

# 서비스 품질 구현

## 목차

### [소개](#)

[어떤 애플리케이션에 QoS가 필요합니까?](#)

[애플리케이션의 특성 이해](#)

[네트워크 토폴로지 파악](#)

[링크 레이어 헤더 크기](#)

[조건을 기반으로 클래스 만들기](#)

[각 클래스를 표시하는 정책 생성](#)

[에지에서 코어로의 작업](#)

[트래픽 처리를 위한 정책 구축](#)

[정책 적용](#)

[QoS 정책 관리자\(QPM\)를 사용하여 정책의 효과 모니터링](#)

[범용 QoS 권장 사항](#)

[관련 정보](#)

## 소개

이 문서에서는 지연에 민감하고 대역폭을 많이 사용하는 애플리케이션을 포함하여 여러 애플리케이션의 전송 역할을 하는 네트워크에서 QoS(Quality of Service)를 구현하기 위한 몇 가지 고급 지침을 제공합니다. 이러한 애플리케이션은 비즈니스 프로세스를 향상시키지만 네트워크 리소스를 늘릴 수 있습니다. QoS는 네트워크에서 지연, 지연 변화(지터), 대역폭 및 패킷 손실을 관리하여 이러한 애플리케이션에 안전하고 예측 가능하고 측정 가능하며 보장된 서비스를 제공할 수 있습니다.

## [어떤 애플리케이션에 QoS가 필요합니까?](#)

먼저 어떤 애플리케이션이 비즈니스에 중요하며 보호가 필요한지 파악합니다. 네트워크 리소스를 위해 경쟁하는 모든 애플리케이션을 검토해야 할 수도 있습니다. 이 경우 Netflow [Accounting](#), [Network-based Application Recognition\(NBAR\)](#) 또는 [QoS Device Manager\(QDM\)](#)를 사용하여 네트워크의 트래픽 패턴을 분석합니다.

NetFlow Accounting은 네트워크 트래픽에 대한 세부 정보를 제공하며 각 흐름과 관련된 트래픽 분류 또는 우선 순위를 캡처하는 데 사용할 수 있습니다.

NBAR는 애플리케이션 레이어까지 트래픽을 식별할 수 있는 분류 툴입니다. 인터페이스를 통과하는 각 트래픽 흐름에 대해 인터페이스별, 프로토콜별 및 양방향 통계를 제공합니다. NBAR는 하위 포트 분류도 수행합니다. 애플리케이션 포트를 넘어 식별하십시오.

QDM은 라우터에서 고급 IP 기반 QoS 기능을 구성 및 모니터링하기 위해 사용하기 쉬운 그래픽 사용자 인터페이스를 제공하는 웹 기반 네트워크 관리 애플리케이션입니다.

## 애플리케이션의 특성 이해

보호가 필요한 애플리케이션의 특성을 이해하는 것이 중요합니다. 일부 애플리케이션은 레이턴시 또는 패킷 손실에 민감한 반면, 다른 애플리케이션은 많은 대역폭을 소모하거나 소비하기 때문에 "공격적"으로 간주됩니다. 응용 프로그램이 버스트된 경우 일정한 버스트 또는 작은 버스트가 있는지 확인합니다. 애플리케이션의 패킷 크기가 크거나 작습니까? 애플리케이션 TCP 또는 UDP가 기반입니까?

특징	지침
지연 또는 손실에 민감한 애플리케이션입니다. (음성 및 실시간 비디오)	WRED(Weighted Random Early Detection), 트래픽 셰이핑, 단편화(FRF-12) 또는 폴리싱을 사용하지 <i>마십시오</i> . 이러한 종류의 트래픽의 경우 LLQ(Low Latency Queuing)를 구현하고 지연에 민감한 트래픽에 우선 순위 큐를 사용해야 합니다.
지속적으로 과부하가 발생하거나 대역폭을 많이 사용하는 애플리케이션입니다.(FTP 및 HTTP)	대역폭을 보장하려면 WRED, 폴리싱, 트래픽 셰이핑 또는 CBWFQ(class-based weighted fair queuing)를 사용합니다.
TCP 기반의 애플리케이션입니다.	손실된 패킷으로 인해 TCP가 꺼진 다음 slow-start 알고리즘을 사용하여 다시 램프되므로 WRED를 사용합니다. 트래픽이 UDP 기반이고 패킷이 삭제될 때 해당 동작이 변경되지 않는 경우 WRED를 사용하지 <i>마십시오</i> . 애플리케이션의 속도를 제한해야 하는 경우 Policing을 사용합니다. 그렇지 않으면 패킷이 tail-drop이 됩니다.

