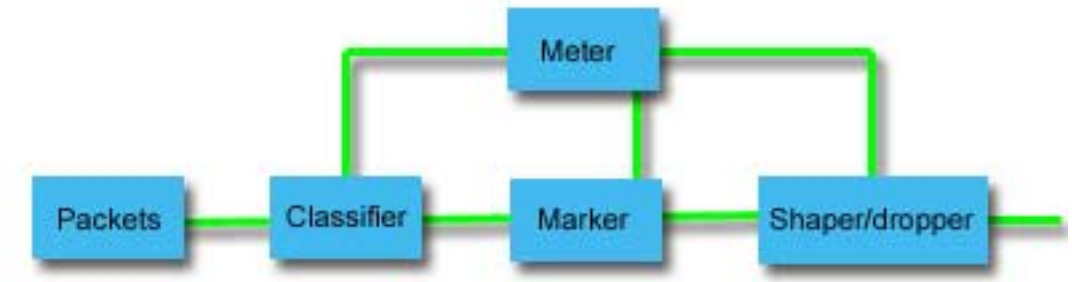
클래스 선택기
클래스 선택기 코드점은 차별화된 서비스 작동의 또다른 유형입니다. 7 가지의 클래스가 있으며, 클래스 0은 우선순위가 가장 낮은 패킷을 제공하고 클래스 7은 클래스 선택기 코드점 값에서 최상의 우선순위를 가진 패킷을 제공합니다. 대부분의 라우터가 이미 유사한 코드점을 사용하기 때문에 이것이 가장 일반적인 홉별 작동입니다.

확실한 이송
확실한 이송은 4개의 홉별 작동 클래스로 나뉩니다. 각각 저, 중, 고 레벨의 드롭 우선권이 있습니다. 드롭 우선권 레벨이 패킷의 드롭 방법을 판별합니다. 각각의 클래스에는 각각의 대역폭 스펙이 있습니다. 클래스 1, 고 레벨은 정책에 가장 낮은 우선순위를 제공합니다. 클래스 4, 저 레벨은 가장 높은 우선순위를 제공합니다. 저 레벨은 정책에 있는 그 패킷이 특정 클래스 레벨에서 드롭될 가능성이 가장 낮은 것을 의미합니다.

통신량 조절기
서비스 품질 정책을 사용하는 네트워크는 QoS를 위한 준비가 잘 되어 있어야 합니다. 이것은 라우터, 스위치와 같은 네트워크 장비에 분류자, 미터(meter), 마커, 셰이퍼(shaper) 및 드롭퍼와 같은 기능이 있어야 한다는 것을 의미합니다. 이러한 용어를 모두 묶어서 *통신량 조절기*라고 합니다. 네트워크 장비에 모든 통신 조절기가 있으면, QoS를 위해 잘 준비된 것입니다.

다음 그림에서는 통신량 조절기가 작동하는 방식을 논리적으로 보여줍니다.

그림 11. 통신량 조절기



다음은 각 통신량 조절기에 관한 자세한 설명입니다.

분류자
패킷 분류자는 IP 헤더의 내용을 기초로 한 통신 스트림에서 패킷을 선택합니다. iSeries 서버는 두 가지의 분류자 유형을 정의합니다. BA(Behavior aggregate)는 차별화된 서비스 코드점을 기초로 패킷을 분류합니다. MF(Multi-field)는 소스 주소, 목적지 주소, 차별화된 서비스 필드, 프로토콜 ID, 소스 포트 및 목적지 포트 번호와 같은 하나 이상의 헤더 필드를 조합한 값을 기초로 패킷을 선택합니다.

미터(meter)
통신량 미터(meter)는 분류자별로 이송 중인 IP 패킷이 통신량 IP 헤더 프로파일에 해당하는 것인지를 측정합니다. IP 헤더의 정보는 이 통신을 위해 사용자가 QoS 정책에 설정한 값으로 결정됩니다. 미터는 하나의 조치를 트리거하기 위해 기타 조건 함수에 정보를 전달합니다. 조치가 프로파일 안에 있는 것인지 아니면 밖에 있는 것인지에 관계없이 각 패킷에 대해 그 조치가 트리거됩니다.

마커
패킷 마커는 차별화된 서비스(DS) 필드를 설정합니다. 그리고 차별화된 서비스 코드점을 찾아서 바이트 안으로 전송합니다. 모든 패킷을 하나의 코드점으로 표시하거나 홉별 작동을 선택하기 위해 사용되는 코드점 세트로 표시하도록 마커를 구성할 수 있습니다.

셰이퍼(shaper)
셰이퍼(shaper)는 통신 스트림의 일부 패킷이나 전체를 지연시켜 통신 프로파일에 맞는 스트림을 발생시킵니다. 셰이퍼의 버퍼 크기는 한정된 것으로서 지연된 패킷을 보유할 수 있는 공간이 충분하지 않으면 패킷이 삭제될 수 있습니다.

드롭퍼
드롭퍼는 통신 스트림의 일부 또는 모든 패킷을 삭제합니다. 따라서, 통신 프로파일에 맞는 스트림을 발생시킵니다.

디렉토리 서버 개념

QoS 정책 구성은 LDAP 디렉토리 서버에 저장됩니다. LDAP 서버는 최신 LDAP 프로토콜 버전 3과 함께 사용해야 합니다.

디렉토리 서버 사용 시 장점

디렉토리 서버를 사용하면 QoS 솔루션을 쉽게 관리할 수 있습니다. 서버 전체에서 QoS 정책을 구성하는 대신 구성 데이터를 하나의 로컬 디렉토리 서버에 저장하여 여러 시스템이 공유하도록 할 수 있습니다. 그러나 자료 공유는 필요하지 않습니다. 디렉토리 서버를 QoS와 함께 사용하는 데에는 두 가지 방법이 있습니다.

1. 한 시스템에 의해서만 자료를 구성, 저장 및 사용합니다.
2. 구성 자료는 다른 시스템의 자료를 가지고 있는 디렉토리 서버에도 있을 수 있지만 그 시스템과 반드시 자료를 공유하는 것은 아닙니다. 단일 위치에서 여러 시스템의 자료를 백업 및 저장할 수 있습니다.

LDAP 자원

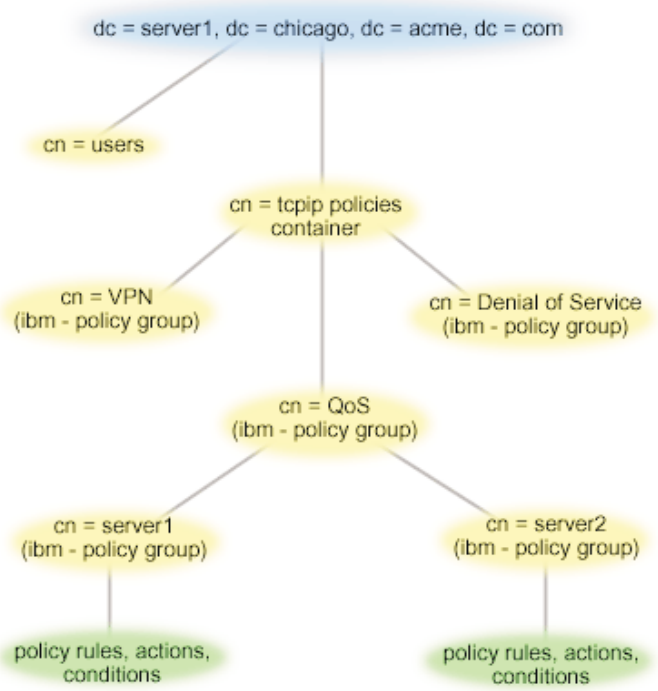
QoS를 사용하기 전에 LDAP 개념 및 디렉토리 구조에 대해 이해하고 있어야 합니다. iSeries Information Center의 디렉토리 서비스(LDAP) 주제 안에 있는 LDAP 기본 사항을 참조하십시오.

QoS 트리 구조

디렉토리의 일부를 관리하고자 할 때 **식별명(DN)** 또는 (원하는 경우) 키워드를 참조할 수 있습니다. 디렉토리

서버를 구성할 때 DN을 지정합니다. DN은 보통 항목 자체의 이름과 디렉토리의 항목 위에 있는 오브젝트(위에서 아래로)로 구성됩니다. 서버는 DN 아래의 디렉토리에 있는 모든 오브젝트에 액세스할 수 있습니다. 예를 들어 다음 디렉토리 구조에 포함된 LDAP 서버를 생각해 봅시다.

그림 12. 샘플 QoS 디렉토리 구조



맨 위의 Server1(dc=server1,dc=chicago,dc=acme,dc=com)은 디렉토리 서버가 상주하는 서버입니다. cn=QoS 또는 cn=tcpip 정책과 같은 다른 서버에도 QoS 서버가 상주합니다. 따라서 cn=server1에서 디폴트 DN은 `cn=server1,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com`으로 읽습니다. cn=server2에서 디폴트 DN은 `cn=server2,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago, dc=acme,dc=com`으로 읽습니다.

디렉토리를 관리할 때 cn이나 dc와 같은 DN에서 서버를 적절하게 변경하는 것이 중요합니다. DN을 편집할 때 주의해야 하는데, 특히 문자열이 너무 길어 화면이동 없이는 표시되지 않는 경우 주의해야 합니다. iSeries Navigator의 서비스 품질 기능에서 디렉토리 서버를 구성하는 방법에 대한 정보는 디렉토리 서버 구성을 참조하십시오.

일부 대체 가능한 LDAP 자원에 대해서는 QoS 관련 정보 페이지를 참조하십시오.

«

키워드

»

디렉토리 서버를 구성할 때 각 QoS 구성에 키워드를 연관시킬 것인지 여부를 판별해야 합니다. 키워드 필드는 선택적이며 무시할 수 있습니다. 다음 정보는 키워드 개념 및 키워드를 사용해야 하는 이유에 대한 설명입니다.

새로운 서비스 품질 구성 마법사에서 디렉토리 서버를 구성합니다. 사용자가 구성하는 서버가 1차 디렉토리 서버인지 2차 시스템인지를 지정해야 합니다. 모든 QoS 정책을 유지보수하는 서버가 1차 시스템입니다.

키워드는 1차 시스템에서 작성된 구성을 식별하는 데 사용됩니다. 1차 시스템에서 작성되지만 키워드는 실제로 2차 시스템에 대하여 사용됩니다. 키워드를 사용하여 2차 시스템은 1차 시스템이 작성한 구성을 로드 및 사용할 수 있습니다. 다음은 각 시스템에서 키워드를 사용하는 방법에 대한 설명입니다.

키워드 및 1차 시스템
키워드는 1차 시스템에서 작성되고 유지보수되는 QoS 구성과 연관됩니다. 키워드가 사용되므로 1차 시스템에서 작성된 구성을 2차 시스템에서 식별할 수 있습니다.

키워드 및 2차 시스템
2차 시스템은 키워드를 사용하여 구성을 탐색합니다. 2차 시스템은 1차 시스템에서 작성된 구성을 로드하고 사용합니다. 2차 시스템을 구성할 때 특정 키워드를 선택할 수 있습니다. 선택한 키워드에 따라 2차 시스템은 선택된 키워드와 연관된 구성을 모두 로드합니다. 따라서 2차 시스템은 여러 1차 시스템에서 작성된 복수 구성을 로드할 수 있습니다.

iSeries Navigator에서 디렉토리 서버 구성을 시작할 때 특정 지침은 QoS 타스크 도움말을 사용하십시오.

«

통합 서비스

통합 서비스는 통신 전달 시간과 특정 통신량 처리 지침을 지정하는 일을 합니다. 자료 전송을 보장하는 것은 상대적으로 비용이 많이 드는 방법이므로 통합 서비스 정책에 있어서 보수적인 자세가 중요합니다. 그러나 자원을 과도하게 공급하면 비용이 더 들 수 있습니다.

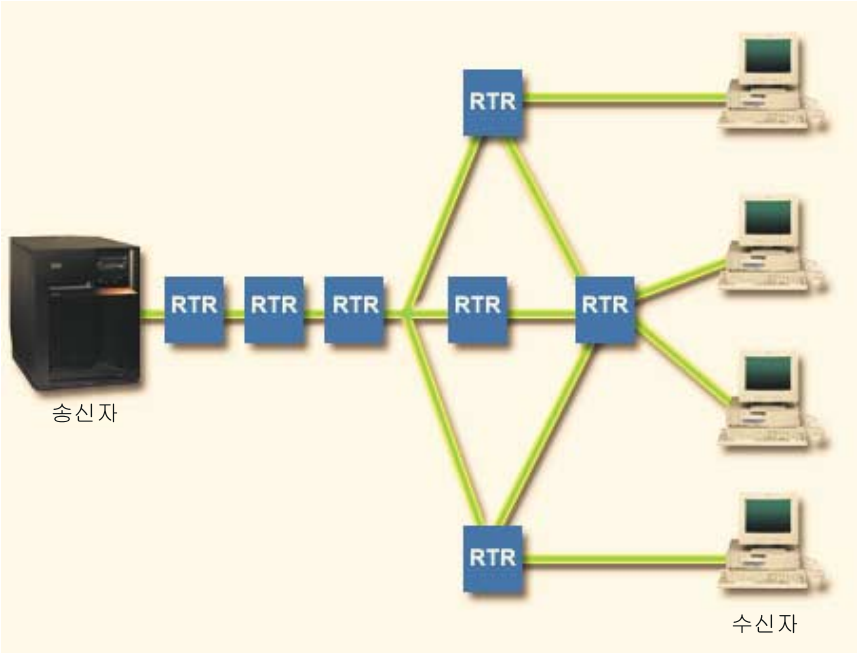
»

통합 서비스는 자료를 송신하기 전에 특정 정책에 대한 자원을 예약합니다. 자료 전송 전에 라우터에 신호가 이루어지고 실제로 네트워크의 동의를 구한 후 정책을 기초로 자료 전송을 처리합니다. **정책**은 조치를 지정하는 규칙 세트입니다. 기본적으로 관리 제어 리스트입니다. 대역폭 요구는 클라이언트로부터의 예약으로 수신됩니다. 경로에 있는 모든 라우터가 요구하는 클라이언트로부터 수신되는 요구사항에 동의하는 경우 요구는 서버 및 intserv 정책에 도달합니다. 요구가 정책에 의해 정의된 한계 내에 들어가면 QoS 서버는 RSVP 연결을 허용하고 어플리케이션에 대한 대역폭을 별도로 설정합니다. 예약은 RSVP(자원 예약 프로토콜) 및 RAPI 및/또는 qtoq QoS 소켓 API를 사용하여 수행됩니다. 자세한 내용은 RSVP 프로토콜 및 QoS API를 참조하십시오.

