Catalyst 6000 제품군 스위치의 QoS 이해

목차

소개

이 문서에서는 Catalyst 6000 제품군 스위치에서 사용할 수 있는 QoS(Quality of Service) 기능에 대해 설명합니다. 이 문서에서는 QoS 컨피그레이션 기능을 다루고 QoS 구현 방법의 몇 가지 예를 제공합니다.

이 문서는 구성 가이드가 아닙니다. 이 백서의 구성 예제는 Catalyst 6000 제품군 하드웨어 및 소프트웨어의 QoS 기능에 대한 설명을 돕기 위해 사용됩니다. QoS 명령 구조에 대한 구문 참조는 Catalyst 6000 제품군에 대한 다음 컨피그레이션 및 명령 가이드를 참조하십시오.

- Catalyst 6500 제품군 스위치

레이어 2 QoS 정의

많은 사람들이 레이어 2(L2) 스위치의 QoS가 단순히 이더넷 프레임의 우선 순위를 정한다고 생각할 수 있지만, 더 많은 것이 필요하다는 것을 아는 사람은 많지 않습니다. L2 QoS에는 다음이 포함됩니다.

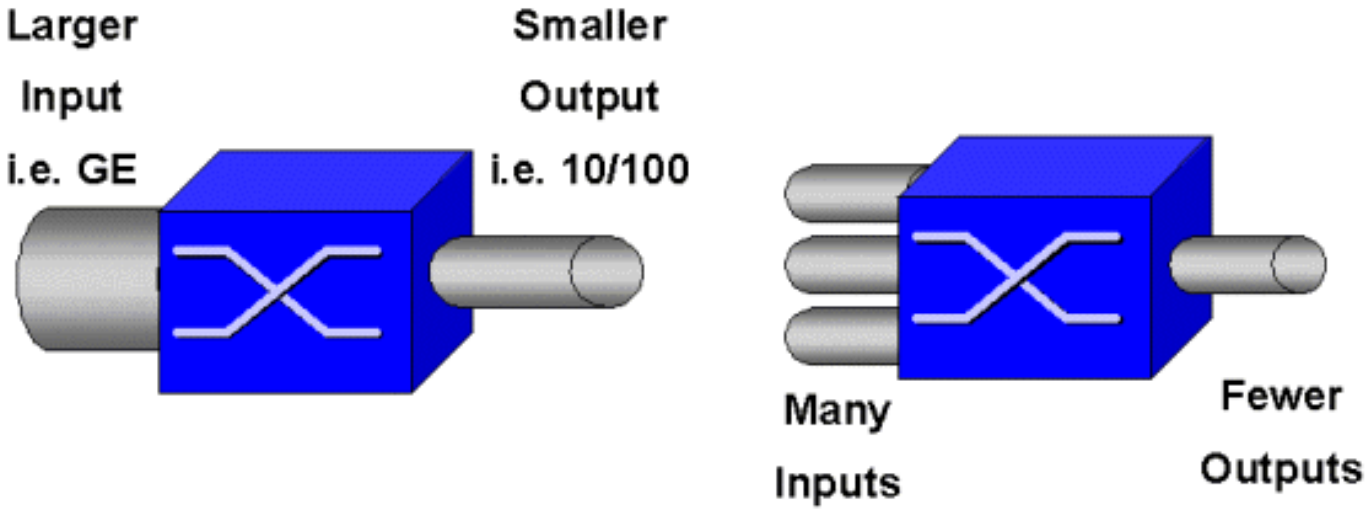
1. **입력 대기열 예약:** 프레임이 포트에 들어가면 이그레스 포트로 전환되도록 예약되기 전에 여러 포트 기반 대기열 중 하나에 할당할 수 있습니다. 일반적으로 서로 다른 트래픽에 서로 다른 서비스 레벨이 필요하거나 스위치 레이턴시를 최소한으로 유지해야 하는 경우 여러 대기열이 사용됩니다. 예를 들어, IP 기반 비디오 및 음성 데이터에는 짧은 레이턴시가 필요하므로 FTP(File Transfer Protocol), 웹, 이메일, 텔넷 등과 같은 다른 데이터를 전환하기 전에 이 데이터를 전환해야 할 수 있습니다.

2. **분류:** 분류 프로세스에는 스위치를 전송할 때 프레임에 적용될 서비스 수준을 결정하는 데 도움이 되도록 이더넷 L2 헤더의 여러 필드(L3(Layer 3) 및 TCP/UDP(Transmission Control Protocol/User Datagram Protocol) 헤더(L4))와 함께 이더넷 L2 헤더의 여러 필드를 검사하는 작업이 포함됩니다.
3. **폴리싱:** 폴리싱은 이더넷 프레임을 검사하여 특정 시간 프레임 내에서 미리 정의된 트래픽 속도를 초과했는지 확인하는 프로세스입니다(일반적으로 이 기간은 스위치의 내부 고정 숫자입니다). 해당 프레임이 프로파일 이외(즉, 미리 정의된 속도 제한을 초과하는 데이터 스트림의 일부)인 경우 삭제되거나 CoS(Class of Service) 값을 아래로 표시할 수 있습니다.
4. **재작성:** 재작성 프로세스는 스위치가 이더넷 헤더의 CoS 또는 IPV4 헤더의 ToS(Type of Service) 비트를 수정하는 기능입니다.
5. **출력 대기열 예약:** 재작성 프로세스 후 스위치는 스위칭을 위한 적절한 아웃바운드(이그레스) 대기열에 이더넷 프레임을 배치합니다. 스위치는 버퍼가 오버플로되지 않도록 하여 이 큐에서 버퍼 관리를 수행합니다. 일반적으로 RED(Random Early Discard) 알고리즘을 사용하여 임의의 프레임을 큐에서 제거(삭제)하는 방식으로 이 작업을 수행합니다. WRED(Weighted RED)는 RED(Catalyst 6000 제품군의 특정 모듈에서 사용)의 파생으로서 CoS 값을 검사하여 삭제할 프레임을 결정합니다. 버퍼가 미리 정의된 임계값에 도달하면 우선 순위가 더 낮은 프레임이 일반적으로 삭제되어 큐의 우선 순위가 더 높은 프레임이 유지됩니다.

이 문서에서는 위의 각 메커니즘과 Catalyst 6000 제품군과 관련된 방법에 대해 자세히 설명합니다.

스위치에서의 QoS 필요성

거대한 백플레인, 초당 수백만 개의 스위치드 패킷, 비차단 스위치는 오늘날 많은 스위치와 동일합니다. QoS가 필요한 이유 정답은 혼잡 때문입니다.



스위치는 세계에서 가장 빠른 스위치일 수 있지만 위의 그림에 나와 있는 두 가지 시나리오 중 하나가 있으면 해당 스위치가 혼잡을 겪게 됩니다. 혼잡 시 혼잡 관리 기능이 없는 경우 패킷이 삭제됩니다. 패킷이 삭제되면 재전송이 발생합니다. 재전송이 발생하면 네트워크 로드가 증가할 수 있습니다. 이미 혼잡해진 네트워크에서는 기존 성능 문제를 가중시키고 성능을 더욱 떨어뜨릴 수 있습니다.

통합 네트워크를 사용하는 경우 혼잡 관리가 더욱 중요합니다. 지연이 발생할 경우 음성 및 비디오와 같은 레이턴시에 민감한 트래픽에 심각한 영향을 미칠 수 있습니다. 단순히 스위치에 버퍼를 추가한다고 해서 혼잡 문제를 해결할 필요는 없습니다. 레이턴시에 민감한 트래픽은 최대한 빨리 전환해야 합니다. 먼저, 분류 기술을 통해 이러한 중요한 트래픽을 식별한 다음, 혼잡 시 우선 순위가

높은 트래픽이 중단되지 않도록 버퍼 관리 기술을 구현해야 합니다. 마지막으로, 가능한 한 빨리 대기열의 중요 패킷을 전환하기 위한 스케줄링 기술을 통합해야 합니다. 이 문서에서 살펴본 바와 같이, Catalyst 6000 제품군은 이러한 모든 기술을 구현하여 QoS 하위 시스템을 현재 업계에서 가장 포괄적인 것으로 만들었습니다.

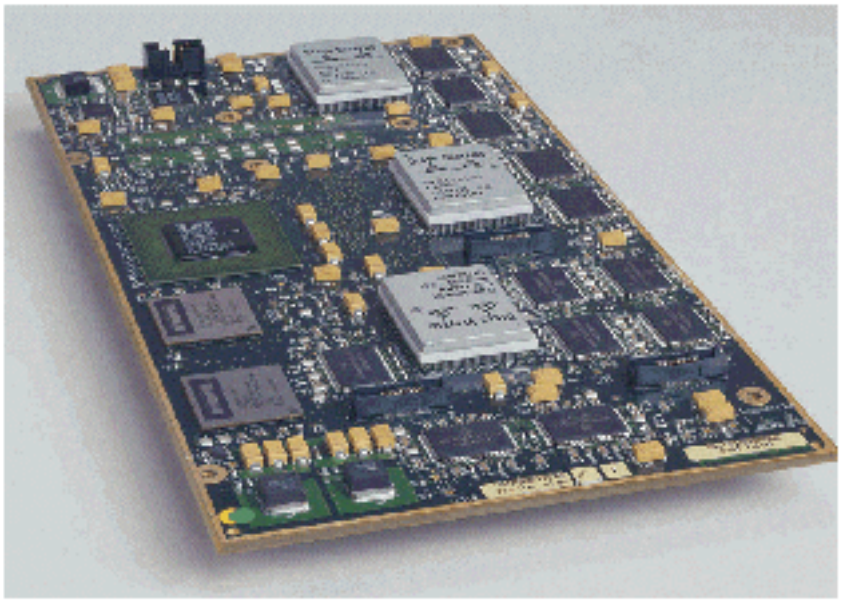
이전 섹션에서 설명한 모든 QoS 기법은 이 문서 전체에서 자세히 살펴봅니다.