## 네트워크 토폴로지 파악

구현할 QoS 기능을 활용하려면 일부 디바이스에 IOS 업그레이드가 필요할 수 있습니다. 각 디바이스의 네트워크 토폴로지, 라우터 컨피그레이션 및 소프트웨어 버전에 대한 다이어그램은 IOS 업그레이드가 필요한 디바이스 수를 추정하는 데 도움이 됩니다. 네트워크 다이어그램을 만드는 데 도움이 되는 아이콘은 [Cisco Icon Library](#)를 참조하십시오.

- 통화 중 각 라우터의 CPU 사용률을 평가하여 로드를 공유하기 위해 디바이스 간에 QoS 기능을 배포하는 방법을 결정할 수 있습니다.
- 비즈니스 크리티컬 트래픽 유형과 이 트래픽이 통과할 인터페이스를 분류합니다. 네트워크의 QoS 목표를 실현하기 위해 생성할 우선순위 그룹 또는 클래스를 결정합니다.
- 가장 중요한 애플리케이션에서 이 지연을 수용하기 위해 트래픽 에어컨(트래픽 스캐너 또는 폴리서)에서 버스트 매개변수를 처리하고 조정할 수 있는 최대 지연 시간을 결정합니다.
- 각 인터페이스에서 어떤 요금이 지원되는지 알아보십시오. PVC 또는 하위 인터페이스와 일치하는 대역폭을 구성합니다.
- 느린 링크를 식별하여 네트워크의 병목 지점이 있는 위치를 확인하고 적절한 인터페이스에서

링크 효율성 메커니즘을 적용하는 방법을 결정합니다.

- 비즈니스 크리티컬 트래픽을 전송할 각 미디어 유형에 대한 레이어 2 및 레이어 3 오버헤드를 계산합니다.이렇게 하면 각 클래스에 필요한 정확한 대역폭 양을 계산할 수 있습니다.
- 또 다른 핵심 정보는 애플리케이션, IP 소스 및 대상을 기반으로 트래픽을 보호할지 아니면 둘 모두를 기반으로 트래픽을 보호할지 여부입니다.

## 링크 레이어 헤더 크기

미디어 유형	링크 레이어 헤더
이더넷	14바이트
PPP	6바이트
프레임 릴레이	4바이트
ATM	5바이트/셀

## 조건을 기반으로 클래스 만들기

애플리케이션 특성에 따라 QoS가 필요한 애플리케이션과 분류 기준을 결정하면 이 정보를 기반으로 클래스를 만들 수 있습니다.

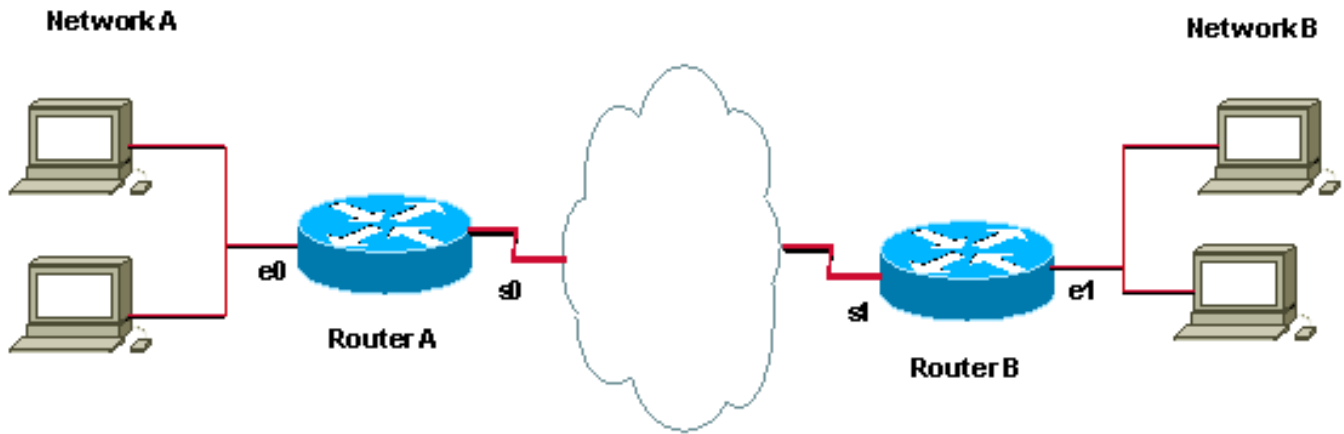
## 각 클래스를 표시하는 정책 생성

각 트래픽 클래스를 적절한 우선순위 값(DSCP(differentiated services control point) 또는 IP Precedence 사용)으로 표시하는 정책을 생성합니다. 트래픽은 인그레스 인터페이스의 라우터로 들어오는 대로 표시됩니다.마킹은 이그레스 인터페이스에서 라우터를 떠나는 트래픽을 처리하는 데 사용됩니다.