«

통신량이 지나는 모든 노드는 반드시 RSVP 프로토콜을 사용할 수 있어야 합니다. 라우터는 패킷 스케줄러, 패킷 분류자 및 허용 제어와 같은 통신량 제어 기능으로 서비스 품질을 제공합니다. 이러한 통신 제어를 수행하는 기능을 RSVP 작동 가능이라고 합니다. 결과적으로, 통합 서비스 정책을 구현함에 있어서 가장 중요한 부분은 네트워크의 자원을 제어하고 예측하는 것입니다. 예측 가능한 결과를 얻으려면 네트워크 내 모든 노드가 RSVP 작동 가능 상태여야 합니다. 예를 들어, 통신량은 RSVP를 인식하는 라우터를 가진 경로가 아니라, 자원을 기초로 라우트됩니다. RSVP를 인식하지 못하는 라우터를 지나는 것은 예상할 수 없는 성능 문제를 발생시킬 수 있습니다. 연결은 이루어지지만 어플리케이션이 요구하는 성능은 라우터에 의해 보장되지 않습니다. 다음 그림은 통합 서비스 기능이 논리적으로 어떻게 작동하는지를 보여줍니다.

그림 13. 클라이언트와 서버 사이의 RSVP 경로



서버의 RSVP 작동 가능 어플리케이션이 클라이언트로부터의 연결 요구를 감지합니다. 이에 대한 응답으로 서버의 어플리케이션이 클라이언트로 PATH 명령을 발행합니다. 이 명령은 RAPI API 또는 qtoq QoS 소켓 API를 사용하여 발행되며 라우터 IP 주소 정보가 들어 있습니다. PATH 명령에는 서버와 클라이언트 사이의 경로 정보와 함께 경로를 따라 서버 및 라우터에 대하여 사용 가능한 자원에 대한 정보가 들어 있습니다. 그러면 클라이언트의 RSVP 작동 가능 어플리케이션은 네트워크 경로를 따라 다시 RESV 명령을 보내 네트워크 자원이 할당된 서버에 신호합니다. 이 명령은 PATH 명령으로부터 나온 라우터 정보를 기초로 예약을 수행합니다. 서버와 모든 라우터는 경로를 따라 RSVP 연결을 위한 자원을 예약합니다. 서버가 RESV 명령을 수신하면 어플리케이션은 클라이언트로의 데이터 전송을 시작합니다. 자료는 예약한 라우터와 같은 라우트를 따라 전송됩니다. 다시 한번 강조하지만 이것은 예약을 처리하는 라우터의 능력이 정책을 성공적으로 구현하는 데 얼마나 중요한 것인지를 보여줍니다.

통합 서비스는 HTTP와 같은 RSVP 연결을 의미하지 않습니다. 물론 이것은 전적으로 사용자의 결정사항입니다. 사용자 자신만이 네트워크를 위한 최상의 조건을 결정할 수 있습니다. 성능 상의 문제가 있으며 서비스 품

질이 요구되는 영역과 어플리케이션을 고려하십시오. 통합 서비스 정책에서 사용되는 어플리케이션은 RSVP 프로토콜을 사용해야 합니다. 현재 사용자 서버에 RSVP 작동 가능 어플리케이션이 없는 경우 RSVP를 사용하도록 어플리케이션을 직접 작성해야 합니다. 자세한 내용은 RSVP 섹션을 참조하십시오.

패킷이 들어와서 네트워크를 나갈 때, 서버는 패킷을 송신하기 위한 자원이 있는지를 판별합니다. 이것은 토큰 버켓에 있는 공간의 크기로 판별됩니다. 토큰 버켓에 허용되는 비트 수, 대역폭 한계, 토큰 비율 한계 및 서버가 허용해야하는 최대 연결 수 등을 수동으로 설정합니다. 이 값을 성능 한계라고 합니다. 수신 패킷으로 인해 버켓이 한계를 초과하면 해당 패킷은 부적합 패킷으로 간주됩니다. 사용자 서버는 몇 가지 방법으로 이러한 부적합 통신을 처리할 수 있습니다. 패킷을 지연, 셰이프, 재전송 또는 드롭할 수 있습니다. 패킷이 서버 한계에 그대로 있으면, 패킷을 규칙에 따라 송신합니다. 통합 서비스에서 각 연결은 자신만의 토큰 버켓을 부여받습니다. 차별화된 서비스에서, 전체 서브네트나 일정 범위의 클라이언트들은 하나의 토큰 버켓을 공유합니다.

통신량 제어 기능

통신 제어 기능은 통합 서비스 정책에만 적용됩니다. 예측 가능한 결과를 얻으려면, 통신 경로에 따라 RSVP 작동 가능 하드웨어가 있어야 합니다. 또한 RSVP 프로토콜을 사용하기 위해서는 라우터에 특정 통신량 제어 기능이 있어야 합니다. 이것을 RSVP 작동 가능 또는 QoS 작동 가능이라고 합니다. 사용자 서버가 클라이언트 또는 서버의 두 가지 역할 중 어느 하나를 수행할 수 있음을 기억하십시오. 이때에는 라우터로 사용될 수 없습니다.

통신량 제어 기능은 다음과 같습니다.

패킷 스케줄러
패킷 스케줄러는 IP 헤더의 정보를 기초로 패킷 이송을 관리합니다. 패킷 스케줄러는 패킷 전달이 사용자가 정책에 설정한 매개변수에 해당하는 것인지 확인합니다. 스케줄러는 패킷이 큐 처리된 위치에서 구현됩니다.

패킷 분류자
패킷 분류자는 IP 흐름 가운데 어느 패킷이 IP 헤더 정보를 기초로 서비스 레벨을 수신하는지 식별합니다. 각각의 수신 패킷은 분류자에 의해 특정 클래스 안으로 맵핑됩니다. 같은 클래스로 분류된 모든 패킷들은 같은 처리를 수신합니다. 이 서비스 레벨은 사용자가 정책에 제공한 정보를 기초로 결정됩니다.

허용 제어
허용 제어는 라우터가 새 흐름에 요구되는 QoS를 수용할만한 충분한 라우팅 자원을 가지고 있는지 판별하기 위해 사용하는 의사결정 알고리즘을 가지고 있습니다. 충분한 자원이 없으면, 새 흐름을 거부합니다. 흐름을 허용할 경우에는 요구된 QoS를 예약하기 위해 라우터가 패킷 분류자와 스케줄러를 할당합니다. 허용 제어는 예약 경로를 따라 각 라우터에서 발생합니다.

여기에서는 분류자와 스케줄러에 관한 모든 것을 논의하지 않습니다. 가능한 대체 소스를 찾으려면 QoS 관련 정보 페이지를 검토하십시오.

통합 서비스 유형

통합 서비스 유형에는 제어를 받는 로드 서비스와 보장 서비스의 두 가지가 있습니다.

제어를 받는 로드

제어를 받는 로드 서비스는 실시간 어플리케이션과 같이 혼잡한 네트워크에 민감한 어플리케이션을 지원합니다. 어플리케이션은 적은 양의 유실 및 지연은 감수해야 합니다. 어플리케이션이, 제어를 받는 로드 서비스를 사용할 경우 증가하는 네트워크 로드만큼 성능이 타격을 받지는 않습니다. 가벼운 조건의 네트워크에서 처리되는 보통의 통신량과 비슷한 서비스가 제공됩니다.

라우터는 제어를 받는 로드 서비스가 적절한 대역폭 및 패킷 처리 자원을 수신하도록 해야 합니다. 이를 위해 라우터는 통합 서비스를 지원하도록 QoS를 작동 가능하게 해야 합니다. 라우터 스펙을 검사하여 통신 제어 기능을 통해 서비스 품질을 제공하는지 확인해야 할 것입니다. 통신 제어는 패킷 스케줄러, 패킷 분류자 및 수락 제어 등으로 구성됩니다.

보장 서비스

보장 서비스는 지정된 전달 시간 내에 패킷이 반드시 도착하도록 합니다. 보장 서비스를 필요로 하는 어플리케이션에는 스트리밍 기술을 사용하는 비디오 및 오디오 브로드캐스팅 시스템이 포함됩니다. 보장 서비스는 최대 대기행렬 지연을 제어하므로 패킷은 지정된 시간 이상 지연되지 않습니다. 패킷 경로를 따라가는 모든 라우터는 전달을 보장하는 RSVP 기능을 제공해야 합니다. 토큰 버켓 한계 및 대역폭 한계를 지정할 때 보장 서비스를 정의합니다.

토큰 버켓 및 대역폭 한계

토큰 버켓 한계 및 대역폭 한계는 함께 성능 한계라고도 합니다. 이러한 성능 한계는 아웃바운드 대역폭 정책인 통합 및 차별화된 서비스에서 패킷 전달을 보장하는데 도움이 됩니다.

토큰 버켓 *크기*

토큰 버켓 *크기*는 자료 버스트를 수용하는 버퍼 용량을 결정합니다. 버스트 자료는 종료할 수 있는 속도보다 더 빠르게 어플리케이션이 서버에게 송신하도록 지정하는 정보입니다. 어플리케이션이 충분한 버스트 자료를 서버에 신속하게 송신하며 버퍼는 가득 차게 됩니다. 어플리케이션이 서버를 종료할 수 있는 것보다 더 느리게 정보를 송신하면 버퍼는 비게 됩니다. 자료가 서버에 들어가는 만큼 빠르게 서버를 떠나는 경우 토큰 버켓 *크기*는 변하지 않고 유지됩니다. 일단 버퍼가 차면 QoS는 추가적인 자료 패킷을 프로파일 외부 패킷으로 처리합니다. 이 정책에서 QoS가 프로파일 외부 통신량을 처리하는 방식을 결정할 수 있습니다.

토큰 비율 한계

비율(대역폭) 한계는 네트워크에 들어 오는 것이 허용되는 장기적인 자료 비율 또는 초당 비트 수를 지정합니다. 서버에서 RSVP를 요구하는 클라이언트는 특정 용량의 대역폭(흐름 한계)을 요구합니다. QoS 정책은 요구된 대역폭을 찾아 이를 이 정책에 대한 비율 및 흐름 한계와 비교합니다. 이 요구로 인해 서버가 한계를 초과하는 경우 서버는 요구를 거부합니다. 토큰 비율 한계는 통합 서비스 정책 내에서 수락 제어에만 사용됩니다. 이는 Kb/s 단위로 측정됩니다. 이 값은 10Kb/s에서 1Gb/s까지 다양합니다.

평균 비율 한계 또는 대역폭 한계는 최고 비율 한계 또는 최고 대역폭 한계보다 낮아야 하므로 전체 인터페이스를 모두 사용하지는 않습니다. 예를 들어 36Kb/s 이하를 사용하는 모뎀이 있는 경우 평균 비율 한계를 전체 인터페이스를 활용하지 않는 정도로 설정할 필요가 있습니다.

힌트: 어떤 한계를 설정할 것인지 결정하기 위해 모니터를 실행하고자 할 수 있습니다. 네트워크에서 대부분의 통신 자료를 수집하기에 충분히 큰 전체 토큰 비율을 설정하여 정책을 작성하십시오. 그리고나서 이 정책에 대한 자료 수집을 시작하십시오. 사용자의 어플리케이션 및 네트워크가 현재 사용하는 전체 비율을 수집하기 위한 한 가지 방법으로 현재 네트워크 통계 모니터 예제를 참조하십시오. 이 결과를 사용하여 한계를 적절히 감소시킬 수 있습니다.

자세한 내용은 차별화된 서비스 클래스 및 통합된 서비스 주제를 참조하십시오.

차별화된 서비스 표시를 사용하는 통합 서비스

이것은 보통 혼합된 환경에서 사용되는 정책입니다. 혼합 환경은 통합 서비스 예약을 지원하지 않지만 차별화된 서비스를 지원하는 다른 라우터를 통해 통합 서비스 예약이 이동할 때 발생합니다. 통신량이 서로 다른 정의역, 서로 다른 서비스 레벨 동의, 서로 다른 성능의 장비를 통과하기 때문에 경우에 따라서는 원하는 서비스를 받지 못할 수 있습니다.

잠재적인 문제를 해결하기 위해, 차별화된 서비스 표시를 통합 서비스 정책에 첨부할 수 있습니다. 정책이 RSVP 프로토콜을 사용할 수 없는 라우터를 통과하더라도 정책에는 계속해서 일정한 우선순위가 유지됩니다. 사용자가 추가한 표시를 홉별 작동이라고 합니다.

무신호

위에서 설명한대로 표시를 사용하는 것과 함께 새로운 기능인 “무신호” 기능을 사용할 수도 있습니다. “무신호”는 통합 서비스 정책 내에 지정됩니다. 통합 서비스 정책의 **등록 정보** 패널에서 무신호를 지정합니다.

1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
2. **서비스 품질**을 마우스 오른쪽 단추로 누른 후 **구성**을 선택하십시오.
3. **아웃바운드 대역폭 정책 —> IntServ**를 확장하십시오.
4. 위에서 작성한 정책 이름을 마우스 오른쪽 단추로 클릭하고 **등록 정보**를 선택하면 IntServ 등록 정보 대화상자가 나타납니다.
5. **통신 관리** 탭을 선택하여 신호를 작동 가능 또는 작동 불가능으로 설정하십시오. 여기에서 스케줄, 클라이언트, 어플리케이션 및 통신 관리도 편집할 수 있습니다.

통신 관리 탭을 선택하면 “무신호” 버전의 API를 사용하여 RSVP 규칙을 서버에 로드하는 어플리케이션을 작성할 수 있고 TCP/IP 대화에서 서버 측 어플리케이션만 RSVP 작동 가능 상태면 됩니다. RSVP 신호는 클라이언트를 대신하여 자동으로 수행됩니다. 클라이언트 측에서 RSVP 프로토콜을 사용할 수 없는 경우에도 어플

리케이션에 대한 RSVP 연결을 작성합니다.