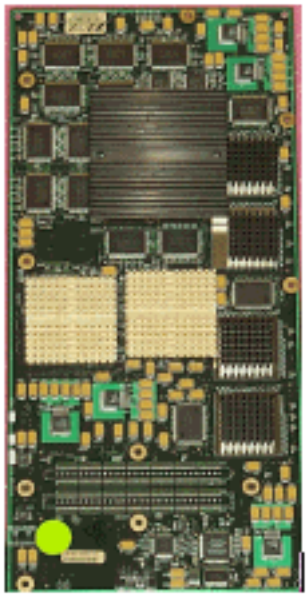
Catalyst 6000 제품군의 QoS에 대한 하드웨어 지원

Catalyst 6000 제품군에서 QoS를 지원하려면 일부 하드웨어 지원이 필요합니다. QoS를 지원하는 하드웨어에는 라인 카드 자체에 MSFC(Multilayer Switch Feature Card), PFC(Policy Feature Card) 및 ASIC(Port Application Specific Integrated Circuits)가 포함됩니다. 이 문서에서는 MSFC의 QoS 기능을 살펴보지 않고 PFC의 QoS 기능과 라인 카드에 있는 ASIC에 집중합니다.

PFC

PFC 버전 1은 Catalyst 6000 제품군의 Supervisor I(SupI) 및 Supervisor IA(SupIA)에 있는 도터 카드입니다. PFC2는 PFC1의 재회전이며 새로운 Supervisor II(SupII) 및 일부 새로운 온보드 ASIC와 함께 제공됩니다. PFC1과 PFC2는 모두 L3 스위칭의 하드웨어 가속화로 주로 알려져 있지만, QoS는 다른 목적 중 하나입니다. PFC는 아래와 같습니다.





PFC 1과 PFC2는 기본적으로 동일하지만 QoS 기능에는 몇 가지 차이점이 있습니다. 즉, PFC2는 다음을 추가합니다.

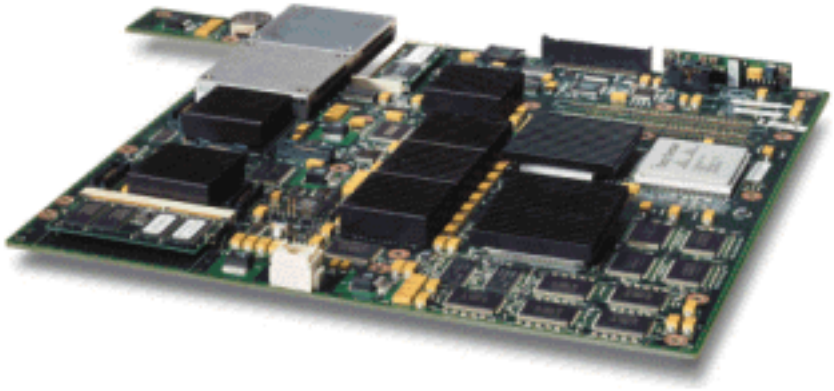
1. QoS 정책을 DFC(Distributed Forwarding Card)로 푸시하는 기능.
2. 폴리싱 결정은 약간 다릅니다. PFC1과 PFC2는 모두 집계 또는 마이크로플로우 정책이 프로파일 밖으로 나온 결정을 반환할 경우 프레임을 삭제하거나 표시하는 정상적인 폴리싱을 지원합니다. 그러나 PFC2는 정책 작업을 수행할 수 있는 두 번째 정책 수준을 나타내는 초과 속도 지원을 추가합니다.

초과 속도 정책이 정의되면 초과 속도를 초과할 때 패킷을 삭제하거나 아래로 표시할 수 있습니다. 초과 경찰 수준을 설정하면 초과 DSCP 매핑을 사용하여 원래 DSCP 값을 표시-다운 값으로 대체합니다. 일반 경찰 레벨만 설정된 경우 일반 DSCP 매핑이 사용됩니다. 두 경찰 레벨이 모두 설정되면 초과 경찰 레벨이 매핑 규칙을 선택하는 우선순위가 됩니다.

앞서 언급한 ASIC에서 수행한 이 문서에 설명된 QoS 기능은 높은 수준의 성능을 제공합니다. 기본 Catalyst 6000 제품군(스위치 패브릭 모듈 없음)에서 QoS 성능을 발휘하면 15MPPS가 생성됩니다. DFC를 사용하는 경우 QoS에 대해 추가적인 성능 향상을 달성할 수 있습니다.

DFC

DFC는 WS-X6516-GBIC에 옵션으로 연결할 수 있습니다. 그러나 WS-X6816-GBIC 카드의 표준 고정장치입니다. 또한 최근에 도입된 패브릭 10/100(WS-X6548-RJ45) 라인 카드, 패브릭 RJ21 라인 카드(WS-X6548-RJ21), 100FX 라인 카드(WS-X6524-MM) 등의 다른 패브릭 라인 카드에서도 지원됩니다. ...을 클릭합니다. DFC는 아래와 같습니다.



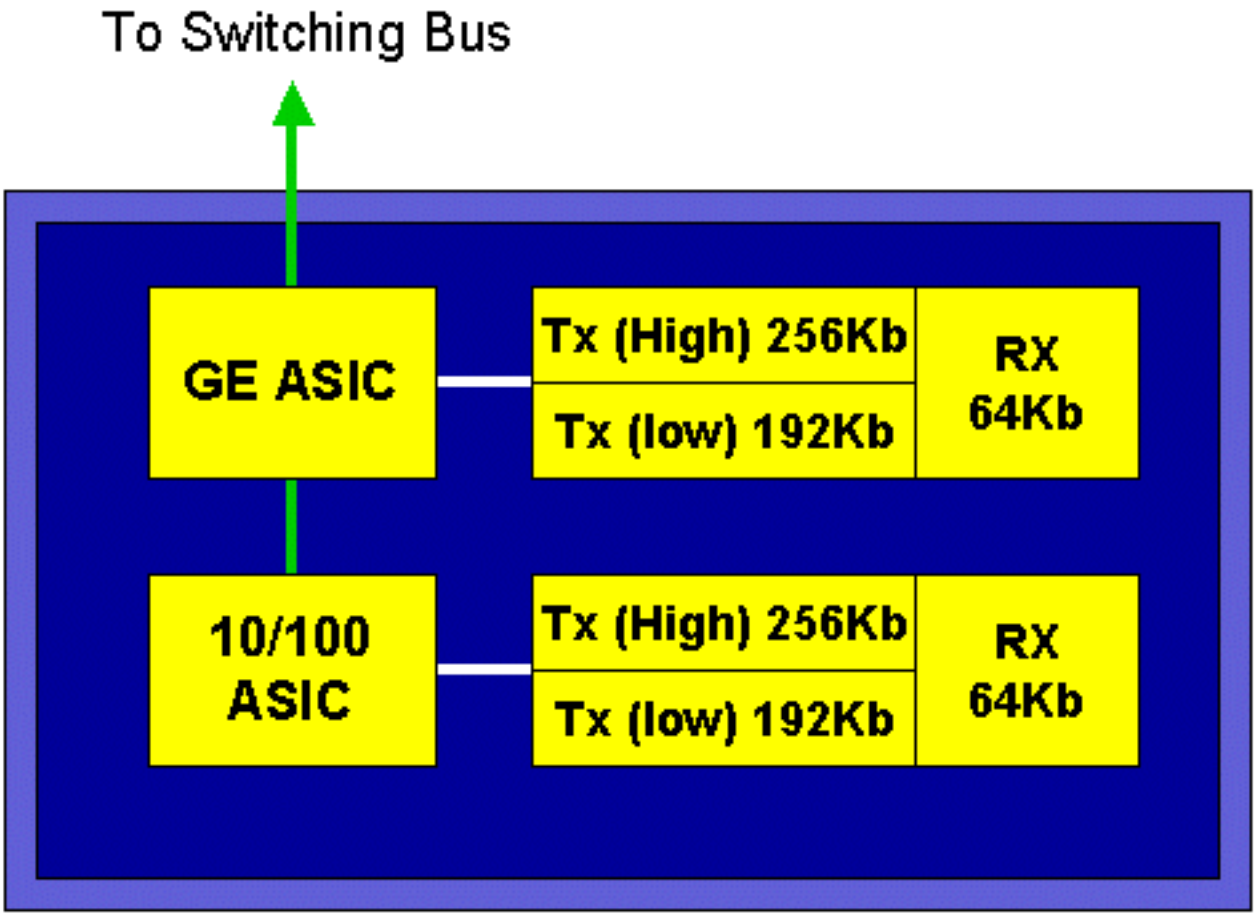
DFC를 사용하면 패브릭(크로스바 연결) 라인 카드가 로컬 스위칭을 수행할 수 있습니다. 이를 위해서는 스위치에 대해 정의된 모든 QoS 정책도 지원해야 합니다. 관리자는 DFC를 직접 구성할 수 없습니다. 즉, 활성 수퍼바이저의 마스터 MSFC/PFC의 제어하에 있습니다. 기본 PFC는 DFC에 L2 및 L3 포워딩 테이블을 제공하는 FIB(Forwarding Information Base) 테이블을 푸시합니다. 또한 QoS 정책의 사본을 푸시하여 라인 카드에도 로컬이 되도록 합니다. 이에 따라, 로컬 스위칭 결정은 하드웨어 QoS 처리 속도를 제공하고 분산 스위칭을 통해 더 높은 수준의 성능을 제공하는 모든 QoS 정책의 로컬 복사본을 참조할 수 있습니다.

포트 기반 ASIC

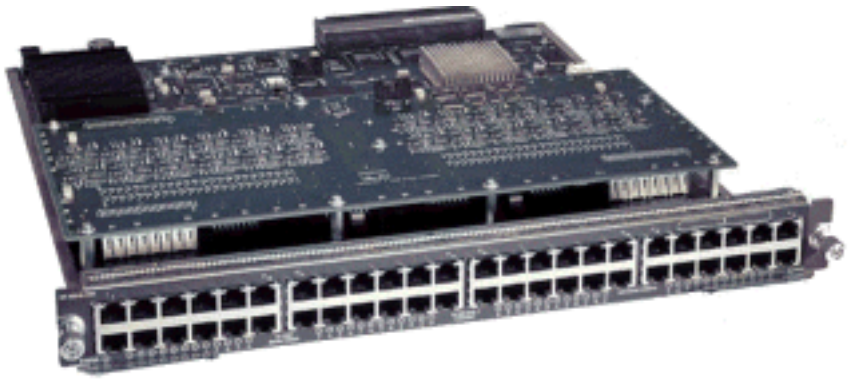
하드웨어 그림을 완성하기 위해 각 라인 카드는 여러 ASIC를 구현합니다. 이러한 ASIC는 스위치를 통과할 때 프레임의 임시 스토리지에 사용되는 대기열, 버퍼링 및 임계값을 구현합니다. 10/100 카드에서는 ASIC의 조합을 사용하여 48개의 10/100 포트를 프로비저닝합니다.