## 에지에서 코어로의 작업

트래픽에 가장 가까운 라우터에서 코어로 작업합니다.라우터의 인그레스 인터페이스에 마킹을 적용합니다.아래 토폴로지에서 라우터 A는 트래픽을 표시하고 네트워크 A에서 소싱되고 라우터 B로 향하는 데이터에 대한 정책을 적용하는 명백한 위치입니다.트래픽은 라우터 A의 Ethernet0 인터페이스로 들어오는 대로 표시되며, QoS 정책은 라우터를 떠날 때 라우터 A의 Serial0 인터페이스에 적용됩니다.동일한 정책을 양쪽 방향으로 적용해야 하는 경우(네트워크 B에서 소싱되고 네트워크 A로 향하는 트래픽이 동일한 처리를 받도록), 네트워크 B에서 오는 트래픽은 라우터 B의 이더넷1 인터페이스로 들어오고 라우터를 Serial1 인터페이스에 남겨둔 상태로 처리되어야 합니다.

한 라우터의 인그레스 인터페이스에 트래픽이 표시되면 여러 홉을 통과하는 것과 동일한 표시를 유지합니다(다시 표시되지 않는 한). 일반적으로 트래픽은 한 번만 표시하면 됩니다.이러한 표시를 기반으로 추가 홉에 QoS 정책을 적용할 수 있습니다.신뢰할 수 없는 도메인에서 트래픽이 도착하는 경우에만 다시 표시해야 합니다.



## 트래픽 처리를 위한 정책 구축

이제 트래픽을 표시했으므로 표시를 사용하여 정책을 구축하고 나머지 네트워크 세그먼트에서 트래픽 분류를 수행할 수 있습니다. 4개 이하의 클래스를 사용하여 정책을 단순화하는 것이 좋습니다.

가능하면 랩 환경에서 QoS 구현을 구현하고 테스트합니다. 결과에 만족하면 라이브 네트워크에 구축합니다.

## 정책 적용

적절한 방향으로 정책을 적용합니다. 정책을 한 방향 또는 양방향으로 적용해야 하는지 결정합니다. 이 문서의 [Creating a Policy to Mark Each Class](#) 섹션에 설명된 대로 항상 트래픽을 최대한 소스에 가깝게 표시 및 처리합니다.

사이트의 양쪽에서 들어오고 나갈 트래픽을 필터링하려면 양방향으로 동일한 정책을 적용하는 것이 좋습니다. 즉, Router A의 직렬 인터페이스와 Router B의 직렬 인터페이스에 동일한 정책 아웃바운드를 적용해야 합니다.

## QoS 정책 관리자(QPM)를 사용하여 정책의 효과 모니터링

QPM을 중앙 집중식 정책 제어 및 신뢰할 수 있는 자동화된 정책 구축을 위한 완전한 시스템으로 사용합니다.

## 범용 QoS 권장 사항

다음은 QoS 카테고리의 목록과 각 카테고리과 관련하여 널리 사용되는 QoS 기능 중 일부입니다.

범주	연결된 QoS 기능
QoS 서비스 모델	필요한 경우 프로비저닝됨(Diffserv) QoS(가능한 경우) 또는 신호 전송(RSVP).
분류/표시	Diffserv 코드 포인트 또는 qos-group ID입니다.
혼잡 관리	LLQ 또는 CBWFQ
혼잡 방지	Diffserv 호환 <a href="#">WRED</a> .

링크 효율성	MLPPP, LFI, FRF.11, FRF.12, CRTP
신호	RSVP, QPPB
교통 체증 / 폴리싱	클래스 기반 폴리서 및 GTS(Generic Traffic Shaping) 또는 FRTS(Frame-Relay Traffic Shaping).
구성/모니터링	QPM, 모듈형 QoS CLI(Command Line Interface), QDM

## 관련 정보

- [QoS 지원 페이지](#)
- [IP 라우팅 프로토콜 지원 페이지](#)
- [IP 라우팅 지원 페이지](#)
- [IS-IS 지원 페이지](#)
- [Technical Support - Cisco Systems](#)