«

자세한 정보는 차별화된 서비스 클래스 및 통합 서비스 주제를 참조하십시오.

RSVP 프로토콜 및 QoS API

»

RSVP(자원 예약 프로토콜)은 RAPI API 또는 qtoq QoS 소켓 API와 함께 통합 서비스 예약을 수행합니다. 통신량이 지나는 모든 노드에 반드시 RSVP 프로토콜을 사용할 수 있는 능력이 있어야 합니다. 통합 서비스 정책을 수행하는 기능을 RSVP 작동 가능이라고 합니다. RSVP 프로토콜을 사용하기 위해 필요한 라우터 기능에 대한 자세한 내용은 통신 제어 기능을 참조하십시오.

RSVP 프로토콜은 통신 경로를 따라 설치된 모든 네트워크 노드에서 RSVP 예약을 작성하는 데 사용됩니다. 그리고 사용자 정책에 서비스(요구되는)를 제공하기에 충분히 예약 기간을 유지합니다. 예약이 대화에서 자료가 요구하는 처리 및 대역폭을 정의합니다. 각 네트워크 노드는 예약에 정의된 자료 처리를 제공하는 데 동의합니다.

RSVP는 한 방향으로(리시버에서)만 예약을 처리하는 단순 프로토콜입니다. 오디오 및 비디오 회의와 같은 더 복잡한 연결에서는 각각의 송신자도 리시버입니다. 이 경우, 반드시 양쪽에 RSVP 세션을 설정해야 합니다.

또한 RSVP 작동 가능 라우터의 경우, 통합 서비스를 사용하기 위해서는 RSVP 작동 가능 어플리케이션이 필요합니다. iSeries 서버에 현재 RSVP 작동 가능 어플리케이션이 없는 경우 RAPI API 또는 qtoq QoS 소켓 API를 사용하여 어플리케이션을 작성해야 합니다. 이것이 RSVP 프로토콜을 사용할 수 있도록 어플리케이션을 작동 가능하게 만듭니다. 자세한 설명이 필요한 경우 이러한 모델, 조작 및 메세지 처리에 대해 설명하는 여러 소스가 있으니 찾아 보시기 바랍니다. RSVP 프로토콜 및 인터넷 RFC 2205에 대해서는 완벽하게 이해할 필요가 있습니다.

qtoq 소켓 API
qtoq QoS 소켓 API를 사용하여 iSeries 시스템에서 RSVP 프로토콜을 사용하는 데 필요한 작업을 단순화할 수 있습니다. qtoq 소켓 API는 RAPI API를 호출하고 일부 복잡한 타스크를 수행합니다. qtoq 소켓 API는 RAPI API만큼 유연하지는 않으나 보다 간단하게 동일한 기능을 제공합니다. ″무신호″ 버전의 API를 사용하여 다음을 작성할 수 있습니다.

- 서버에서 RSVP 규칙을 로드하는 어플리케이션
- RSVP를 작동하기 위해 (TCP/IP 대화에서) 서버 측 어플리케이션만을 필요로 합니다.

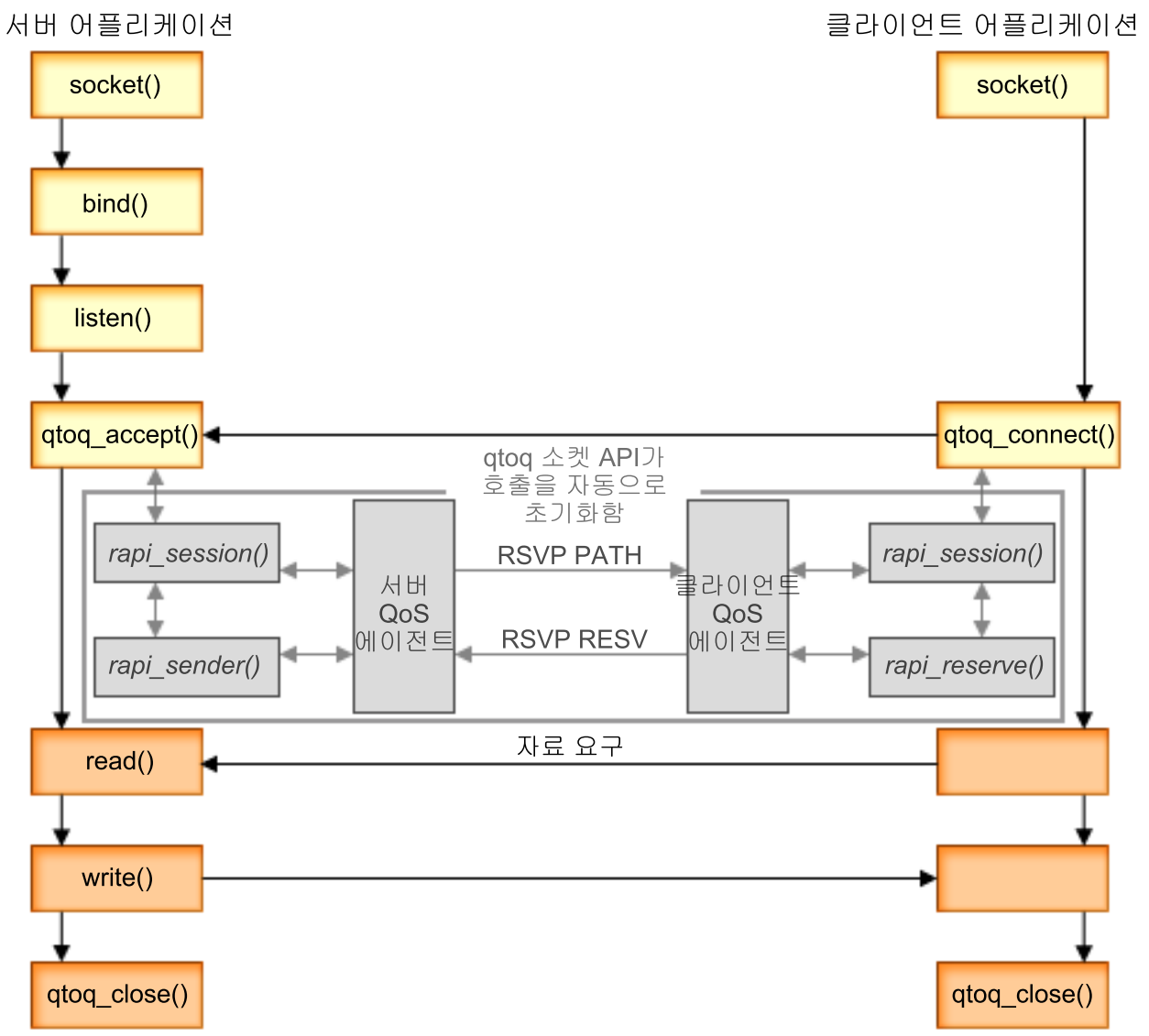
RSVP 신호는 클라이언트를 대신하여 자동으로 수행됩니다.

연결 지향 또는 무접속 qtoq QoS 소켓을 사용하는 어플리케이션/프로토콜에 대한 일반적인 QoS API 흐름은 QoS API 연결 지향 기능 흐름 페이지 또는 QoS API 무접속 기능 흐름 페이지를 참조하십시오.

QoS API 연결 지향 기능 흐름

다음 그림은 TCP와 같은 연결 지향 프로토콜에 대한 QoS 작동 가능 API qtoq 소켓 기능의 클라이언트/서버 관계를 보여줍니다.

QoS 작동 가능 API 기능이 RSVP 초기화를 요구하는 연결 지향 흐름에 대해 호출되었을 때 추가적인 기능이 초기화됩니다. 이 기능으로 인해 클라이언트와 서버의 QoS 에이전트는 클라이언트와 서버 간의 자료 흐름에 대해 RSVP 프로토콜을 설정할 수 있습니다.



qtoq 이벤트 흐름: 다음 소켓 호출 순서는 그래픽 설명을 제공합니다. 또한 연결 지향 설계에서 서버와 클라이언트 어플리케이션 사이의 관계를 설명합니다. 이것은 기본적인 소켓 API를 수정한 것입니다.

서버 측

"무신호"로 표시된 규칙에 대한 qtoq_accept()

1. 어플리케이션은 소켓 설명자를 얻기 위해 socket() 함수를 사용합니다.
2. 어플리케이션은 listen()을 호출하여 어떤 연결이 대기할 것인지를 지정합니다.
3. 어플리케이션은 qtoq_accept()를 호출하여 클라이언트로부터의 연결 요구를 기다립니다.
4. API는 rapi_session() API를 호출하고 이것이 성공하면 QoS 세션 ID가 지정됩니다.
5. API는 표준 accept() 함수를 호출하여 클라이언트 연결 요구를 기다립니다.

6. 연결 요구가 수신되면 수락 제어가 요구된 규칙에 대해 수행됩니다. 규칙은 유효한 경우 TCP/IP 스택으로 보내지고 결과 및 세션 ID와 함께 호출 어플리케이션으로 리턴됩니다.
7. 서버 및 클라이언트에 대한 어플리케이션은 원하는 자료 전송을 수행합니다.
8. 어플리케이션은 qtoq_close() 함수를 호출하여 소켓을 닫고 규칙을 언로드합니다.
9. QoS 서버는 QoS 관리자로부터 규칙을 삭제하고 QoS 세션을 삭제하고 기타 필요한 클린업 조치를 수행합니다.

일반적인 RSVP 신호를 사용하는 qtoq_accept()

1. 어플리케이션은 소켓 설명자를 얻기 위해 socket() 함수를 사용합니다.
2. 어플리케이션은 listen()을 호출하여 어떤 연결이 대기할 것인지를 지정합니다.
3. 어플리케이션은 qtoq_accept()를 호출하여 클라이언트로부터의 연결 요구를 기다립니다.
4. 연결 요구가 수신되면 rapi_session() API가 호출되어 이 연결에 대한 Qos 서버에서 세션을 작성하고 QoS 세션 ID를 획득하여 호출자에게 리턴됩니다.
5. rapi_sender() API가 호출되어 QoS 서버로부터의 PATH 메세지를 시작하고 클라이언트로부터 RESV 메세지를 기다리고 있음을 QoS 서버에 알립니다.
6. rapi_getfd() API가 호출되어 어플리케이션이 QoS 이벤트 메세지를 기다리는 데 사용하는 설명자를 확보합니다.
7. 수락 설명자 및 QoS 설명자가 어플리케이션으로 리턴됩니다.
8. QoS 서버는 수신할 RESV 메세지를 기다립니다. 메세지가 수신되면 QoS 관리자와 함께 적절한 규칙을 로드하고 어플리케이션에서 qtoq_accept() API 호출에 대한 통지를 요구한 경우 메세지를 보냅니다.
9. QoS 서버는 계속해서 설정된 세션에 대한 화면정리를 제공합니다.
10. 어플리케이션은 연결이 완료되면 qtoq_close()를 호출합니다.
11. QoS 서버는 QoS 관리자로부터 규칙을 삭제하고 QoS 세션을 삭제하고 필요한 기타 클린업 조치를 수행합니다.

클라이언트 측

일반적인 RSVP 신호를 사용하는 qtoq_connect()

1. 어플리케이션은 소켓 설명자를 얻기 위해 socket() 함수를 사용합니다.
2. 어플리케이션은 qtoq_connect() 함수를 호출하여 연결하려는 서버 어플리케이션에 알립니다.
3. qtoq_connect() 함수는 rapi_session() API를 호출하여 이 연결에 대한 QoS 서버를 사용하여 세션을 작성합니다.
4. QoS 서버는 요구된 연결로부터 PATH 명령을 기다리도록 우선순위가 지정됩니다.
5. rapi_getfd() API가 호출되어 어플리케이션이 QoS 메세지를 기다리는 데 사용할 QoS 설명자를 확보합니다.
6. connect() 함수가 호출됩니다. connect() 결과 및 QoS 설명자가 어플리케이션에 리턴됩니다.

7. QoS 서버는 수신할 PATH 메세지를 기다립니다. 메세지가 수신되면 RESV 메세지를 사용하여 어플리케이션 서버 기계에 있는 QoS 서버에 응답합니다.
8. 어플리케이션이 통지를 요구한 경우 QoS 서버는 QoS 설명자를 통해 어플리케이션으로 통지를 보냅니다.
9. QoS 서버는 계속해서 설정된 세션에 대한 화면정리를 제공합니다.
10. 어플리케이션은 연결이 완료되면 qtoq_close()를 호출합니다.
11. QoS 서버는 QoS 세션을 닫고 기타 필요한 클린업 조치를 수행합니다.