원래 10/100 라인 카드(WS-X6348-RJ45)

10/100 ASIC는 각 10/100 포트에 대해 일련의 Receive(Rx) 및 Transmit(TX) 대기열을 제공합니다. ASIC는 10/100 포트당 128K 버퍼링을 제공합니다. 각 라인 카드에서 포트 버퍼링당 사용 가능한 항목에 대한 자세한 내용은 릴리스 정보를 참조하십시오. 이 라인 카드의 각 포트는 1개의 Rx 큐 및 2개의 TX 대기열을 지원합니다. 아래 다이어그램에 나와 있습니다.



위의 다이어그램에서 각 10/100 ASIC는 12 10/100 포트에 대한 분할 영역을 제공합니다. 각 10/100 포트에 대해 128K 버퍼가 제공됩니다. 128K의 버퍼는 3개의 큐 각각에 분할됩니다. 위 대기열에 표시된 수치는 기본값이 아니지만 구성 가능한 것을 나타내는 것입니다. 단일 Rx 큐는 16K를 가져오고 나머지 메모리(112K)는 두 Tx 큐 간에 분할됩니다. 기본적으로 CatOS에서는 높은 대기열이 이 공간의 20%를 차지하고 낮은 대기열은 80%를 가져옵니다. Catalyst IOS에서 기본값은 높은 대기열 10% 및 낮은 대기열 90%를 제공하는 것입니다.

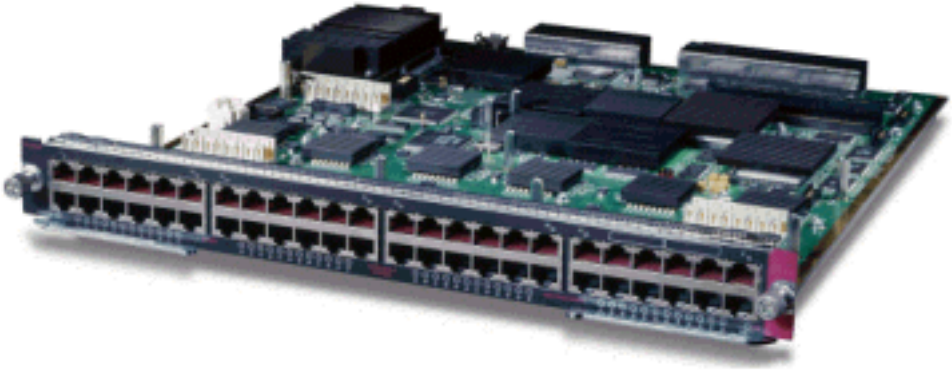


카드는 이중 단계 버퍼링을 제공하지만 QoS 컨피그레이션 중에 10/100 ASIC 기반 버퍼링만 조작할 수 있습니다.

패브릭 10/100 라인 카드(WS-X6548-RJ45)

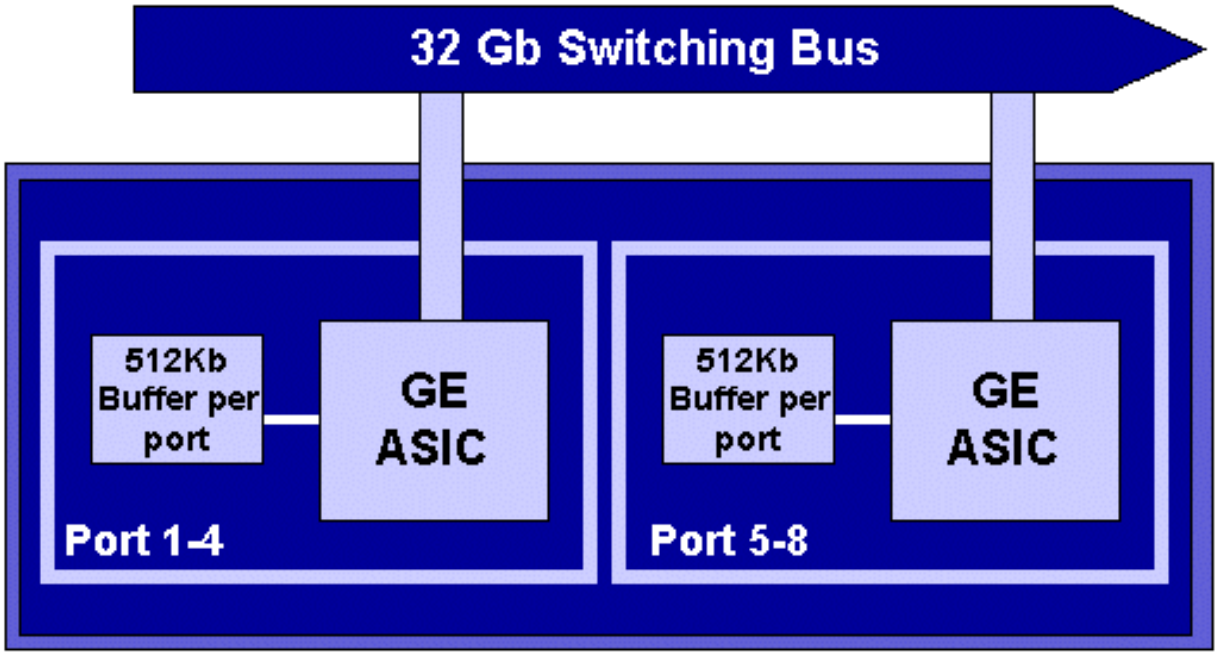
새로운 10/100 ASIC는 각 10/100 포트에 대해 일련의 Rx 및 TX 대기열을 제공합니다. ASIC는 10/100 포트에서 사용 가능한 공유 메모리 풀을 제공합니다. 각 라인 카드에서 포트 버퍼링당 사용 가능한 항목에 대한 자세한 내용은 릴리스 정보를 참조하십시오. 이 라인 카드의 각 포트는 2개의 Rx 대기열과 3개의 TX 대기열을 지원합니다. Rx 큐 1개와 TX 큐 1개는 각각 절대 우선순위 큐로 표시됩니다. 이는 VoIP(Voice over IP) 트래픽과 같은 레이턴시에 민감한 트래픽에 적합한 낮은 레이

턴시 대기열 역할을 합니다.

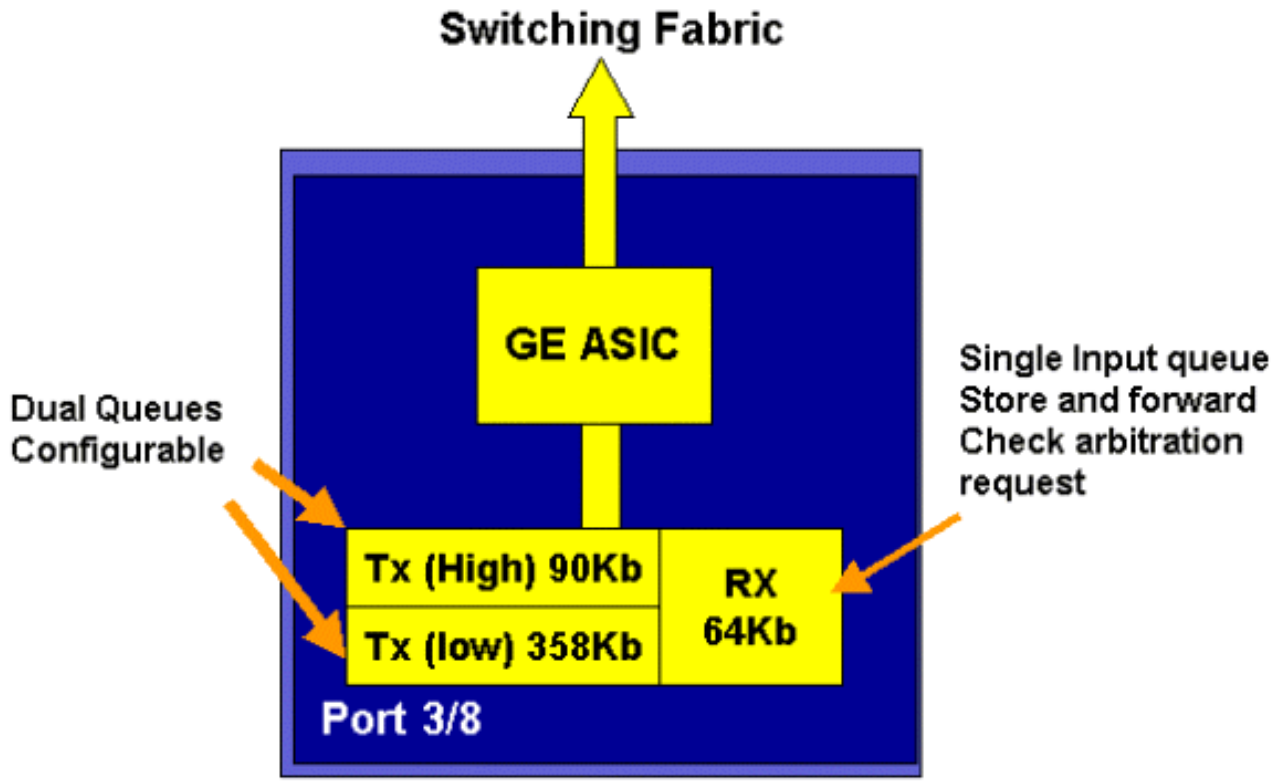


GE 라인 카드(WS-X6408A, WS-X6516, WS-X6816)