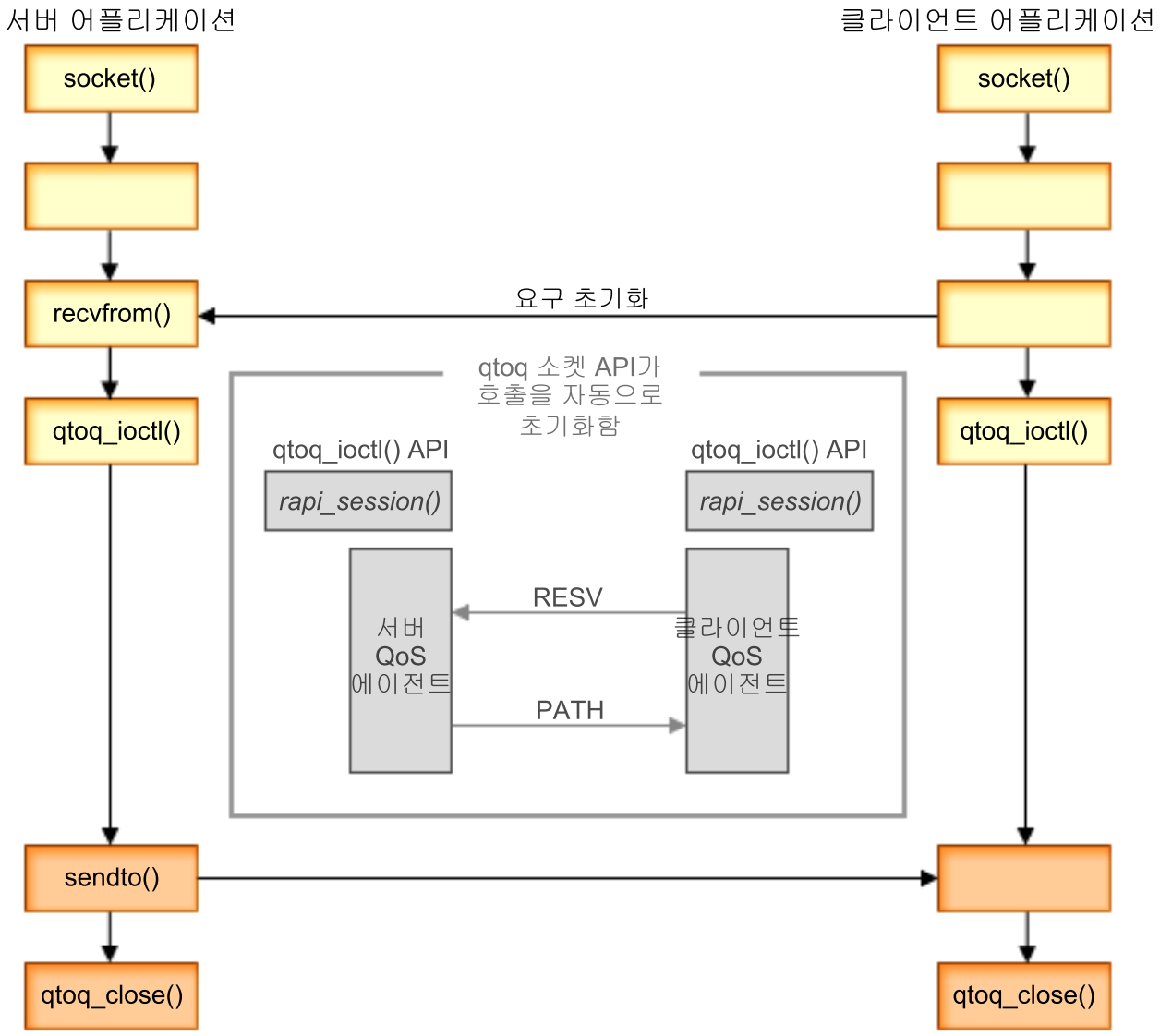
″무신호″로 표시된 규칙에 대한 qtoq_connect()

이 경우 클라이언트로부터 응답을 받을 필요가 없으므로 이 요청은 클라이언트 측에서는 유효하지 않습니다.

QoS API 무접속 기능 흐름

다음의 서버 및 클라이언트 예제는 무접속 흐름을 위해 작성된 qtoq QoS 소켓 API를 보여줍니다.

QoS 작동 가능한 API 기능이 RSVP 초기화를 요구하는 무접속 흐름에 대하여 호출되었을 때 추가적인 기능이 초기화됩니다. 이 기능으로 인해 클라이언트와 서버의 QoS 에이전트는 클라이언트와 서버 간의 자료 흐름에 대해 RSVP 프로토콜을 설정할 수 있습니다.



qtoq 이벤트 흐름: 다음 소켓 호출 순서는 그래픽 설명을 제공합니다. 또한 무접속 설계에서 서버와 클라이언트 어플리케이션 사이의 관계를 설명합니다. 이것은 기본적인 소켓 API를 수정한 것입니다.

서버 측

"무신호"로 표시된 규칙에 대한 qtoq_ioctl()

1. 요구된 규칙에 대해 수락 제어를 수행하라고 요청하는 메세지를 QoS 서버에 보냅니다.
2. 규칙이 수락될 수 있는 경우 규칙을 로드하도록 요구하는 메세지를 QoS 서버에 보내는 기능을 호출합니다.
3. 호출자에게 해당 요구의 성공 또는 실패 여부를 나타내는 상태를 리턴합니다.
4. 해당 연결을 사용하여 어플리케이션이 완료되면 qtoq_close() 기능을 호출하여 연결을 닫습니다.

5. QoS 서버는 QoS 관리자로부터 규칙을 삭제하고 QoS 세션을 삭제한 후 기타 필요한 클린업 조치를 수행합니다.

일반적인 RSVP 신호를 사용하는 qtoq_ioctl()

1. 요구된 연결에 대한 수락 제어를 요구하는 메세지를 QoS 서버에 보냅니다.
2. rapi_session()을 호출하여 규칙에 대한 세션 설정을 요구하고 호출자에게 QoS 세션 ID를 리턴하도록 합니다.
3. rapi_sender()를 호출하여 PATH 메세지를 다시 클라이언트로 초기화합니다.
4. rapi_getfd()를 호출하여 QoS 이벤트를 기다리기 위한 파일 설명자를 확보합니다.
5. select() 설명자, QoS 세션 ID 및 상태를 호출자에게 리턴합니다.
6. QoS 서버는 RESV 메세지를 수신하면 규칙을 로드합니다.
7. 연결이 완료되면 어플리케이션이 qtoq_close()를 발행합니다.
8. QoS 서버는 QoS 관리자로부터 규칙을 삭제하고 QoS 세션을 삭제하고 필요한 기타 클린업 조치를 수행합니다.

클라이언트 측

일반적인 RSVP 신호를 사용하는 qtoq_ioctl()

1. rapi_session()을 호출하여 연결에 대한 세션 설정을 요구합니다. rapi_session() 함수는 해당 연결에 대한 수락 제어를 요구합니다. 클라이언트에 대해 구성된 규칙이 있는 경우 및 현재 활동 중이 아닌 경우에만 클라이언트 측에서 연결을 거부합니다. 이 함수는 어플리케이션으로 다시 전달된 QoS 세션 ID를 리턴합니다.
2. rapi_getfd()를 호출하여 QoS 이벤트를 기다리기 위한 파일 설명자를 확보합니다.
3. qtoq_ioctl()은 대기중 설명자 및 세션 ID와 함께 호출자에게 리턴합니다.
4. QoS 서버는 수신할 PATH 메세지를 기다립니다. 경로 메세지를 수신하면 RESV 메세지로 응답한 후 이벤트가 세션 설명자를 통해 발생했음을 어플리케이션에 신호합니다.
5. QoS 서버는 계속해서 설정된 세션에 대한 화면정리를 제공합니다.
6. 클라이언트 코드는 연결이 완료되면 qtoq_close()를 호출합니다.

″무신호″로 표시된 규칙에 대한 qtoq_ioctl()

이 경우 클라이언트로부터 응답을 받을 필요가 없으므로 이 요청은 클라이언트 측에서는 유효하지 않습니다.

«

QoS 계획

»

서비스 품질 구현에 있어서 가장 중요한 단계는 계획입니다. 예상된 결과를 수신하기 위해서는 반드시 네트워크 장비를 검토하고 네트워크 통신량을 모니터해야 합니다. QoS계획 어드바이저는 계획 단계 중에 사용자가 답해야 하는 기본 질문을 통해 안내를 제공합니다.어드바이저 외에도 QoS를 시작하기 전에 하위 주제들을 모두 살펴보십시오.

권한 요구사항
QoS 및 디렉토리 서버를 정상적으로 구성하는 데 필요한 권한을 모두 나열합니다.

시스템 요구사항
QoS를 작동시키기 위해 필요한 모든 요구사항이 나옵니다.

QoS 정책 순서화
파일에 나타난 정책 순서가 처리 순서입니다. 이것은 차별화된 서비스 정책 및 연결 비율 정책에만 적용합니다.

서비스 레벨 동의
서비스 레벨 동의는 QoS 가운데 중요한 부분 중 하나입니다. QoS 계획의 일부로 네트워크 제공자와 함께 SLA를 이해하고 설정해야 합니다.

네트워크 하드웨어 및 소프트웨어
서비스 품질은 가장 취약한 링크나 다름없습니다. 네트워크 내부 장비와 네트워크 외부 장비의 성능은 QoS 결과에 영향을 미칩니다.

네트워크 성능
QoS는 네트워크 성능에 대한 모든 것입니다. QoS를 고려하게 된 기본 이유는 이미 네트워크 혼잡과 패킷 유실을 경험하고 있기 때문일 것입니다. 정책을 구현할 때는 먼저 IP 통신량의 현재 성능 레벨를 확인하기 위해 QoS 모니터를 사용할 수 있습니다. 이 결과를 통해 혼잡이 발생하는 위치를 판별하는 데 도움을 받을 수 있습니다. 문제 해결 아래 나오는 서버 트랜잭션 모니터 주제를 참조하십시오.

QoS 계획 어드바이저
서비스 품질(QoS)를 구현하기 전에 기본적인 질문 내용을 고려하십시오. 현재 사용하는 어플리케이션의 성능을 기초로 제안된 정책과 함께 계획 작업 양식을 수신하게 됩니다.

권한 요구사항

서비스 품질 정책에는 사용자 네트워크에 대한 중요한 정보가 들어 있을 수 있습니다. 따라서 QoS 관리 권한은 필요한 경우에만 부여해야 합니다. QoS 정책 또는 LDAP 디렉토리 서버를 구성하려면 다음과 같은 권한이 필요합니다. QoS 정책이 LDAP 디렉토리 서버에 저장되므로 두 가지 권한이 모두 필요합니다.

디렉토리 서버 관리에 필요한 권한 부여
QoS 관리자는 *ALLOBJ 권한 및 *IOSYSCFG가 필요합니다. 이를 대신할 수 있는 권한에 대한 내용은 디렉토리 서버 구성을 참조하십시오.

TCP/IP 서버를 시작하기 위한 권한 부여
STRTCPSVR 및 ENDTCPSVR 명령에 오브젝트 권한을 부여하려면 다음 단계를 따르십시오.

1. **STRTCPSVR**: 명령행에서 GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE)를 입력하십시오. ADMINPROFILE은 사용자의 관리자 프로파일 이름으로 대체하고 **Enter**를 클릭하십시오.
2. **ENDTCPSVR**: 명령행에서 GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE)를 입력하십시오. ADMINPROFILE은 사용자의 관리자 프로파일 이름으로 대체하고 **Enter**를 클릭하십시오.

모든 오브젝트 액세스 및 시스템 구성 권한을 부여하십시오.
QoS를 구성하려는 사용자는 보안 담당자 액세스를 가지고 있는 것이 좋습니다. 모든 오브젝트 액세스 및 시스템 구성 권한을 부여하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 사용자 서버 —> **사용자 및 그룹**을 확장하십시오.
2. **모든 사용자**를 더블 클릭하십시오.
3. 관리자의 사용자 프로파일을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
4. 등록 정보 대화 상자에서 **기능**을 클릭하십시오.
5. 기능 페이지에서 **모든 오브젝트 액세스 및 시스템 구성**을 선택하십시오.
6. **확인**을 클릭하여 기능 페이지를 닫으십시오.
7. **확인**을 눌러 등록 정보 대화 상자를 닫으십시오.

시스템 요구사항

서비스 품질(QoS)은 오퍼레이팅 시스템의 통합 부분입니다. QoS를 구성하고 시작하기 위해서는 최소한 버전 5 릴리스 1 OS/400(R)이 있어야 합니다. 또한 다음 요구사항을 완료해야 합니다.

1. TCP/IP 연결 유틸리티(*xx*-TC1) 설치.
2. PC에 iSeries Navigator를 설치하십시오. Client Access를 설치하는 동안 네트워킹 섹션이 설치되는지 확인하십시오. 서비스 품질은 네트워킹 안의 IP 정책에 있습니다.

주: TCP/IP, 네트워킹 또는 IP 주소에 대한 자세한 내용은 QoS 관련 정보의 TCP/IP Tutorial and Technical Overview 및 V4 TCP/IP for AS/400(R): More Cool Things Than Ever를 참조하십시오.

QoS 정책 순서화

두 개의 차별화된 서비스 정책이 겹치거나 두 개의 연결 비율 정책이 겹치는 경우 iSeries Navigator에서의 정책의 실제 순서가 중요합니다. 중첩된 정책은 같은 클라이언트, 어플리케이션, 스케줄 또는 프로토콜를 사용하는 두 개의 정책을 말합니다. iSeries Navigator 화면의 정책은 순서화된 리스트로 표시됩니다. 정책의 우선권은 리스트에 나오는 정책의 순서에 따라 결정됩니다. 하나의 정책이 다른 정책에 대해 우선권을 행사하기 위해서는 높은 우선순위 정책을 리스트에 먼저 표시해야 합니다.

정책이 다른 정책과 중첩되는지 판별하려면, 다음 지침을 수행하십시오.

1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭하십시오.
3. **구성**을 선택하십시오.
4. 특정 정책 폴더를 선택하십시오.
5. 중첩된 정책에 연관된 정책명을 마우스 오른쪽 버튼으로 클릭하십시오. 중첩된 정책은 정책 앞의 아이콘으로 중첩 상태를 나타냅니다.
6. **중첩 표시**를 선택하십시오. 중첩 패널이 표시됩니다.

화면에서 정책 순서를 변경하려면 다음 단계를 사용하십시오.

- 정책을 강조표시하고 화면에서 위, 아래 화살표를 사용하여 정책 순서를 변경할 수 있습니다.
- 정책명을 마우스 오른쪽 버튼으로 클릭하고 **위로 이동** 또는 **아래로 이동**을 선택하십시오.
- QoS 서버를 갱신하십시오. 자세한 지침은 도구 모음에서 서버 갱신 버튼을 사용하거나 QoS 타스크 도움말을 사용하십시오.

서비스 레벨 계약

이 절은 서비스 레벨 계약(SLA) 제공자에 관한 교육용 정보가 아니라 SLA 가운데 서비스 품질(QoS) 구현 시 사용자에게 영향을 줄 수 있는 중요한 요소들을 정리한 것입니다. 귀사의 정책과 예약은 가장 취약한 링크에 다름없습니다. 클라이언트와 서버 사이의 노드가 차별화된 서비스나 통합 서비스 주제에서 논의된 통신량 처리 특성을 수행할 수 없다면 사용자가 의도한대로 정책이 처리되지 않을 것입니다. 귀사의 SLA가 충분한 자원을 허용하지 않을 경우에는 최상의 정책이라 할지라도 네트워크 혼잡 문제에 도움이 되지 않을 것입니다.

또한 이 섹션에는 ISP 간의 계약 내용도 들어 있습니다. 정의역 전체에 걸쳐서 모든 ISP가 반드시 요구되는 서비스 품질을 제공할 것에 동의해야 합니다. 경우에 따라서는 상호운영성이 문제(challenge)를 발생시킬 수도 있습니다.

사용자가 실제로 수신하는 서비스 레벨을 반드시 이해하도록 하십시오. 통신량 조건지정 동의는 통신량을 어떻게 처리할지(드롭, 표시, 셰이프 또는 재전송)에 관한 설명입니다. 서비스 품질(QoS)를 제공하는 주된 목적은 잠재성, 지터, 대역폭, 패킷 유실, 가용성 및 처리량 등을 조절하기 위한 것입니다. 서비스 계약은 요구하는 정책을 사용자에게 제공할 수 있어야 합니다. 필요한 만큼 충분한 서비스를 받고 있는지 확인하십시오. 그렇지 않다면, 자원을 낭비하는 것일 수 있습니다. 예를 들어 IP 전화 통신에 500kbps 예약을 요청하지만 어플리케이션에 20kbps만 필요하다면, ISP로부터 어떤 통지도 받지 못한 채 여분의 비용을 지불해야 합니다.

네트워크 하드웨어 및 소프트웨어

내부 장비와 네트워크 밖의 기타 장비가 제공하는 기능이 QoS 결과에 많은 영향을 미칩니다.

어플리케이션
통합 서비스 정책에는 RSVP 작동 가능 어플리케이션이 필요합니다. iSeries 어플리케이션이 현재 RSVP 작동 가능 상태가 아니기 때문에, RSVP 프로토콜을 사용하기 위해서는 작동 가능하게 해야 합니다. 어플리케이션을 작동하게 하려면 RAPI(Resource Reservation Setup Protocol) API 및 qtoq QoS 소켓 API를 사용하여 특별한 프로그램을 작성해야 합니다. 이 프로그램을 통해 어플리케이션이 RSVP를 사용할 수 있습니다. 자세한 내용은 RSVP 프로토콜 및 QoS API를 참조하십시오.

네트워크 노드
라우터, 스위치 및 사용자 서버까지도 서비스 품질을 사용할 수 있는 기능을 가지고 있어야 합니다. 차별화된 서비스 정책을 사용하기 위해서는 차별화된 서비스를 작동할 수 있는 장비가 필요합니다. 이것은 네트워크 노드가 IP 패킷을 분류, 미터, 마크, 셰이프할 수 있어야 한다는 것을 의미합니다. 통신량 조절기(분류, 미터, 마크, 드롭)에 대한 자세한 내용은 통신량 조절기를 참조하십시오.

통합 서비스 정책을 사용하기 위해서는 RSVP를 작동할 수 있는 장비가 필요합니다. 이것은 네트워크 노드가 RSVP 프로토콜을 지원할 수 있어야 한다는 것을 의미합니다. RSVP 프로토콜에 대한 자세한 내용은 RSVP를 참조하십시오.

QoS 구성

iSeries Navigator에서 마법사를 사용하여 QoS 정책을 작성합니다. 마법사가 사용자의 구성을 통해 완벽하게 작업을 완료합니다.

»

정책을 구성한 후에는 iSeries Navigator에서 구성 오브젝트를 사용하여 정책 구성을 편집할 수 있습니다. 구성 오브젝트는 정책을 구성하는 각 부분들입니다. iSeries Navigator에서 서비스 품질을 열면 클라이언트, 어플리케이션, 스케줄, 정책, 서비스 클래스, 홉별 작동 및 URI로 레이블 처리된 폴더가 있습니다. 이 오브젝트를 사용하여 정책을 작성할 수 있습니다. 오브젝트에 대한 자세한 내용은 iSeries Navigator의 서비스 품질 개요 도움말을 참조하십시오.

디렉토리 서버 구성
QoS에서 디렉토리 서버를 구성하는 방법에 대한 정보가 필요할 때 사용하십시오.

마법사를 사용하여 QoS 구성
QoS 마법사에 액세스하는 방법에 관한 지침이 필요할 때 사용하십시오.

«

QoS 작동 가능
정책을 유효하게 만들기 위해서는 먼저 정책을 작동 가능하게 해야 합니다. 마법사를 사용할 경우, 사용자를 대신하여 서버가 자동으로 정책을 작동 가능하게 합니다. 구성 오브젝트를 사용하여 정책을 변경한

경우 정책을 사용하기 전에 동적으로 서버 갱신을 수행해야 할 것입니다. 작동 가능하게 만들기 전에 문제를 발생시킬 가능성이 있는 중첩된 정책은 없는지 확인하십시오. 자세한 내용은 QoS 정책 순서화를 참조하십시오.

디렉토리 서버 구성

QoS 정책 구성은 이제 LDAP 디렉토리 서버에 저장됩니다. 그러면 QoS 솔루션 관리가 훨씬 쉬워집니다. 서버 전체에서 QoS 정책을 구성하는 대신 구성 데이터를 하나의 로컬 디렉토리 서버에 저장하여 여러 시스템이 공유하도록 할 수 있습니다. 맨 처음 서버에서 서비스 품질을 구성할 때 초기 구성 마법사가 나타납니다. 이 마법사에서 디렉토리 서버를 구성하도록 프롬트합니다.

디렉토리 서버를 구성하려면 다음과 같은 정보를 결정하거나 알고 있어야 합니다.

- 디렉토리 서버 이름
- QoS 정책을 참조할 식별명(DN)을 결정하십시오.
- LDAP 디렉토리 서버와 함께 SSL 보안을 사용할 것인지 여부를 결정하십시오.
- 디렉토리 서버에서 정책 검색 성능을 향상시키기 위한 키워드를 사용할 것인지 여부를 결정하십시오.

주: 현재 Kerberos는 QoS 서버가 디렉토리에 액세스할 때 사용할 인증 메소드로 구성할 수 없습니다.

LDAP 디렉토리 서버를 관리하려면 다음 권한 세트 중 하나가 있어야 합니다.

- *ALLOBJ 권한 및 *IOSYSCFG 권한
- ENDTCP(TCP/IP 종료), STRTCP(TCP/IP 시작), STRTCPSVR(TCP/IP 서버 시작) 및 ENDTCPSVR(TCP/IP 서버 종료) 명령에 대한 *JOBCTL 권한 및 오브젝트 권한
- OS/400(R) 보안 감사를 구성하기 위한 *AUDIT 권한.

iSeries Navigator를 사용하는 경우 이미 디폴트 QoS 스키마에 대한 액세스를 갖게 됩니다. 그러나 iSeries Navigator 이외의 편집기를 사용하는 경우 아래에서 설명되는 LDIF 파일을 가져와야 합니다. 또한 편집 후에 원래의 디폴트 파일을 다시 로드하려고 하는 경우에도 이 파일을 가져올 수 있습니다.

QoS 스키마

QoS 서버에 유효한 LDAP 오브젝트 유형을 지정하는 스키마라고 하는 규칙 세트가 있습니다. V5R2 iSeries 서버에서의 스키마에는 QoS에 필요한 규칙이 포함됩니다. 그러나 사용된 LDAP 서버가 iSeries 서버가 아닌 경우 이 규칙을 LDAP 서버로 가져와야 합니다. 이는 LDIF(LDAP 자료 교환 형식) 파일을 사용하여 이루어집니다. LDIF 파일을 다운로드하려면 iSeries LDAP web page  를 참조하십시오. 왼쪽 분할 창의 **범주 —> TCP/IP 정책**에서 이 파일을 찾을 수 있습니다.

LDIF 파일 편집

IBM(R) SecureWay(R) 디렉토리 관리 툴(DMT)을 사용하여 LDAP 서버에 대한 스키마 파일을 편집할 수 있습니다. 또한 DMT의 setup.exe 파일을 PC로 FTP할 수도 있습니다. setup.exe 파일은 서버의 /qibm/proddata/os400/dirsrv/UserTools/Windows에 위치해야 합니다. 원래의 QoS 스키마는 iSeries LDAP

웹 페이지에서 구할 수 있습니다. QoS 스키마에 대한 LDAP 개념을 참조하십시오. 스키마 파일은 서버의 /QIBM/UserData/OS400/DirSrv에 위치합니다.

마법사를 사용하여 QoS 구성

서비스 품질 정책을 구성하려면 iSeries Navigator에 있는 QoS 마법사를 사용해야 합니다. 다음은 마법사 및 그 기능에 관한 리스트입니다.

초기 구성 마법사
이 마법사를 사용하여 시스템 특정 구성 및 디렉토리 서버 정보를 설정할 수 있습니다.

신규 IntServ 정책 마법사
신규 IntServ 정책 마법사를 사용하여 통합 서비스 정책을 작성할 수 있습니다. 이 정책은 서버 대역폭을 간접적으로 제어하는 RSVP 요구를 수락 또는 거부합니다. 사용자가 설정한 정책 성능 한계는 서버가 클라이언트의 RSVP 어플리케이션으로부터 수신하는 요구된 대역폭을 처리할 수 있는지 여부를 결정합니다. 이 마법사에서 작성된 통합 서비스 정책을 구현하려면 RSVP 준비 완료 라우터 및 어플리케이션이 필요합니다.

> **주:** 통합 서비스 정책을 설정하기 전에 RSVP 프로토콜을 사용할 어플리케이션을 직접 작성해야 합니다. 자세한 내용은 RSVP 프로토콜 및 QoS API를 참조하십시오.

신규 DiffServ 정책 마법사
이 마법사를 통해 TCP/IP 통신량에 우선순위를 지정하고 차별화할 수 있습니다. 또한 정책을 작성하여 통신량을 차별화할 수 있습니다. 정책 내에서 어플리케이션과 포트에 우선순위를 지정하고 이 정책의 활동 시점을 지정할 수 있습니다.

신규 DiffServ 서비스 클래스 마법사
네트워크에서 라우터와 스위치에 사용되는 패킷 표시를 설정하려면 차별화된 서비스 클래스 마법사를 사용하십시오. 또한 네트워크의 통신량에 대한 성능 한계를 지정할 수 있습니다. DiffServ 정책의 서비스 클래스를 사용합니다.

신규 연결 비율 마법사
인바운드 연결 비율 마법사를 사용하여 서버에 대한 연결을 제한하십시오. TCP/IP 주소, 어플리케이션 또는 로컬 인터페이스에 의해 액세스를 제한할 수 있습니다. 이를 사용하여 시스템 관리자는 특정 클라이언트에서 사용자 서버로의 액세스 또는 서버 어플리케이션이나 인터페이스로의 액세스를 제어할 수 있습니다. 또한 서버 성능을 향상시킬 수 있습니다.

신규 URI 마법사
인바운드 URI 마법사를 사용하여 서버에 대한 연결을 제한할 수 있습니다. URI, 어플리케이션 또는 iSeries

서버의 로컬 인터페이스에 의해 액세스를 제한할 수 있습니다. 이를 사용하여 시스템 관리자는 서버 상의 특정 URI, 어플리케이션 또는 인터페이스에 대한 액세스를 제어할 수 있습니다. 또한 서버 성능을 향상시킬 수 있습니다.

주: URI 요구 비율 정책을 설정하기 전에 다음 단계를 수행해야 합니다.

1. `WRKHTTPCFG` - Apache 웹 서버 인스턴스를 수정하십시오. FRCA(빠른 응답 캐시 가속기) 옵션을 사용하여 청취 지시문을 통해 포트를 작동 가능하게 하십시오.
2. `STRTCPSVR SERVER(*HTTP) HTTPSRV(`인스턴스 이름`)`.
3. iSeries Navigator에서 QoS를 사용하여 URI 정책을 작성 또는 수정하십시오. URI 정책에 정의된 어플리케이션 포트가 Apache 웹 서버 인스턴스에 정의된 FRCA ″청취 지시문″과 일치하도록 하십시오.
4. `STRTCPSVR SERVER(*QOS)`.

신규 URI 정책에 할당된 어플리케이션 포트는 Apache 웹 서버 구성에서 FRCA에 대해 작동 가능한 '청취' 지시문과 일치해야 합니다. 포트 값이 일치하지 않는 경우 QoS URI 정책은 예상대로 작동하지 않을 것입니다. URI 요구 비율 정책에 대한 설명은 연결 요구 비율 및 URI 요구 비율을 참조하십시오.

작성할 정책 유형을 결정하고 나면 위에서 설명한 적절한 마법사에서 정책을 구성할 수 있습니다. 정책 구성을 시작하려면 iSeries Navigator에서 QoS 마법사에 액세스를 참조하십시오.

iSeries Navigator에서 QoS 마법사에 액세스

QoS 마법사에 액세스하여 신규 정책을 작성하려면, 다음 단계를 수행하십시오.

1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭한 후 **구성**을 선택하십시오.
   주: 초기 구성 마법사는 다음과 같은 상황에서 표시됩니다.
   - 서버를 새로운 릴리스로 업그레이드하려고 합니다. 이 때 정보를 저장할 디렉토리 서버를 구성해야 합니다. 이 변환 중에 자료는 유실되지 않습니다.
   - 이 시스템에서 최초로 QoS 그래픽 사용자 인터페이스(GUI)를 사용하는 경우입니다.
   - 이전 구성 정보를 수작업으로 제거하고 다시 시작하고자 합니다. 이는 QoS 인터페이스가 이미 열려 있는 경우에만 발생합니다.
3. **초기 구성 마법사**를 완료하십시오. 초기 구성 마법사가 나타나지 않으면 4단계로 가십시오.
4. **정책**을 선택하십시오. **IntServ**, **DiffServ**, **연결 비율** 또는 **서버 요구 —> URI** 중 하나를 마우스 오른쪽 버튼으로 클릭하십시오.
5. **신규 정책**을 선택하십시오.

QoS 관리

QoS 정책을 활성화하고 실행했으면, 갱신이 필요할 것입니다. 다음과 같이 하여 정책을 관리할 수 있습니다.

iSeries Navigator에서 QoS 타스크 도움말에 액세스
이 주제에서는 iSeries Navigator의 QoS 타스크 도움말에 대해 매우 자주 참조합니다. 타스크 도움말을 사용하는 방법을 확실히 알지 못하면, 다음 지침을 검토하십시오.