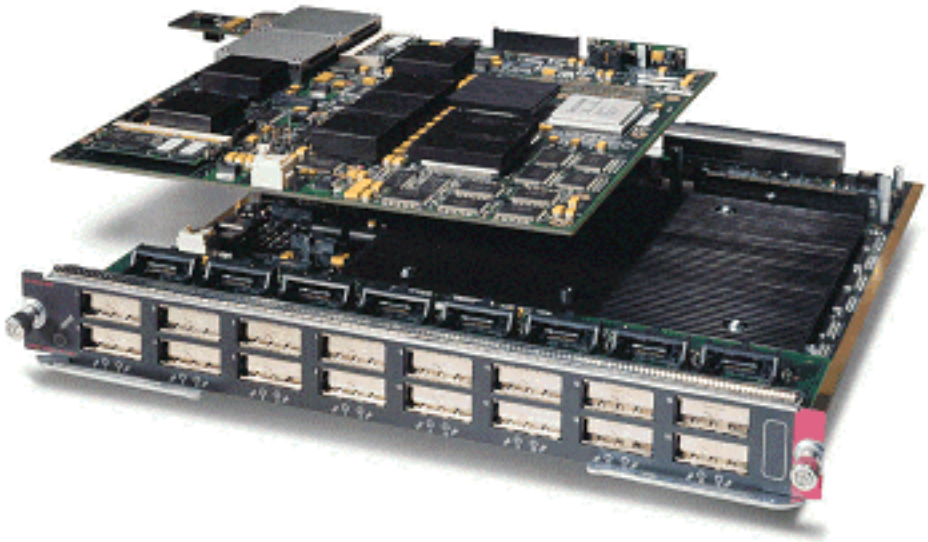
GE 라인 카드의 경우 ASIC는 포트 버퍼링당 512K를 제공합니다. 8포트 GE 라인 카드의 표시가 아래 다이어그램에 나와 있습니다.



10/100 포트와 마찬가지로 각 GE 포트에는 3개의 대기열, 1개의 Rx 및 2개의 TX 대기열이 있습니다. 이것은 WS-X6408-GBIC 라인 카드의 기본값이며 아래 다이어그램에 나와 있습니다.



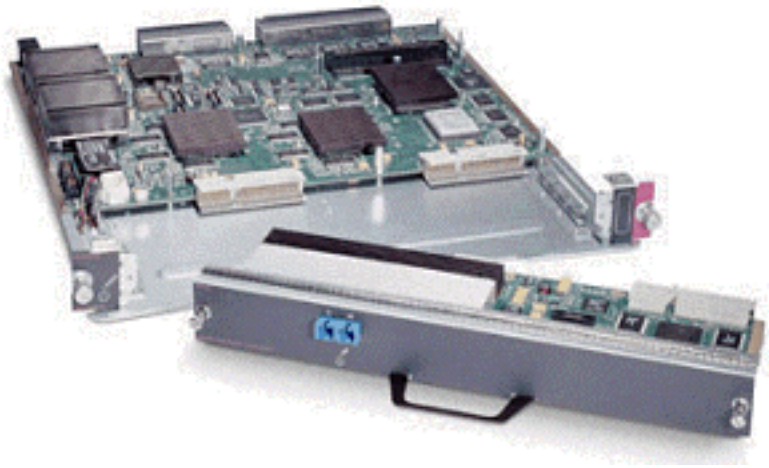
최신 라인 16포트 GE 카드에는 SupIA와 SupII의 GBIC 포트 및 WS-X6408A-GBIC 8 포트 GE 카드에 2개의 추가 SP(Strict Priority) 큐가 제공됩니다. 한 SP 대기열이 Rx 대기열로 할당되고 다른 대기열은 TX 대기열로 할당됩니다. 이 SP 대기열은 주로 음성과 같은 대기 시간에 민감한 트래픽을 대기하는 데 사용됩니다. SP 대기열에서 이 대기열에 있는 모든 데이터는 높은 대기열과 낮은 대기열의 데이터보다 먼저 처리됩니다. SP 대기열이 비어 있는 경우에만 높은 대기열과 낮은 대기열이 처리됩니다.



10GE 라인 카드(WS-X6502-10GE)

2001년 후반기에 Cisco는 라인 카드당 10GE 포트 1개를 제공하는 10GE 라인 카드 세트를 도입했습니다. 이 모듈은 6000 섀시에서 하나의 슬롯을 사용합니다. 10GE 라인 카드는 QoS를 지원합니다. 10GE 포트의 경우 Rx 큐 2개와 TX 큐 3개를 제공합니다. Rx 큐 1개와 TX 큐 1개가 각각 SP 큐로 지정됩니다. 또한 포트에 버퍼링이 제공되어 총 256K의 Rx 버퍼링 및 64MB의 TX 버퍼링을 제공합니다. 이 포트는 Rx 측에 대한 1p1q8t 큐 구조와 TX 측에 대한 1p2q1t 큐 구조를 구현합니다.

대기열 구조는 이 문서의 뒷부분에서 자세히 설명합니다.



Catalyst 6000 제품군 QoS 하드웨어 요약

Catalyst 6000 제품군에서 위 QoS 기능을 수행하는 하드웨어 구성 요소는 아래 표에 자세히 설명되어 있습니다.

QoS Process	Catalyst 6500 Component that performs function
Input Scheduling	Performed by port ASIC's L2 only with or without the PFC
Classification	Performed by Supervisor or PFC L2 only is done by Supervisor L2/3 is done by PFC
Policing	Done by PFC via L3 forwarding Engine
Packet Re-write	Done by port ASIC's L2/L3 based on classification done in point 2 above
Output Scheduling	Done by port ASIC's L2/L3 based on classification done in point 2 above

QoS를 위한 Catalyst 6000 제품군 소프트웨어 지원

Catalyst 6000 제품군은 두 개의 운영 체제를 지원합니다. 원래 소프트웨어 플랫폼인 CatOS는 Catalyst 5000 플랫폼에 사용된 코드 기반에서 파생되었습니다. 더 최근에 Cisco는 Cisco Router IOS에서 파생된 코드 베이스를 사용하는 Integrated Cisco IOS ®(Native Mode)(이전의 Native IOS)를 도입했습니다. 두 OS 플랫폼(CatOS 및 Integrated Cisco IOS(Native Mode) 모두 이전 섹션에서 설명한 하드웨어를 사용하여 Catalyst 6000 스위치 제품군 플랫폼에서 QoS를 활성화하는 소프트웨어 지원을 구현합니다.

참고: 이 문서에서는 두 OS 플랫폼의 컨피그레이션 예를 사용합니다.

IP 및 이더넷의 우선순위 메커니즘

데이터에 QoS 서비스를 적용하려면 IP 패킷 또는 이더넷 프레임에 태그를 지정하거나 우선 순위를 지정하는 방법이 있어야 합니다. ToS 및 CoS 필드를 사용하여 이를 달성할 수 있습니다.

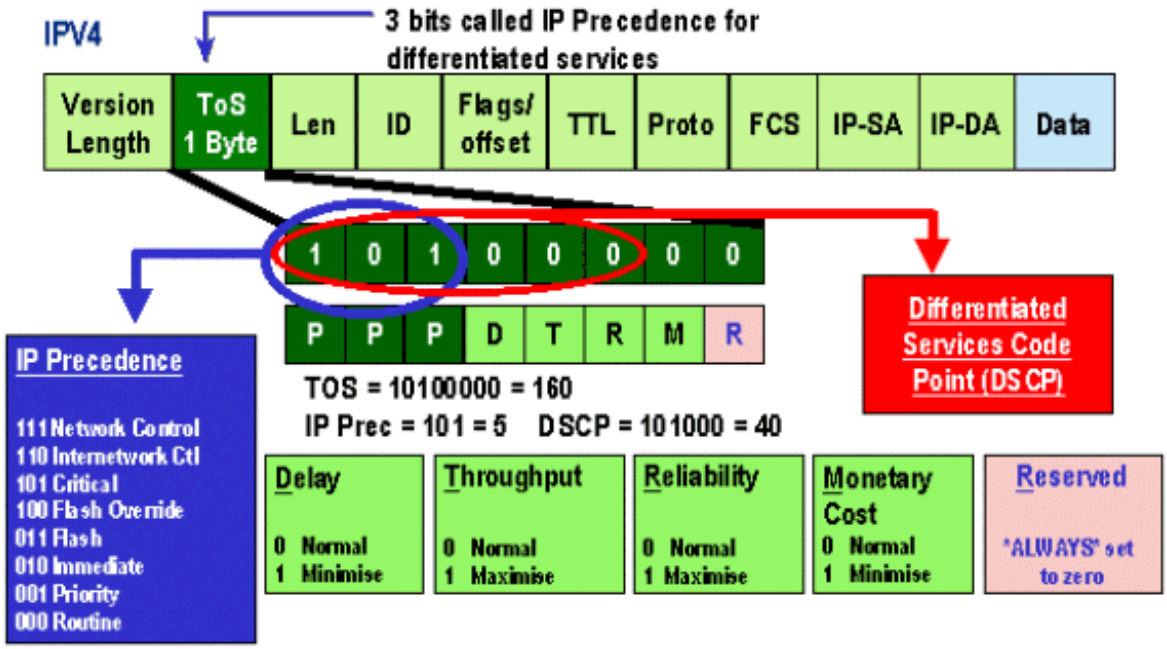
대상

ToS는 IPV4 헤더에 있는 1바이트 필드입니다. ToS 필드는 8비트로 구성되며, 이 중 첫 번째 3비트는 IP 패킷의 우선순위를 나타내는 데 사용됩니다. 이러한 처음 3비트를 IP 우선 순위 비트라고도 합니다. 이러한 비트는 0에서 7로 설정할 수 있으며, 0은 가장 낮은 우선 순위이고 7은 가장 높은 우선 순위입니다. IOS에서 IP 우선 순위를 설정하는 데 수년간 지원을 제공해 왔습니다. IP 우선 순위 재설정은 MSFC 또는 PFC(MSFC에 독립적)에 의해 가능합니다. 신뢰할 수 없는 신뢰 설정은 들어오는 프레임의 IP 우선 순위 설정도 지울 수 있습니다.

IP 우선 순위에 대해 설정할 수 있는 값은 다음과 같습니다.

IP Precedence bits	IP Precedence Value
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

아래 다이어그램은 ToS 헤더에 있는 IP 우선순위 비트를 나타낸 것입니다. 세 MSB(Most Significant Bits)는 IP 우선순위 비트로 해석됩니다.