QoS 정책 백업
자료 유실로부터 자신을 보호하기 위해 정책을 백업할 수 있습니다.

기존 정책 복사
작성하려는 정책과 유사한 기존의 정책을 복사할 수 있습니다.

동적으로 정책 갱신
서버가 실행되는 중에 동안 정책을 동적으로 갱신할 수 있습니다. 단계별 지침은 iSeries Navigator의 QoS 타스크 도움말의 *QoS 서버 갱신*을 사용하십시오.

QoS 정책 편집
기존 정책의 매개변수를 변경할 수 있습니다.

QoS 구성 등록 정보 편집
서비스 품질 구성의 등록 정보를 변경할 수 있습니다. 이 등록 정보에는 디렉토리 서버 구성, 저널링 및 서버 자동 시작에 대한 설정이 포함됩니다. 단계별 지침은 iSeries Navigator의 QoS 타스크 도움말의 *QoS 등록 정보 편집*을 사용하십시오.

QoS 정책 작동 가능
정책을 유효하게 만들기 위해서는 먼저 정책을 작동 가능하게 해야 합니다. 정책을 작동 가능하게 하기 전에 발생 가능성이 있는 오류들을 수동으로 검사하십시오. 예를 들어, 정책이 올바른 순서로 되어 있는지 확인해야 합니다. 정책 순서에 대한 자세한 정보는 QoS 정책 순서화를 참조하십시오. 단계별 지침은 iSeries Navigator의 QoS 타스크 도움말의 *QoS 정책 작동 가능*을 사용하십시오.

QoS 정책 모니터
정책을 관리할 때, 정책이 사용자의 의도대로 작업하는지 확인하기 위해 QoS 모니터를 분석할 수 있습니다.

QoS 정책 보기
중첩된 정책을 조사하여, 예상한 것과 서로 다른 결과를 발생시키는 곳을 판별할 수 있습니다. 문제의 발생 소지가 있는 정책에서 중첩을 검사할 수 있습니다. 활성화 및 테스트 전 또는 인쇄 및 백업 전에 중첩을 볼 수 있습니다. 이것은 테스트에 앞서 오류를 최소화하거나 제거하는 데 유용한 방법입니다. 겹쳐진 정책을 보려면 QoS 정책 순서화를 참조하십시오.

iSeries Navigator에서 QoS 도움말에 액세스

서비스 품질 도움말에 액세스하려면 iSeries Navigator를 사용해야 합니다.

1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭한 후 **구성**을 선택하십시오.
3. 메뉴 바에서 **도움말 —> 도움말 주제**를 선택하십시오. 화면에 타스크 도움말 창이 나타납니다.

QoS 정책 백업

구성 파일을 백업하는 것은 매우 바람직합니다. 정책은 로컬로도 저장되고 디렉토리 서버에도 저장됩니다. 특히 통합 파일 시스템 디렉토리인 QIBM/UserData/OS400/QOS/ETC, QIBM/UserData/OS400/QOS/TEMP 및 QIBM/UserData/OS400/QOS/USR는 반드시 백업해야 합니다. 또한 QoS 서버에 대한 디렉토리 서버 발표(publishing) 에이전트를 백업해야 합니다. 발표 에이전트에는 디렉토리 서버 이름, QoS 서버에 대한 식별명(DN), 디렉토리 서버에 액세스하는 데 사용되는 포트 및 인증 정보가 포함됩니다. 유실이 발생하더라도 백업으로 시간을 절약할 수 있으며, 스크래치에서 정책을 다시 작성하는 작업을 할 수 있습니다. 다음은 사용자에게 유실된 파일을 대체할 수 있는 간단한 방법이 있는지 확인할 때 사용할 수 있는 일반적인 추가 정보입니다.

1. **통합 파일 시스템 백업 및 회복 프로그램 사용**
   아래에 표시된 백업 및 회복 책에 대한 링크를 사용하십시오.
2. **정책 인쇄**
   가장 안전한 곳에 인쇄 출력을 저장했다가 필요에 따라 정보를 다시 입력할 수 있습니다.
3. **정보를 디스크에 복사**
   복사의 경우 수동으로 다시 입력할 필요없이 정보가 전자적으로 존재하기 때문에 인쇄보다 유익합니다. 이것은 하나의 온라인 소스에서 다른 소스로 정보를 전송하기 위한 직접적인 방법을 제공합니다.

   주: iSeries 서버는 플로피 디스크가 아닌 시스템 디스크에 정보를 복사합니다. 규칙 파일은 QIBM/UserData/OS400/QOS/ETC 및 PC가 아닌 사용자가 구성한 디렉토리 서버의 식별명 내에 위치합니다. 시스템 디스크에 저장된 자료를 보호하기 위한 백업 수단으로 디스크 보호 방법을 사용할 수 있습니다.

iSeries 서버를 사용할 때는 반드시 백업 및 회복 전략을 계획해야 합니다. 자세한 내용은 백업 및 회복 을 참조하십시오.

기존 정책 복사

사용자에게 서로 간에 매우 유사한 정책이 있는 것을 발견할 때가 있습니다. 스크래치에서 모든 정책을 작성하지 말고 원래 정책을 복사한 후 원래 정책과 다른 섹션을 편집하십시오. iSeries Navigator에서 이 QoS 기능은 *신규 기본 기능*이라고 합니다. iSeries Navigator를 사용하여 정책을 복사할 수 있는 QoS 대화 상자에 액세스합니다.

기존 정책의 사본을 작성하려면 iSeries Navigator 도움말의 **기존 정책을 기초로 신규 정책 작성**에 나오는 단계를 수행하십시오.

정책이 유효하려면 QoS 서버를 시작하거나 동적 서버 갱신을 수행하여 작동 가능하게 만드십시오. 작동 가능하게 만들기 전에 문제를 발생시킬 가능성이 있는 중첩된 정책은 없는지 확인하십시오. 자세한 내용은 QoS 정책 순서화를 참조하십시오.

QoS 모니터

모니터를 사용하여 서버를 통해 IP 통신량을 분석할 수 있습니다. 이것은 네트워크에서 혼잡이 발생하는 위치를 판별하는 데 도움이 됩니다. QoS 계획 중에 유용할 뿐 아니라 문제 해결 툴로서도 유용합니다. QoS 모니터는 사용자가 네트워크를 지속적으로 모니터할 수 있게 함으로써 필요에 따라 사용자가 정책을 조정할 수 있습니다.

QoS 모니터를 실행하려면 iSeries Navigator QoS 도움말의 지침을 사용하십시오.

주: QoS 자료 콜렉션이 켜져 있고 QoS 구성을 변경할 계획이라면 모니터가 정확한 데이터를 수집하도록 다음 단계를 수행해야 합니다.

1. QoS 자료 콜렉션을 중단하십시오.
2. 구성을 변경하십시오.
3. QoS 서버를 다시 시작/갱신하십시오.
4. QoS 자료 콜렉션을 시작하십시오.

모니터 출력

수신하게 될 출력 정보는 사용자가 모니터하는 정책 유형에 따라 다릅니다. 정책 유형에는 DiffServ, IntServ(제어를 받는 로드), IntServ(보장), 연결 비율 및 URI 등이 있습니다. 평가할 필드는 정책 유형에 따라 다릅니다. 가장 관심을 끄는 값은 평가 결과를 표시하는 값입니다. 또한 기존 정의 외에 수락된 요구, 활동 연결, 연결 서비스, 연결 비율, 드롭(drop)된 요구, 프로파일 내부 패킷 수, 프로파일 내부 비트 수, 적합하지 않은 비트 수, 프로파일 외부 비트 수, 총 비트 수, 총 패킷 수 및 총 요구 수 등을 평가합니다.

위에서 측정된 필드의 정보를 참조하여 네트워크 통신량이 정책에 얼마나 적합한 것인지를 그림으로 나타낼 수 있습니다. 각 정책 유형에 대한 모니터 출력 필드에 대한 자세한 내용은 아래의 설명을 참조하십시오. 모니터를 QoS 정책과 함께 사용하는 방법에 대한 샘플은 QoS 시나리오를 참조하십시오.

- 차별화된 서비스 정책(50 페이지 참조)
- 통합 서비스(제어를 받는 로드) 정책(51 페이지 참조)
- 통합 서비스(보장) 정책(52 페이지 참조)
- URI 정책(53 페이지 참조)
- 연결 비율 정책(52 페이지 참조)

차별화된 서비스 정책

필드	설명

정책명	이 정책에 지정된 이름
프로토콜	UDP, TCP, ALL
평균 토큰 비율 한계	흐름 경로에 따라 각 라우터와 서버에서 이 정책에 의해 허용되는 평균 토큰 비율
토큰 깊이 한계	흐름 경로에 따라 각 라우터와 서버에서 이 정책에 의해 허용되는 최대 토큰 버퍼 *크기*
최고 토큰 비율 한계	연결에서 허용하는 최대 비율
프로파일 내부 패킷 수	이 정책의 매개변수에 적합하게 전송된 IP 패킷 수
프로파일 내부 비트 수	이 정책의 매개변수 내에 포함되는 전송된 비트 수
프로파일 외부 비트 수	정책 매개변수를 초과하는 전송된 비트 수
비트율	이 연결에서 허용되는 측정된 비트 수
활동 연결 수	총 활동 연결 수
통신량 프로파일	프로파일 외부 패킷에 사용된 패킷 유형. 형식은 다음과 같습니다. • 다시 표시 • 형성(shaping) • 드롭핑
총 비트 수	전송이 시작된 시간부터 모니터 콜렉션 시간까지 이 정책이 사용한 전송된 비트 수
프로파일 내부 코드점	패킷이 새 코드점으로 다시 표시될 경우, 정책 매개변수에 적합할 때 IP 패킷이 사용하는 코드점입니다.
프로파일 외부 코드점	패킷이 새 코드점으로 다시 표시될 경우 이것은 정책 매개변수를 초과할 때 IP 패킷이 사용하는 코드점입니다.
목적지 주소 범위	패킷(이 정책의 제어를 받는) 목적지 지점을 판별하는 주소 범위
총 패킷 수	모니터 콜렉션이 시작된 시간부터 이 정책을 사용하여 전송된 패킷 수
소스 포트 범위	정책으로 제어를 받는 어플리케이션을 판별하는 소스 포트 범위

통합 서비스(제어를 받는 로드) 정책

필드	설명
정책명	이 정책에 지정된 이름
프로토콜	UDP 또는 TCP
목적지 주소	패킷(이 정책의 제어를 받는) 목적지 지점을 판별하는 주소 범위
평균 토큰 비율 한계	연결 경로에 따라 각 라우터와 서버에서 이 정책에 의해 허용되는 평균 토큰 비율
토큰 깊이 한계	연결 경로에 따라 각 라우터와 서버에 이 정책으로 허용할 수 있는 최대 토큰 버퍼 *크기*
최고 토큰 비율 한계	연결에서 허용하는 최대 비율
총 패킷 수	모니터 콜렉션이 시작된 시간부터 이 정책을 사용하여 전송된 패킷 수
부적합 비트 수	정책 매개변수를 초과하는 전송된 비트 수
총 비트 수	전송이 시작된 시간부터 모니터 콜렉션 시간까지 이 정책이 사용한 전송된 비트 수

비트율	이 연결에서 허용되는 측정된 비트 수
적합한 비트 수	이 정책의 매개변수 내에 포함되는 전송된 비트 수
최대 패킷 *크기*	정책으로 제어를 받는 최대 허용 패킷 *크기*
최소 정책 단위	토큰 버켓에서 제거할 최소 비트 수 예를 들어 최소 정책 단위가 100비트인 경우 100비트 미만의 패킷은 100비트에서 제거됩니다.
적합한 패킷 수	이 정책의 매개변수에 적합하게 전송된 IP 패킷 수
소스 포트 범위	정책으로 제어를 받는 어플리케이션을 판별하는 소스 포트 범위

통합 서비스(보장) 정책

필드	설명
정책명	이 정책에 지정된 이름.
프로토콜	UDP 또는 TCP
목적지 주소	패킷(이 정책의 제어를 받는) 목적지 지점을 판별하는 주소 범위
평균 토큰 비율 한계	연결 경로에 따라 각 라우터와 서버에 이 정책으로 허용할 수 있는 최대 토큰 비율
토큰 깊이 한계	연결 경로에 따라 각 라우터와 서버에 이 정책으로 허용할 수 있는 최대 토큰 버퍼 *크기*
최고 토큰 비율 한계	연결에서 허용하는 최대 비율
총 패킷 수	모니터 콜렉션이 시작된 시간부터 이 정책을 사용하여 전송된 패킷 수
총 비트 수	전송이 시작된 시간부터 모니터 콜렉션 시간까지 이 정책이 사용한 전송된 비트 수
부적합 비트 수	정책 매개변수를 초과하는 전송된 비트 수
보장 비율	보장 비율(초당 비트 수)
적합한 비트 수	이 정책의 매개변수 내에 포함되는 전송된 비트 수
최대 패킷 *크기*	정책으로 제어를 받는 최대 허용 패킷 *크기*
최소 정책 단위	토큰 버켓에서 제거할 최소 비트 수 예를 들어 최소 정책 단위가 100비트인 경우 100비트 미만의 패킷은 100비트에서 제거됩니다.
적합한 패킷 수	이 정책의 매개변수에 적합하게 전송된 IP 패킷 수
활동 중지 기간	의도된 지연과 실제 지연 사이의 차이(초 단위)
소스 포트 범위	정책으로 제어를 받는 어플리케이션을 판별하는 소스 포트 범위

연결 비율 정책

필드	설명
정책명	이 정책에 지정된 이름
연결 비율	초당 수락된 연결 요구 수
총 요구 수	이 서버에 대한 총 연결 요구 수
수락된 요구	이 서버에 의해 수락된 총 연결 요구 수
드롭(drop)된 요구	이 서버에 의해 드롭(drop)된 총 요구 수

평균 연결 비율 한계	초당 허용 가능한 신규 수락 연결 요구 수
연결 버스트 한계	동시에 수락되는 최대 신규 연결 요구 수
최고 연결 비율 한계	서버가 네트워크로부터 연결을 수락하는 최대 허용 가능 비율
우선순위	QoS Manager에 로드된 각 규칙에 할당된 우선순위
대기행렬 우선순위	청취 대기행렬에 수신되는 연결에 할당되는 우선순위
목적지 포트 범위	서버에서 통신 목적지로 지정된 포트 범위 또는 포트
인터페이스 주소	모니터되는 시스템 인터페이스의 IP 주소
소스 주소 범위	서버로 요구를 송신하는 클라이언트의 IP 주소 범위

서버 요구 - URI 정책

필드	설명
정책명	이 정책에 지정된 이름.
요구율	초당 수신된 요구 수
총 요구 수	목표 서버에서 수신된 총 요구 수
수락된 요구	수락된 총 요구 수
드롭(drop)된 요구	드롭(drop)된 총 요구 수
URI	정책 URI의 ID
평균 요구율 한계	초당 허용 가능한 평균 신규 수락 요구 수
요구 버스트 한계	동시에 수락되는 최대 신규 요구 수
최고 요구 버스트 한계	서버가 네트워크로부터 요구를 수락하는 최대 허용 가능 비율
대기행렬 우선순위	청취 대기행렬에 수신된 연결에 할당된 우선순위
목적지 포트	서버에서 통신 목적지로 지정된 포트
인터페이스 주소	모니터되는 시스템 인터페이스의 IP 주소

QoS 문제 해결

다음 하위 주제에서 QoS 문제점에 대한 문제 해결 방법을 제공합니다.

통신 추적
사용자 서버는 근거리 통신망(LAN) 또는 광역 네트워크(WAN) 인터페이스와 같은 통신 회선에 대한 자료를 수집하기 위해 통신 추적을 제공합니다. 대부분의 사용자들은 추적 자료의 전반적인 내용을 이해하지 못할 것입니다. 그러나 두 지점 간에 실제로 자료 교환이 발생하는지를 판별할 때 추적 항목을 사용할 수 있습니다. 자세한 내용은 TCP/IP 문제 해결 주제의 통신 추적을 참조하십시오.

서버에서 QoS 작동 가능
QoS 서버가 시작되지 않는 경우 맨 처음 CHGTCP 명령을 사용하여 IPQOSENB 값을 검사하십시오. 최초로 정책을 구성한 경우 초기 구성 마법사가 자동으로 서버에서 QoS를 작동 가능하게 해줍니다. 어떤 이유에서건 이 값이 변경된 경우 서버는 시작되지 않습니다. 명령행 인터페이스에서 CHGTCPA IPQOSENB(*YES)를 입력하십시오.

QoS 정책 저널
서비스 품질 기능(QoS)에는 저널링 피처가 들어 있습니다. 서버에 추가, 제거 또는 수정된 IP 정책을 기록하기 위해 저널링을 사용할 수 있습니다. 이를 통해 정책을 디버그하고, 검사하고, 의도한대로 정책이 작동하는지 확인할 수 있습니다.

QoS 정책 기록
서버에서 문제가 발생할 경우 작업 기록부를 분석할 수 있습니다.

서버 트랜잭션 모니터
QoS 문제점을 발견하고 올바르게 정정하기 위한 첫 번째 단계가 바로 QoS 모니터입니다. 이것이 QoS 성능 정보를 기록하며 이를 통해 사용자가 볼 수 있습니다.

TCP 어플리케이션 추적
서버 조치 레벨을 기록할 때 추적 명령을 사용하십시오. 이것은 QoS 정책 문제점을 판별할 경우에도 유용합니다.

QoS 정책 순서화
파일 내의 정책 순서는 서비스 품질의 성공적인 구현을 위해 매우 중요합니다.

QoS 정책 저널

QoS는 저널링 기능을 포함하고 있습니다. 저널링은 정책을 추가, 제거 또는 수정한 시기 등 QoS 정책 조치를 추적할 수 있게 해 줍니다. 저널링을 On으로 설정하면 정책 조치 기록부가 작성됩니다. 이것은 사용자의 예상대로 작동하지 않는 정책을 디버그하고 검사할 때 도움이 됩니다. 예를 들어, 정책을 오전 9:00 - 오후 4:00에 실행하도록 설정합니다. 그리고나서 정책이 실제로 오전 9:00에 추가되고 오후 4:00에 제거되는지 알아보기 위해 저널 기록부를 검사할 수 있습니다.

저널링이 켜지면, 정책이 추가, 제거 또는 수정될 때 저널 항목이 생성됩니다. 이 저널을 사용하여, iSeries 서버에서 일반 파일을 작성할 수 있습니다. 그리고나서 시스템이 어떻게 사용되는지를 판별하기 위해 시스템 저널에 기록된 정보를 사용할 수 있습니다. 이것은 정책의 여러 요소들을 변경하는 것과 관련하여 결정을 내릴 때 유용합니다.

저널에 대한 사용자의 선택사항을 선택할 수 있도록 만드십시오. 저널링은 시스템 자원에 부담이 될 수 있습니다. 저널링을 시작 또는 중단하려면 iSeries Navigator를 사용하십시오. 저널 기록부를 보기 위해서는 반드시 문자 기반의 인터페이스를 사용해야 합니다.

저널링을 시작하거나 중단하려면, 다음을 수행하십시오.

1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
2. **서비스 품질**을 마우스 오른쪽 단추로 누른 후 **구성**을 선택하십시오.
3. **QoS**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
4. 저널링을 켜려면 **저널링 실행**을 선택하십시오.
5. 저널링을 끄려면 **저널링 실행**을 선택 취소하십시오.

주의: 위의 단계를 완료하기 전에 서버가 이미 시작된 경우, 반드시 서버를 중단했다가 다시 시작해야 합니다. 일단 저널링이 켜지면, 그것을 활성화하는 방법에는 두 가지가 있습니다. 서버를 중단했다가 다시 시작하거나 서버 갱신을 수행하는 것입니다. 두 가지 방법 중 하나를 통해 policy.conf 파일을 다시 읽고 저널링 속성을 찾을 수 있습니다.

모니터에서 저널 항목 보기

화면에서 저널 항목을 보려면, 다음을 수행하십시오.

1. iSeries 서버의 명령 프롬트에 다음을 입력하십시오. DSPJRN JRN(QUSRSYS/QQOS) 보려는 저널 항목에서 **옵션 5**를 선택하십시오.

출력 파일에서 저널 항목 보기

저널 항목이 하나의 폴더로 형식화되었는지 알아보려면, QUSRSYS 디렉토리에서 MODEL.OUT을 보십시오. 저널 항목을 출력 파일에 복사하여 Query/400 또는 SQL과 같은 조회 유틸리티를 사용하여 항목을 쉽게 볼 수 있습니다. 또한 출력 파일의 항목을 처리하기 위해 HLL 프로그램을 작성할 수 있습니다.

QoS 저널 항목에 시스템 제공 출력 파일를 복사하려면 다음을 수행하십시오.

1. 시스템 제공 출력 파일 QSYS/QATOQQOS의 복사본을 사용자 라이브러리에 작성합니다. 이것은 CRTDUPOBJ(중복 오브젝트 작성) 명령을 사용하여 수행할 수 있습니다. 다음은 CRTDUPOBJ 명령 예입니다.

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

2. DSPJRN(저널 표시) 명령을 사용하여 QUSRSYS/QQOS 저널의 항목을 이전 단계에 작성된 출력 파일에 복사할 수 있습니다. DSPJRN를 현재 없는 출력 파일로 복사할 경우, 시스템이 파일을 작성하더라도 이 파일이 올바른 필드 설명을 포함하지 않습니다.

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

   b. `DSPF FILE(userlib/userfile)`

QoS 서버 작업 기록

QoS 정책과 관련하여 문제가 발생할 때는 항상 iSeries 서버 작업 기록부를 분석해야 합니다. 작업 기록부에는 오류 메세지 및 QoS에 관련된 기타 정보가 들어 있습니다.

단 하나의 QoS 작업, QTOQSRVR만 QSYSWRK 서브시스템에서 실행됩니다. iSeries Navigator에서 이전 및 현재 QoS 서버 작업 기록부를 볼 수 있습니다.

기록부를 보려면, 다음을 수행하십시오.

1. **네트워크**를 확장하고 **IP 정책**을 클릭하십시오.
2. **서비스 품질**을 마우스 오른쪽 버튼으로 클릭하십시오.
3. **진단 툴 —> QoS 서버 기록부**를 선택하십시오.

작업에 대해 작업할 수 있는 창이 열립니다.

다음 리스트는 작업의 사용 목적에 관한 간단한 설명과 함께 가장 중요한 작업명을 보여줍니다.

QTCP
이 작업은 모든 TCP/IP 인터페이스를 시작하는 기본 작업입니다. 보통 TCP/IP에 대한 기본적인 문제가 발생 때 QTCPIP 작업 기록부를 분석합니다.

QTOQSRVR
이 작업은 QoS 고유의 기록부 정보를 제공하는 기본 QoS 작업입니다. WRKSPLF(작업 스풀 파일) QTCP를 실행하고 QTOQSRVR 기록부를 찾아 보십시오.

작업 스풀 파일에서 오류를 확인하려면 다음 타스크를 수행하십시오.

1. 명령행 인터페이스에서 **WRKSPLF QTCP**를 입력하고 Enter를 누르십시오.
2. 모든 스풀 파일에 대한 작업 창이 표시됩니다. 사용자 자료 열에서 QTOQSRVR을 찾아 QoS 서버와 관련된 오류가 있는지 확인하십시오.
3. 표시하려는 행에서 **옵션 5**를 선택하십시오. 이 내용을 읽고 해당 문제점을 설명하는 메세지 ID를 기록해 두십시오. 예를 들면 TCP920C 등입니다.
4. **F3**을 두 번 눌러 기본 메뉴로 돌아가십시오.
5. 명령행 인터페이스에서 **WRKMSGF**를 입력하고 **Enter**를 누르십시오.
6. 메세지 파일에 대한 작업 화면에서 다음 정보를 입력하고 **Enter**를 누르십시오.
   메세지 파일: QTCPMSG
   라이브러리: *LIBL
7. 메세지 파일에 대한 작업 화면에서 **옵션 5**를 눌러 보려는 메세지 파일을 표시한 후 **Enter**를 누르십시오.
8. 메세지 설명 표시 화면에서 다음 정보를 입력하십시오.
   위치: 위 3번의 메세지 ID를 입력하고 Enter를 누르십시오. 예를 들면 TCP920C입니다.
9. 원하는 메세지 ID에서 **옵션 5**를 선택하고 **Enter**를 누르십시오.
10. 표시할 메세지 세부사항 선택에서 30(위 항목 모두)을 선택하고 **Enter**를 누르십시오.
11. 메세지에 대한 자세한 설명이 표시됩니다.

서버 트랜잭션 모니터

QoS 모니터는 QoS의 계획 단계 및 문제 해결 단계에서 도움이 됩니다.

서버를 지나는 IP 통신량을 분석하기 위해 모니터를 사용할 수 있습니다. 이것은 네트워크에서 혼잡이 발생하는 위치를 판별하는 데 도움이 됩니다. QoS 모니터는 사용자가 네트워크를 지속적으로 모니터할 수 있게 함으로써 필요에 따라 사용자가 정책을 조정할 수 있습니다.

성능 계획 및 유지보수

QoS를 구현함에 있어서 가장 어려운 부분 중 하나는 정책에 어느 정도의 성능 한계를 설정해야 할지를 판별하는 것입니다. 네트워크마다 그 환경이 서로 다르므로 특별한 권장사항이 없습니다. 사용자에게 적합한 값을 판별하기 위해서 업무별로 정책을 시작하기 시작하기 전에 모니터를 사용할 수 있습니다.

현재 네트워크 통신이 작동하는 방식을 알아보려면 미터링을 선택하지 않은 상태에서 차별화된 서비스 정책을 작성해 보십시오. 그리고 이 정책을 작동 가능하게 한 후 모니터를 시작하십시오. 모니터의 결과를 기초로 사용자의 특정 요구에 맞게 정책을 조정할 수 있습니다. 현재의 통신 작동 방식을 식별하는 샘플 모니터 정책을 참조하십시오.

성능 문제 해결

또한 문제를 해결하기 위해 모니터를 사용할 수 있습니다. 모니터 출력을 사용하여, 정책에 지정한 매개변수가 다음에 나오는지 판별할 수 있습니다. 모니터 출력의 예는 QoS 시나리오를 방문하거나 모니터의 모든 모니터 필드를 보십시오.

현재 네트워크 통계 모니터

문제점

마법사에서 성능 한계를 설정하겠느냐는 질문을 받게 됩니다. 이것은 개별 네트워크 요구사항을 기초로 한 것이므로 권장할 수 있는 값이 아닙니다. 이 한계를 설정하려면 현재 네트워크 성능을 이해하고 있어야 합니다. 서비스 품질 정책을 구성하려 하고 있으므로 현재 네트워크 요구사항을 잘 알고 있을 것입니다. 토큰 버켓 비율과 같은 정확한 비율 한계를 결정하려면 서버에서의 통신량을 모두 모니터하여 설정할 비율 한계를 더 잘 결정하고자 할 것입니다.

솔루션

제한사항(최대 값 없음)이 포함되지 않은 매우 광범위한 차별화된 서비스 정책을 작성하고 모든 인터페이스 및 모든 IP 주소에 적용하십시오. QoS 모니터를 사용하여 이 정책에 대한 데이터를 기록하십시오.

1단계: iSeries Navigator에서 QoS 열기

1. iSeries Navigator에서 사용자 서버 —> **네트워크 —> IP 정책**을 확장하십시오.
2. **서비스 품질**을 마우스 오른쪽 단추로 누른 후 **구성**을 선택하십시오.
3. **아웃바운드 대역폭 정책**을 확장하십시오.
4. **DiffServ**를 마우스 오른쪽 단추로 누르고 **신규 정책**을 선택하십시오. 새로운 DiffServ 정책 마법사가 표시됩니다.

2단계: 차별화된 서비스 정책 작성
네트워크로 들어가는 대부분의 통신 자료를 수집하고자 하므로 이 정책의 이름을 **Network**로 지정합니다. 모든 IP 주소, 모든 포트, 모든 로컬 IP 주소 및 모든 시간(해당되는 경우)을 사용하십시오. 마법사에서 다음 설정값을 사용하십시오.