최근에는 DSCP라고 하는 6개의 MSB를 포함하도록 ToS 필드를 확장했습니다. DSCP는 IP 패킷에 할당할 수 있는 64개의 우선순위 값(2에서 6의 거듭제곱)을 생성합니다.

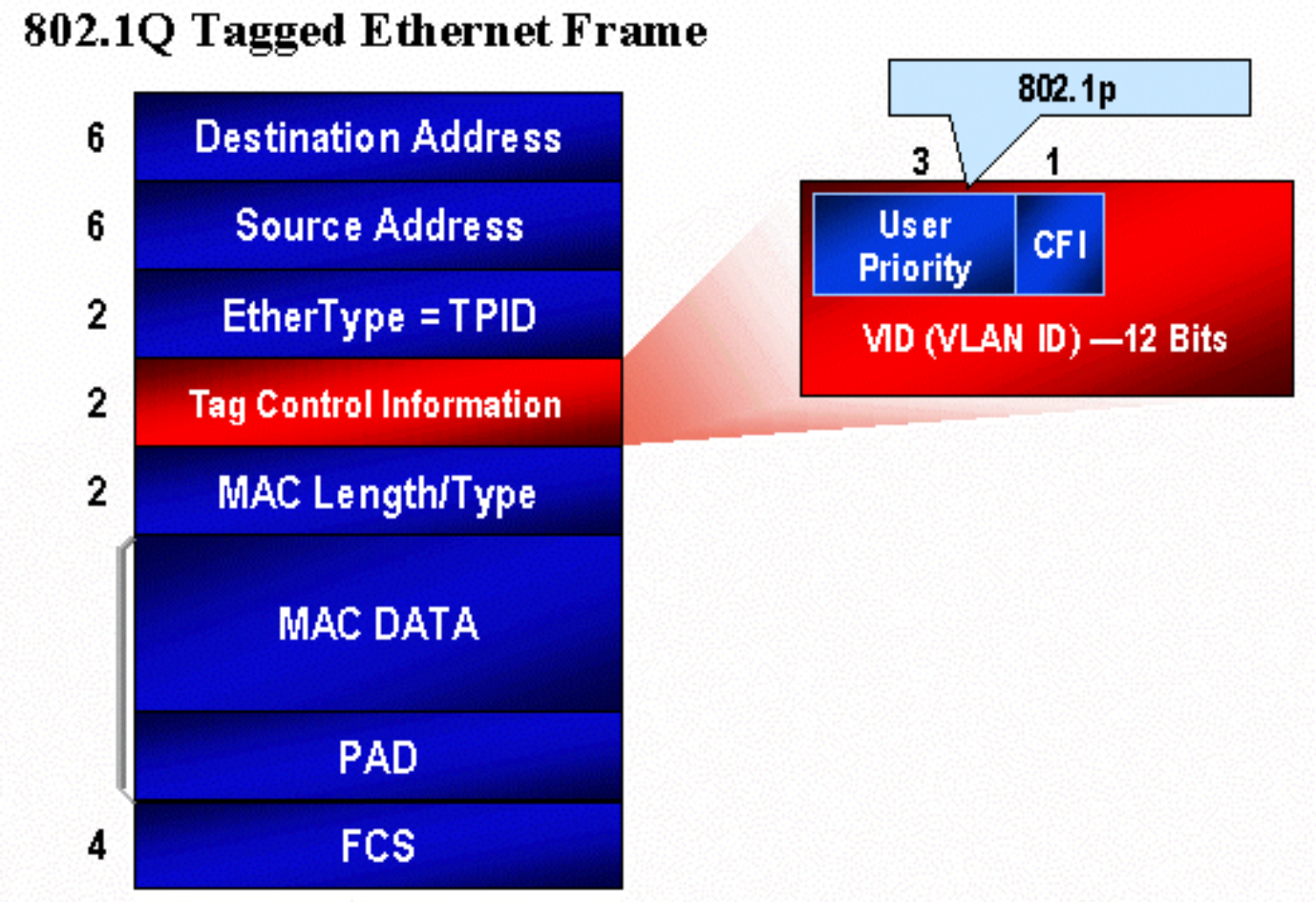
Catalyst 6000 제품군은 ToS를 조작할 수 있습니다. 이는 PFC 및/또는 MSFC를 모두 사용하여 수행할 수 있습니다. 프레임이 스위치에 들어오면 DSCP 값이 할당됩니다. 이 DSCP 값은 관리자가 정의한 서비스 수준(QoS 정책)을 할당하기 위해 스위치 내부에서 사용됩니다. DSCP는 프레임에 이미 있으므로 사용할 수 있으며, 또는 프레임의 기존 CoS, IP 우선 순위 또는 DSCP에서 DSCP를

파생할 수 있습니다(포트를 신뢰할 수 있어야 함). 맵은 DSCP를 파생하기 위해 스위치에서 내부적으로 사용됩니다. 가능한 CoS/IP 우선순위 값 8개와 가능한 DSCP 값 64개를 사용하여 기본 맵은 CoS/IPPrec 0을 DSCP 0, CoS/IPPrec 1을 DSCP 7로, CoS/IPPrec 2를 DSCP 15로 매핑합니다. 이러한 기본 매핑은 관리자가 재정의할 수 있습니다. 프레임을 아웃바운드 포트로 예약하면 CoS를 다시 쓸 수 있으며 DSCP 값을 사용하여 새 CoS를 파생시킬 수 있습니다.

CoS

CoS는 스위치드 네트워크를 통과할 때 이더넷 프레임의 우선순위를 나타내는 데 사용되는 ISL 헤더 또는 802.1Q 헤더의 3비트를 나타냅니다. 이 문서에서는 802.1Q 헤더의 사용만을 참조합니다. 802.1Q 헤더의 CoS 비트는 일반적으로 802.1p 비트라고도 합니다. 당연히 IP 우선 순위에 사용되는 비트 수와 일치하는 3개의 CoS 비트가 있습니다. 많은 네트워크에서 QoS를 엔드 투 엔드 상태로 유지하기 위해 패킷이 L2 및 L3 도메인을 모두 통과할 수 있습니다. QoS를 유지하기 위해 ToS를 CoS에 매핑할 수 있으며 CoS를 ToS에 매핑할 수 있습니다.

아래 다이어그램은 2바이트 Ethertype과 2바이트 태그로 구성된 802.1Q 필드가 포함된 이더넷 프레임입니다. 2바이트 태그 내에 사용자 우선 순위 비트(802.1p라고 함)가 있습니다.

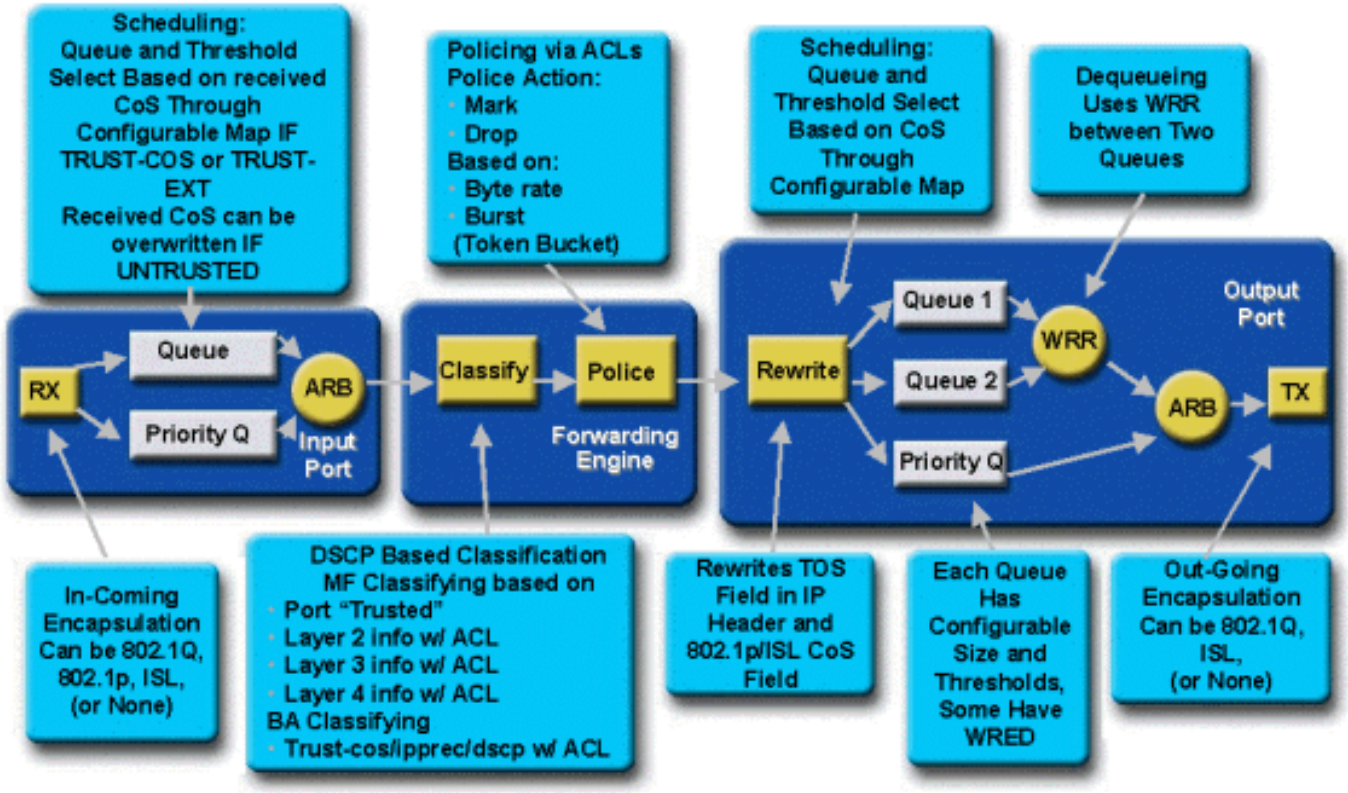


Catalyst 6000 제품군의 QoS 흐름

Catalyst 6000 제품군의 QoS는 현재 모든 Cisco Catalyst 스위치에서 가장 포괄적인 QoS 구현입니다. 다음 섹션에서는 스위치를 전송할 때 다양한 QoS 프로세스가 프레임에 어떻게 적용되는지 설명합니다.

이 문서의 앞부분에서는 많은 L2 및 L3 스위치가 제공할 수 있는 QOS 요소가 많이 있다는 점에 주목했습니다. 이러한 요소는 분류, 입력 대기열 스케줄링, 폴리싱, 재작성 및 출력 대기열 스케줄링입니다. Catalyst 6000 제품군과 차이점은 이러한 QoS 요소는 L3 및 L4 세부 정보 및 L2 헤더 정보에

대한 통찰력을 갖춘 L2 엔진에 의해 적용된다는 점입니다. 다음 다이어그램에는 Catalyst 6000 제품군이 이러한 요소를 구현하는 방법이 요약되어 있습니다.



프레임은 스위치에 진입하여 프레임을 수신한 포트 ASIC에 의해 초기에 처리됩니다. 프레임을 Rx 큐에 넣습니다. Catalyst 6000 제품군 라인 카드에 따라 하나 또는 두 개의 Rx 대기열이 있습니다.

포트 ASIC는 CoS 비트를 프레임을 배치할 대기열의 표시기로 사용합니다(입력 대기열이 여러 개인 경우). 포트가 신뢰할 수 없는 것으로 분류되면 포트 ASIC는 미리 정의된 값을 기반으로 기존 CoS 비트를 덮어쓸 수 있습니다.

그런 다음 L2/L3 포워딩 엔진(PFC)에 프레임이 전달되며, 이 엔진은 프레임을 분류하고 선택적으로 폴리싱합니다(속도 제한). 분류는 프레임을 DSCP 값으로 할당하는 프로세스로, 프레임을 처리하기 위해 스위치에서 내부적으로 사용됩니다. DSCP는 다음 중 하나에서 파생됩니다.

1. 스위치로 들어가는 프레임 이전에 설정된 기존 DSCP 값
2. 수신된 IP 우선순위 비트가 IPV4 헤더에 이미 설정되어 있습니다. 64개의 DSCP 값과 8개의 IP 우선순위 값만 있으므로 관리자는 스위치가 DSCP를 파생시키는 데 사용하는 매핑을 구성합니다. 관리자가 맵을 구성하지 않으면 기본 매핑이 적용됩니다.
3. 받은 CoS 비트가 스위치로 진입하기 전에 이미 설정되었습니다. IP 우선 순위와 마찬가지로 최대 8개의 CoS 값이 있으며 각 값은 64개의 DSCP 값 중 하나에 매핑되어야 합니다. 이 맵을 구성하거나 스위치가 기본 맵을 사용할 수 있습니다.
4. 일반적으로 ACL(Access Control List) 항목을 통해 할당된 DSCP 기본값을 사용하여 프레임에 대해 설정합니다.

프레임에 DSCP 값이 할당된 후 폴리싱 컨피그레이션이 있으면 폴리싱(속도 제한)이 적용됩니다. 폴리싱은 프로파일링되지 않은 트래픽을 삭제 또는 표시하여 PFC를 통한 데이터 흐름을 제한합니다. out-of-profile은 트래픽이 PFC가 전송할 초당 비트 수로 관리자가 정의한 제한을 초과했음을 나타내는 데 사용되는 용어입니다. 프로필 외 트래픽을 삭제하거나 CoS 값을 아래로 표시할 수 있습니다. PFC1 및 PFC2는 현재 입력 폴리싱(속도 제한)만 지원합니다. 새 PFC의 릴리스에서 입력 및 출력 폴리싱을 지원할 수 있습니다.

그런 다음 PFC는 처리를 위해 프레임을 이그레스 포트로 전달합니다. 이 시점에서 프레임의 CoS 값과 IPV4 헤더의 ToS 값을 수정하기 위해 재작성 프로세스가 호출됩니다. 내부 DSCP에서 파생됩니다. 그런 다음 CoS 값을 기반으로 전송 대기열에 프레임을 배치합니다. 전송 준비입니다. 프레임이 대기열에 있는 동안 포트 ASIC는 버퍼를 모니터링하고 버퍼가 폴러딩되지 않도록 WRED를 구현합니다. 그런 다음 이그레스 포트에서 프레임을 예약하고 전송하는 데 WRR 스케줄링 알고리즘을 사용합니다

아래 각 섹션에서는 위에 설명된 각 단계에 대한 컨피그레이션 예를 자세히 살펴봅니다.

대기열, 버퍼, 임계값 및 매핑

QoS 컨피그레이션에 대해 자세히 설명하려면 스위치의 QoS 컨피그레이션 기능을 완전히 이해할 수 있도록 특정 용어를 더 자세히 설명해야 합니다.

대기열

스위치의 각 포트에는 데이터의 임시 저장 영역으로 사용되는 일련의 입력 및 출력 대기열이 있습니다. Catalyst 6000 제품군 라인 카드는 각 포트에 대해 서로 다른 수의 대기열을 구현합니다. 대기열은 일반적으로 각 포트의 하드웨어 ASIC에서 구현됩니다. 1세대 Catalyst 6000 제품군 라인 카드에서 일반적인 컨피그레이션은 입력 큐 하나와 출력 대기열 두 개였습니다. 최신 라인 카드(10/100 및 GE)에서 ASIC는 추가 대기열(1개의 입력과 1개의 출력)을 구현하여 2개의 입력 대기열과 3개의 출력 대기열을 만듭니다. 이 두 개의 추가 대기열은 VoIP와 같은 레이턴시에 민감한 트래픽에 사용되는 특수 SP 대기열입니다. SP 방식으로 제공됩니다. 즉, 프레임이 SP 큐에 도착하면 대기열 하단의 일정 프레임 때문에 SP 큐의 프레임이 처리되지 않습니다. SP 대기열이 비어 있는 경우에만 하위 대기열에서 패킷을 스케줄링합니다.

프레임이 혼잡 시 포트(입력 또는 출력)에 도착하면 대기열에 배치됩니다. 프레임이 배치되는 대기열의 결정 과정은 일반적으로 수신 프레임의 이더넷 헤더에 있는 CoS 값을 기준으로 수행됩니다.

이그레스 시 TX(출력) 대기열을 비우는 일정 알고리즘이 사용됩니다. WRR은 이를 달성하기 위해 사용되는 기술입니다. 각 대기열에 대해 가중치를 사용하여 다음 대기열로 이동하기 전에 대기열에서 비울 데이터의 양을 지정합니다. 관리자가 할당한 가중치는 1에서 255 사이의 숫자이며 각 TX 대기열에 할당됩니다.

버퍼

각 대기열에는 전송 데이터를 저장할 특정 양의 버퍼 공간이 할당됩니다. 포트 ASIC에 상주하는 메모리는 포트 단위로 분할되어 할당됩니다. 각 GE 포트에 대해 GE ASIC는 512K의 버퍼 공간을 할당합니다. 10/100 포트의 경우 포트 ASIC는 포트 버퍼링당 64K 또는 128K(라인 카드에 따라 다름)를 예약합니다. 그런 다음 이 버퍼 공간은 Rx(인그레스) 큐와 TX(이그레스) 큐 사이에서 분할됩니다.

임계값

일반 데이터 전송의 한 가지 측면은 패킷이 삭제되면 해당 패킷이 재전송된다는 것입니다(TCP 흐름). 혼잡 시 네트워크 부하가 가중될 수 있으며 잠재적으로 버퍼에 과부하가 더 발생할 수 있습니다. Catalyst 6000 제품군 스위치는 버퍼가 오버플로되지 않도록 하기 위해 다양한 기술을 사용합니다.

임계값은 혼잡 관리 알고리즘이 대기열에서 데이터를 삭제하기 시작할 수 있는 활용률을 정의하는 스위치(또는 관리자)가 지정하는 가상 레벨입니다. Catalyst 6000 제품군 포트에는 일반적으로 입력 대기열과 연결된 4개의 임계값이 있습니다. 출력 대기열과 관련된 임계값은 일반적으로 두 가지입니다.

이러한 임계값은 QoS 맥락에서 이러한 임계값에 다른 우선 순위를 가진 프레임을 할당하는 방법으로 구축됩니다. 버퍼가 채워지고 임계값이 위반되기 시작하면 관리자는 임계값이 초과될 때 어떤 프레임을 삭제할지 나타내는 다른 우선 순위를 다른 임계값에 매핑할 수 있습니다.

매핑

위의 대기열 및 임계값 섹션에서는 이더넷 프레임의 CoS 값을 사용하여 프레임을 넣을 대기열을 결정하고 버퍼 가득 찬 시점에는 삭제할 수 있는 프레임을 결정할 수 있다고 언급했습니다. 이는 매핑의 목적입니다.

Catalyst 6000 제품군에 QoS가 구성된 경우 다음을 정의하는 기본 매핑이 활성화됩니다.

- 특정 CoS 값이 있는 임계값 프레임을 삭제할 수 있는 대상
- CoS 값에 따라 프레임이 배치되는 대기열

기본 매핑이 존재하는 동안 관리자가 이러한 기본 매핑을 재정의할 수 있습니다. 다음에 대한 매핑이 있습니다.

- DSCP 값으로 들어오는 프레임의 CoS 값
- DSCP 값에 대한 수신 프레임의 IP 우선순위 값
- 나가는 프레임에 대한 CoS 값에 대한 DSCP 값
- 수신 대기열에서 임계값을 삭제할 CoS 값
- 전송 대기열에서 임계값을 삭제할 CoS 값
- 폴리싱 문을 초과하는 프레임에 대한 DSCP 마크업 값
- 특정 대상 MAC 주소가 있는 프레임에 대한 CoS 값

WRED 및 WRR

WRED와 WRR은 Catalyst 6000 제품군에 상주하는 두 가지 매우 강력한 알고리즘입니다. WRED와 WRR 모두 이더넷 프레임 내에서 CoS(priority tag)를 사용하여 향상된 버퍼 관리 및 아웃바운드 예약을 제공합니다. B

WRED

WRED는 Catalyst 6000 제품군에 의해 사용되는 버퍼 관리 알고리즘으로, 혼잡 시 우선 순위가 높은 트래픽 삭제의 영향을 최소화합니다. WRED는 RED 알고리즘을 기반으로 합니다.