이름 = 네트워크(사용자가 지정한 이름)
클라이언트 = 모든 IP 주소
어플리케이션 = 모든 포트
프로토콜 = 모든 프로토콜
스케줄 = 모든 시간

iSeries Navigator는 사용자 서버에서 작성된 차별화된 서비스 정책을 모두 나열합니다.

3단계: 새로운 서비스 클래스 완료
마법사를 완료하는 동안 홉별 작동, 성능 한계 및 프로파일 외부 통신량 처리를 지정할 것을 요청받습니다. 이것은 서비스 클래스에 정의되어 있습니다. 가능한 한 많은 통신량을 허용할 수 있도록 매우 큰 값을 선택하십시오.

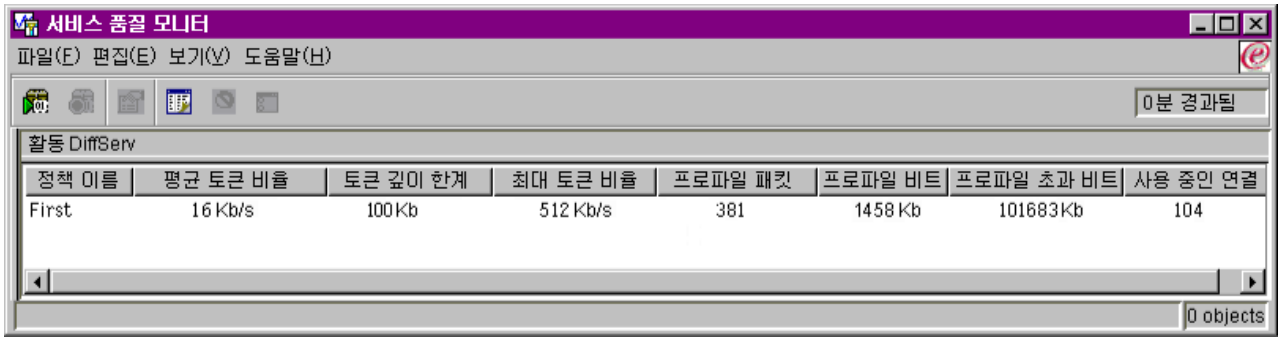
실제로 서비스 클래스가 통신량이 라우터에서 수신되는 성능 레벨을 결정합니다. 이 서비스 클래스의 이름을 **Unlimited**로 하여 통신량이 매우 높은 레벨의 서비스를 수신함을 나타냅니다. iSeries Navigator는 서버에서 정의된 모든 서비스 클래스를 나열합니다.

4단계: 정책 모니터
정책에 사용자가 구성한대로 통신이 작동하는지 검사하려면 모니터를 사용하십시오.

1. 특정 정책 폴더를 선택하십시오(DiffServ, IntServ, 서버 요구 —> URI 또는 연결 비율).
2. 모니터하려는 정책을 마우스 오른쪽 단추로 누르고 **모니터**를 선택하십시오.

다음은 위에서 설정한 정책에 대해 가능한 모니터 출력 리스트입니다.

그림 14. 서비스 품질 모니터



통신량에서 자료를 구할 수 있는 필드를 찾아 보십시오. 총 비트 수, 프로파일 내부 비트 수, 프로파일 내부 패킷 수, 프로파일 외부 비트 수 필드를 반드시 검사하십시오. 프로파일 외부 비트 수는 통신량이 구성된 정책

값을 초과할 때 표시됩니다. 차별화된 서비스 정책에서는 프로파일 외부 수가 드롭된 바이트 수를 나타냅니다. 프로파일 내부 패킷 수는 이 정책에서 제어하는 바이트 수를 나타냅니다(패킷이 시작된 시간에서 현재 모니터 출력 시간까지).

평균 토큰 비율 한계 필드에 지정한 값도 중요합니다. 패킷 수가 이 한계를 초과할 때부터 서버가 드롭을 시작합니다. 그 결과 프로파일 외부 비트 수가 증가합니다. 이것은 사용자가 구성한대로 정책이 작동하는 것을 보여줍니다. 프로파일 외부 비트 수의 양을 변경하려면 성능 한계를 조정해야 합니다. 모든 모니터 필드에 대한 설명은 모니터 절을 참조하십시오.

5단계: 필요에 따라 값 수정
모니터 후에 이전에 선택했던 값을 수정할 수 있습니다. 이 정책에서 작성한 서비스 클래스 이름을 마우스 오른쪽 버튼으로 클릭하십시오. **등록 정보**를 선택하면 CoS 등록 정보 대화 상자가 사용자의 통신을 제어하는 값과 함께 표시됩니다.

6단계: 정책 다시 모니터
결과를 검토한 후 “추측 및 검사” 방법을 사용하여 네트워크가 필요로 하는 최적의 한계를 찾아 내십시오.

TCP 어플리케이션 추적

추적 기능에 대한 작업과 현재 추적 버퍼를 보려면 QoS 추적을 사용하십시오. 서버에서 추적을 실행하려면, TRCTCPAPP를 입력하십시오. 다음은 추적 선택이 완료된 샘플입니다.

```
TCP/IP 어플리케이션......> *QOS
추적 옵션 설정.............> *ON
추적용 최대 기억장치.........> *APP
완전 추적 조치 .............> *WRAP
인수 리스트 ................> 'lvl=4'
QoS 추적 유형 ..............> *ALL
```

다음은 추적에서 사용할 수 있는 매개변수를 소개하는 표입니다. 설정이 문자 기반 엔터페이스에 표시되지 않으면 다음을 명령에 입력해야 합니다. 예를 들면 TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i').

설정	옵션
TCP/IP 어플리케이션	QOS
추적 옵션 설정	*ON, *OFF, *END, *CHK
추적용 최대 기억장치(60 페이지 참조)(MAXSTG)	1-16000, *APP
추적이 가득 참 조치(60 페이지 참조)(TRCFULL)	*WRAP, *STOPTRC
인수 리스트(60 페이지 참조)(ARGLIST)	레벨: ‘lvl=1’, ‘lvl=2’, ‘lvl=3’, ‘lvl=4’ 내용: ‘c=a’, ‘c=i’, ‘c=d’ , ‘c=m’, ‘c=r’, ‘c=s’
QoS 추적 유형	*ALL

추적 출력을 해석하는 데 도움이 필요하다면 추적 출력 읽기를 참조하십시오. 추적 출력 페이지에는 해석에 도움이 되도록 주석이 사용된 출력 샘플이 있습니다.

추적용 최대 기억장치

1-16000
추적 자료에 대한 최대 기억장치 *크기*입니다. 이 *크기*에 도달하면 추적이 중단되거나 랩 처리됩니다. 디폴트 *크기*는 4MB입니다. 디폴트 *크기*를 지정하려면, *APP를 선택하십시오.

***APP**
이것은 디폴트 옵션입니다. 어플리케이션이 디폴트 추적 *크기*를 사용하도록 지시합니다. QoS 서버에 대한 디폴트 추적 서버는 4MB입니다.

완전 추적 조치

***WRAP**
추적이 최대 디스크 *크기*(추적 버퍼 *크기*)에 도달할 때 추적 정보를 랩 처리합니다. 랩핑은 시스템이 파일의 가장 오래된 정보를 겹쳐쓰기로 처리하게 함으로써 계속해서 추적 정보가 기록되도록 합니다. 랩을 선택하지 않으면, 디스크가 가득 찰 때 추적 조작이 중단됩니다.

***STOPTRC**
시스템이 최대 디스크 간격에 도달하면 정보 수집이 중단됩니다.

인수 리스트

기록될 오류 레벨 및 내용을 지정합니다. TRCTCPAPP 명령에 허용되는 인수는 추적 레벨 및 추적 내용의 두 가지가 있습니다. 추적 레벨 및 추적 내용을 지정하는 경우 반드시 모든 속성을 단일 인용 부호 안에 넣어야 합니다. 예를 들면 `TRCTCPAPP 'l=1 c=a'`와 같습니다.

주: 기록 레벨은 포괄적입니다. 이것은 사용자가 기록부 레벨를 선택하면 모든 이전 기록부 레벨도 선택된다는 의미입니다. 예를 들어, 레벨 3을 선택할 경우 레벨 1, 2가 자동으로 포함됩니다.
추적 레벨

레벨 1: 시스템 오류(SYSERR)
시스템 조작 시 발생한 오류를 기록합니다. 이 오류가 발생하면, QoS 서버가 작업을 계속할 수 없습니다. 예를 들어, 시스템 오류는 시스템 메모리 밖에서 실행 중일 때 또는 시스템이 TCP/IP와 통신할 수 없을 때 발생합니다.

레벨 2: 오브젝트 사이의 오류(OBJERR)
QoS 서버 코드에서 발생한 오류를 기록합니다. 예를 들어, 서버 조작이 일부 예상치 않는 결과를 만났을 때 오브젝트 오류가 발생합니다. 일반적으로 서비스에 기록될 수 있는 심각한 조건입니다.

레벨 3: 특정 이벤트(EVENT)
발생된 모든 QoS 조작을 기록합니다. 예를 들어, 이벤트 기록부에 명령이나 요구가 기록됩니다. 결과는 QoS 저널링 기능과 유사합니다.

레벨 4: 추적 메세지(TRACE)
QoS 서버에서 전송된 모든 자료를 추적합니다. 예를 들면, 문제 디버깅에 유용하다고 생각되는 모든 기록부에 대해 상위 레벨 추적을 사용할 수 있습니다. 이 정보는 문제가 발생된 위치와 그 문제를 똑같이 다시 발생시키는 방법을 알아볼 때 유용합니다.

추적 내용

주: 단 하나의 내용 유형만을 지정하십시오. 추적할 내용을 지정하지 않으면 디폴트로 모든 내용이 추적됩니다.

Content = All ('c=a')
QoS 서버의 기능을 모두 추적합니다. 이것이 디폴트 값입니다. 처음에 문제점을 찾아낼 때 이 기능을 사용하십시오.

Content = Intserv ('c=i')
IntServ 조작만 추적합니다. IntServ 관련 문제점을 판별할 때 이 기능을 사용하십시오.

Content = Diffserv ('c=d')
DiffServ 조작만 추적합니다. DiffServ 관련 문제점을 판별할 때 이 기능을 사용하십시오.

Content = Monitor ('c=m')
모니터 조작만 추적합니다.

Content = Rate ('c=r')
인바운드 연결 비율 이벤트를 추적합니다.

Content = Server ('c=s')
모니터 조작을 제외한 모든 것을 추적합니다. 모니터 추적에서 추적 출력을 불필요하게 복잡하게 만드는 정보를 많이 생성하므로 이 기능이 유용할 수 있습니다.

TRCTCPAPP 명령에 대한 자세한 내용은 CL 명령 주제 내의 TRCTCPAPP(TCP/IP 어플리케이션 추적) 명령 설명을 참조하십시오.

추적 출력 읽기

여기에서는 추적 출력을 읽는 방법에 관한 모든 것을 논의하지 않습니다. 단지 추적 정보에서 참조할 수 있는 중요한 이벤트들을 중심으로 설명합니다.

통합 서비스 정책에서 반드시 참조해야 할 가장 중요한 이벤트는 연결에 대한 정책을 찾을 수 없음으로 인해 RSVP 연결 거부가 발생하는지의 여부입니다. 다음은 성공적인 메세지의 예입니다.

```
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]
```

다음은 성공하지 못한 통합 서비스 연결 메세지의 예입니다.

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

차별화된 서비스 정책에서 가장 중요한 메세지는 서버에 정책 규칙이 로드되었는지 또는 정책 구성 파일에서 오류가 발생했는지를 보여주는 메세지입니다.

예:

```
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
```

또한 정책 구성 파일의 태그에 오류가 있음을 나타내는 메세지가 있습니다. 다음은 샘플 메세지입니다.

```
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.
```

주: % 부호는 인식되지 않는 태그를 나타내는 변수입니다.

QoS 관련 정보

업계에는 서비스 품질에 관해 정보를 구할 수 있는 많은 소스가 있습니다. QoS에 대한 일반적인 정보는 최신 RFC, 백서, 레드북(TM) 및 기타 소스를 참조하십시오. 다음은 사용자들이 참조할 수 있는 소스 중 일부를 나열한 것입니다.

IBM 이외의 소스

RFC 1349

이 RFC는 IP 패킷 헤더의 새로운 TOS 필드 정의에 관해 설명합니다.

RFC 2205

이 RFC는 자원 예약 프로토콜(RSVP)에 관해 설명합니다.

RFC 2210

이 RFC는 IETF 통합 서비스와 함께 RSVP를 사용하는 것에 관해 설명합니다.

RFC 2474

이 RFC는 차별화된 서비스 필드(DS 필드) 정의에 관해 설명합니다.

RFC 2475

이 RFC는 차별화된 서비스 구조에 관해 설명합니다.

IBM(R) 레드북

TCP/IP More Cool Things than Ever

이 매뉴얼에서는 구성 예제와 함께 일반적인 솔루션을 보여주는 샘플 시나리오를 제공합니다. 이 매뉴얼의 정보는 iSeries 서버에서 TCP/IP를 계획, 설치, 조정, 구성 및 문제 해결을 수행하는 데 도움이 됩니다. 여기에서는 서비스 품질을 다루지 않지만 LDAP 디렉토리 서버 정보를 간략하게 다루고 있습니다.

TCP/IP Tutorial and Technical Overview

이 매뉴얼은 TCP/IP 프로토콜 및 어플리케이션에 대한 참조로 이에 대한 소개를 제공합니다. 제 22장의 *제 3 부. 고급 개념 및 새로운 기술*에서 서비스 품질에 대한 내용을 찾을 수 있습니다.

관련된 iSeries Information Center 주제

디렉토리 서비스(LDAP)

이 주제에서 디렉토리 서버에 대한 기본 사항, 구성, 관리 및 문제 해결에 대한 내용을 참조하십시오. 디렉토리 서비스 주제에서는 디렉토리 서버 구성을 위한 추가 자원에 대한 설명도 제공합니다.

Printed in U.S.A