RED 및 WRED를 이해하려면 TCP 흐름 관리 개념을 다시 살펴봅니다. 플로우 관리를 통해 TCP 발신자가 네트워크를 압도하지 않습니다. TCP 느린 시작 알고리즘은 이를 해결하기 위한 솔루션의 일부입니다. 플로우가 시작될 때 단일 패킷이 승인 대기 전에 전송되도록 지시합니다. 그런 다음 ACK가 수신되기 전에 두 개의 패킷이 전송되므로 각 ACK가 수신되기 전에 전송되는 패킷 수가 점진적으로 증가합니다. 이 작업은 플로우가 부하를 유발하지 않고 네트워크에서 처리할 수 있는 전송 수준(즉 패킷 수 *x*개)에 도달할 때까지 계속됩니다. 혼잡이 발생하면 느린 시작 알고리즘은 윈도우 크기(즉, 승인을 대기하기 전에 전송된 패킷 수)를 조절하여 해당 TCP 세션(플로우)의 전반적인 성능을 줄입니다.

RED는 대기열 채우기가 시작될 때 대기열을 모니터링합니다. 특정 임계값을 초과하면 패킷이 무작위로 삭제되기 시작합니다. 특정 플로우에 대해서는 아무런 관심도 없습니다. 대신 임의의 패킷이 삭제됩니다. 이러한 패킷은 우선 순위가 높거나 낮은 흐름에서 발생할 수 있습니다. 삭제된 패킷은 단일 흐름 또는 여러 TCP 플로우의 일부가 될 수 있습니다. 위에서 설명한 것처럼 여러 플로우가 영

향을 받는 경우, 이는 각 플로우 윈도우 크기에 상당한 영향을 미칠 수 있습니다.

RED와 달리 WRED는 프레임을 삭제할 때 무작위가 아닙니다. WRED는 프레임의 우선 순위를 고려합니다(Catalyst 6000 제품군 케이스에서는 CoS 값을 사용합니다). 관리자는 WRED를 사용하여 특정 CoS 값이 있는 프레임을 특정 임계값에 할당합니다. 이러한 임계값이 초과되면 이러한 임계값에 매핑된 CoS 값이 있는 프레임을 삭제할 수 있습니다. 더 높은 임계값에 할당된 CoS 값이 있는 다른 프레임은 대기열에 유지됩니다. 이 프로세스에서는 우선 순위가 높은 플로우를 그대로 유지하여 더 큰 윈도우 크기를 그대로 유지하고 발신자에서 수신자로 패킷을 가져오는 데 소요되는 지연 시간을 최소화할 수 있습니다.

라인 카드가 WRED를 지원하는지 어떻게 알 수 있습니까? 다음 명령을 실행합니다. 출력에서 해당 포트에서 WRED 지원을 나타내는 섹션을 확인합니다.

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        40% 100%
2        40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ----------------
--------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ---------------------------------- 1 100 2 255 Console> (enable)
```

포트에서 WRED를 사용할 수 없는 경우 포트는 버퍼 관리의 tail drop 방법을 사용합니다. 테일 드롭은 이름에서 알 수 있듯이 버퍼가 완전히 활용되면 수신 프레임을 삭제합니다.

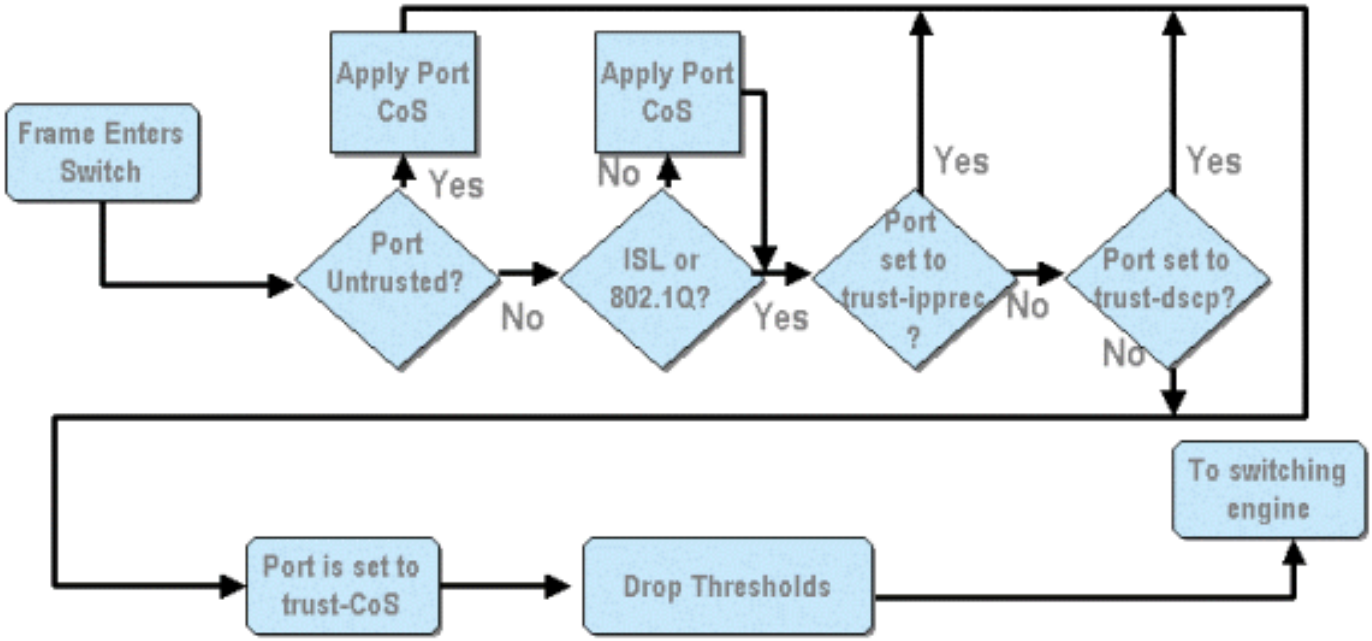
경고

WRR은 TX 큐에서 이그레스 트래픽을 예약하는 데 사용됩니다. 일반 라운드 로빈 알고리즘은 다음 대기열로 이동하기 전에 각 대기열에서 동일한 수의 패킷을 전송하는 TX 대기열 간에 대체 됩니다. WRR의 가중치 적용 측면을 사용하면 스케줄링 알고리즘이 대기열에 할당된 가중치를 검사할 수 있습니다. 이렇게 하면 정의된 대기열에 더 많은 대역폭에 액세스할 수 있습니다. WRR 스케줄링 알고리즘은 식별된 대기열에서 다른 대기열보다 더 많은 데이터를 비우기 때문에 지정된 대기열에 대한 편차를 제공합니다.

WRR의 구성과 위에서 설명한 내용의 기타 부분은 다음 섹션에서 설명합니다.

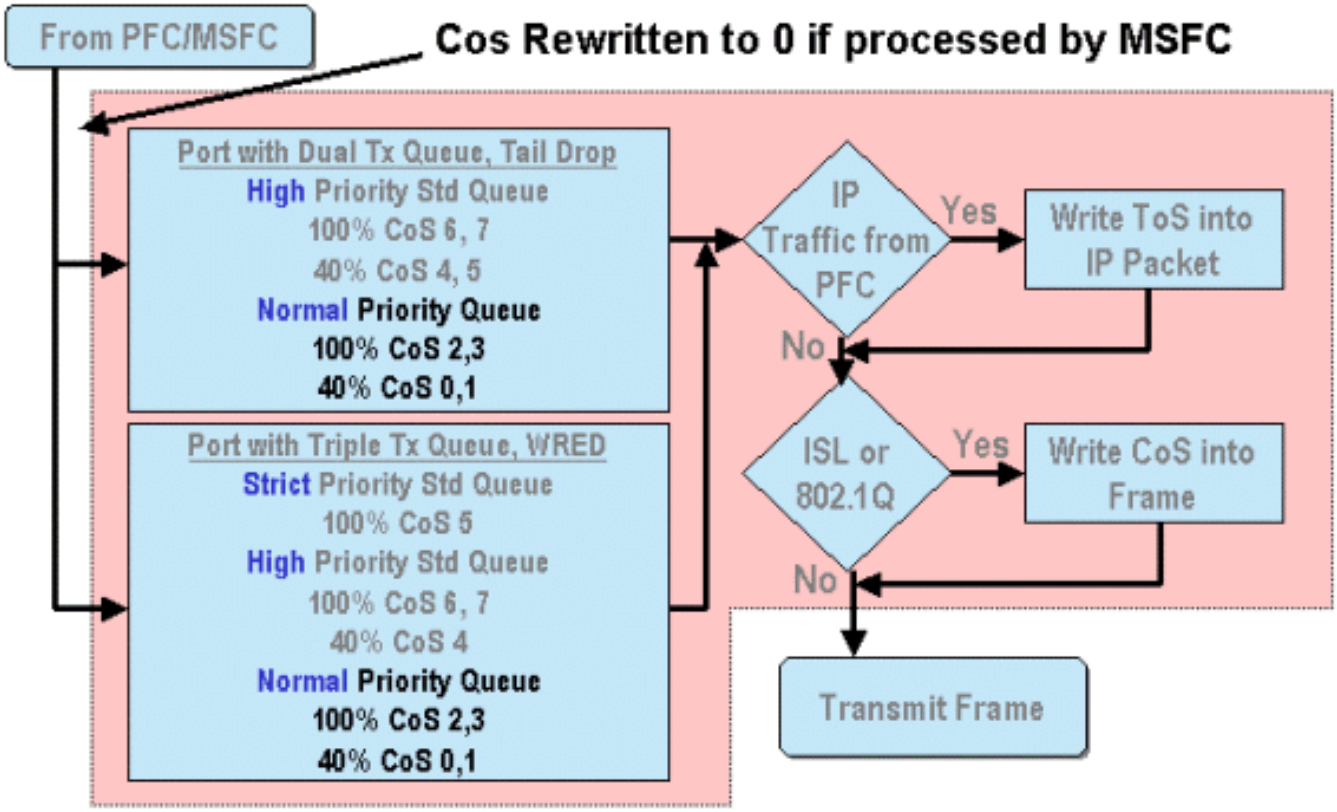
Catalyst 6000 제품군에서 포트 ASIC 기반 QoS 구성

QoS 컨피그레이션은 포트 ASIC 또는 PFC에 QoS 작업을 수행하도록 지시합니다. 다음 섹션에서는 이 두 프로세스에 대한 QoS 컨피그레이션을 살펴봅니다. 포트 ASIC에서 QoS 컨피그레이션은 인바운드 및 아웃바운드 트래픽 흐름에 모두 영향을 미칩니다.



위 다이어그램에서 다음 QoS 컨피그레이션 프로세스가 적용되는 것을 확인할 수 있습니다.

1. 포트의 신뢰 상태
2. 포트 기반 CoS 적용
3. Rx 삭제 임계값 할당
4. CoS-Rx 삭제 임계값 맵



MSFC 또는 PFC에서 프레임을 처리하면 추가 처리를 위해 아웃바운드 포트 ASIC에 전달됩니다. MSFC에서 처리되는 모든 프레임에는 CoS 값이 0으로 재설정됩니다. 아웃바운드 포트에서 QoS 처리를 고려해야 합니다.

위 다이어그램은 아웃바운드 트래픽에 대해 포트 ASIC에서 수행한 QoS 처리를 보여줍니다. 아웃바운드 QoS 처리에서 호출되는 프로세스 중 일부는 다음과 같습니다.

1. TX tail drop 및 WRED 임계값 할당

2. CoS-TX 테일 드롭 및 WRED 맵

또한 위의 다이어그램에는 표시되지 않지만 DSCP를 CoS 맵에 사용하여 아웃바운드 프레임에 CoS를 재할당하는 프로세스입니다.

다음 섹션에서는 포트 기반 ASIC의 QoS 컨피그레이션 기능을 자세히 살펴봅니다.

참고: 중요한 점은 CatOS를 사용하여 QoS 명령을 호출하면 일반적으로 지정된 대기열 유형의 모든 포트에 적용됩니다. 예를 들어 WRED 삭제 임계값이 대기열 유형이 1p2q2t인 포트에 적용된 경우 이 WRED 삭제 임계값은 이 대기열 유형을 지원하는 모든 라인 카드의 모든 포트에 적용됩니다. Cat IOS에서는 일반적으로 QoS 명령이 인터페이스 레벨에서 적용됩니다.

QoS 활성화

Catalyst 6000 제품군에서 QOS 컨피그레이션을 수행하려면 먼저 스위치에서 QoS를 활성화해야 합니다. 이는 다음 명령을 실행하여 달성할 수 있습니다.

CatOS

```
Console> (enable) set qos enable
```

```
!-- QoS is enabled. Console> (enable)
```

통합 Cisco IOS(기본 모드)

```
Cat6500(config)# mls qos
```

Catalyst 6000 제품군에서 QoS가 활성화되면 스위치에서 스위치에 대한 일련의 QoS 기본값을 설정합니다. 이러한 기본값에는 다음 설정이 포함됩니다.

QoS Feature	Default setting
Trust state of each port	Un-trusted
Receive Queue drop threshold percentages	Threshold 1 – 50% Threshold 2 – 60% Threshold 3 – 80% Threshold 4 – 100%
Transmit Queue drop threshold percentages	Low priority queue threshold 1 – 80% Low priority queue threshold 2 – 100% High priority queue threshold 1 – 80% High priority queue threshold 2 – 100%
CoS value to Drop threshold mapping	Receive queue 1/drop threshold 1: CoS 0 and 1 Transmit queue 1/drop threshold 1: CoS 0 and 1 Receive queue 1/drop threshold 2: CoS 2 and 3 Transmit queue 1/drop threshold 2: CoS 2 and 3 Receive queue 1/drop threshold 3: CoS 4 and 5 Transmit queue 2/drop threshold 1: CoS 4 and 5 Receive queue 1/drop threshold 4: CoS 6 and 7

	Transmit queue 2/drop threshold 2: CoS 6 and 7
CoS to DSCP Mapping (DSCP set from CoS value)	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP Precedence to DSCP Map (DSCP set from IP Precedence value)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to CoS map (CoS set from DSCP values)	DSCP 0-7 = CoS 0 DSCP 8-15 = CoS 1 DSCP 16-23 = CoS 2 DSCP 24-31 = CoS 3 DSCP 32-39 = CoS 4 DSCP 40-47 = CoS 5 DSCP 48-55 = CoS 6 DSCP 56-63 = CoS 7

신뢰할 수 있는 포트 및 신뢰할 수 없는 포트

Catalyst 6000 제품군의 특정 포트는 신뢰할 수 있거나 신뢰할 수 없는 포트로 구성할 수 있습니다. 포트의 신뢰 상태는 스위치를 전송할 때 프레임을 표시, 분류 및 스케줄링하는 방법을 결정합니다. 기본적으로 모든 포트는 신뢰할 수 없는 상태입니다.

신뢰할 수 없는 포트(포트의 기본 설정)

포트를 신뢰할 수 없는 포트로 구성할 경우, 처음에 포트에 들어갈 때 프레임에는 포트 ASIC에 의해 CoS 및 ToS 값이 0으로 재설정됩니다. 즉, 프레임에는 스위치를 통해 해당 경로에서 우선 순위가 가장 낮은 서비스가 제공됩니다.

또는 관리자는 신뢰할 수 없는 포트를 입력한 이더넷 프레임의 CoS 값을 미리 결정된 값으로 재설정할 수 있습니다. 이 구성 방법은 이후 섹션에서 설명합니다.

포트를 신뢰할 수 없는 상태로 설정하면 스위치에서 혼잡 방지를 수행하지 않도록 지시합니다. 혼잡 방지란 CoS 값이 해당 대기열에 대해 정의된 임계값을 초과하면 해당 CoS 값을 기반으로 프레임을 삭제하는 데 사용되는 방법입니다. 이 포트에 들어가는 모든 프레임은 버퍼가 100%에 도달하면 모두 삭제될 수 있습니다.

CatOS에서 다음 명령을 실행하여 10/100 또는 GE 포트를 신뢰할 수 없는 것으로 구성할 수 있습니다.

CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

이 명령은 모듈 3의 포트 16을 신뢰할 수 없는 상태로 설정합니다.

참고: 통합 Cisco IOS(기본 모드)의 경우 소프트웨어는 현재 GE 포트에 대한 신뢰 설정만 지원합니다.

통합 Cisco IOS(기본 모드)

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

위의 예에서 인터페이스 컨피그레이션을 입력하고 **no** 형식의 명령을 적용하여 IOS이므로 포트를 신뢰할 수 없음으로 설정합니다.

신뢰할 수 있는 포트

스위치를 입력하는 이더넷 프레임에는 CoS 또는 ToS 설정이 있을 때가 있는데, 이는 프레임이 스위치를 이동할 때 관리자가 유지하려는 설정입니다. 이 트래픽의 경우 관리자는 트래픽이 스위치로 들어오는 포트의 신뢰 상태를 신뢰할 수 있는 상태로 설정할 수 있습니다.

앞에서 언급한 대로 스위치는 내부적으로 DSCP 값을 사용하여 해당 프레임에 미리 결정된 서비스 레벨을 할당합니다. 프레임이 신뢰할 수 있는 포트로 들어가면 관리자는 기존 CoS, IP 우선 순위 또는 DSCP 값을 확인하여 내부 DSCP 값을 설정하도록 포트를 구성할 수 있습니다. 또는 관리자가 미리 정의된 DSCP를 포트에 들어가는 모든 패킷으로 설정할 수 있습니다.

다음 명령을 실행하여 포트의 신뢰 상태를 신뢰할 수 있는 포트로 설정할 수 있습니다.

CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

이 명령은 WS-X6548-RJ45 라인 카드에서 적용할 수 있으며 포트 3/16의 신뢰 상태를 trusted로 설정합니다. 스위치는 수신 프레임에 설정된 CoS 값을 사용하여 내부 DSCP를 설정합니다. DSCP는 스위치에서 QoS를 활성화했을 때 생성된 기본 맵에서 파생되거나 관리자가 정의한 맵에서 파생됩니다. trust-COs 키워드 대신 관리자는 trust-dscp 또는 trust-ipprec 키워드를 사용할 수도 있습니다.

이전 10/100 라인 카드(WS-X6348-RJ45 및 WS-X6248-RJ45)에서 **set qos acl** 명령을 실행하여 포트 트러스트를 설정해야 합니다. 이 명령에서 신뢰 상태는 set qos acl 명령의 하위 매개 변수**로** 할당할 수 있습니다. 아래 그림과 같이 이러한 라인 카드의 포트에서 신뢰 CoS를 설정할 수 없습니다.

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to
turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so
port is set to untrusted.
```

위의 명령은 입력 대기열 예약을 활성화해야 함을 나타냅니다. 따라서 WS-X6248-RJ45 및 WS-X6348-RJ45 라인 카드의 10/100 포트의 경우 **set port qos/y trust-COs** 명령을 구성해야 하지만 신

뢰 상태를 설정하려면 ACL을 사용해야 합니다.

Integrated Cisco IOS(Native Mode)를 사용하면 GE 인터페이스와 새 WS-X6548-RJ45 라인 카드의 10/100 포트에서 신뢰 설정을 수행할 수 있습니다.

통합 Cisco IOS(기본 모드)

```
Cat6500(config)# interface gigabitethernet 5/4
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

이 예에서는 GE 포트 5/4의 신뢰 상태를 trusted로 설정합니다. 프레임의 IP 우선 순위 값은 DSCP 값을 파생시키는 데 사용됩니다.

입력 분류 및 포트 기반 CoS 설정

스위치 포트에 인그레스(ingress)할 때 이더넷 프레임이 다음 두 기준 중 하나를 충족하면 CoS를 변경할 수 있습니다.

1. 포트가 신뢰할 수 없는 것으로 구성됨 또는
2. 이더넷 프레임에 이미 설정된 기존 CoS 값이 없습니다.

수신 이더넷 프레임의 CoS를 다시 구성하려면 다음 명령을 실행해야 합니다.

CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

이 명령은 모듈 3의 포트 16에 있는 수신 이더넷 프레임의 CO를 표시가 없는 프레임이 도착하거나 포트가 신뢰할 수 없음으로 설정된 경우 값 3으로 설정합니다.

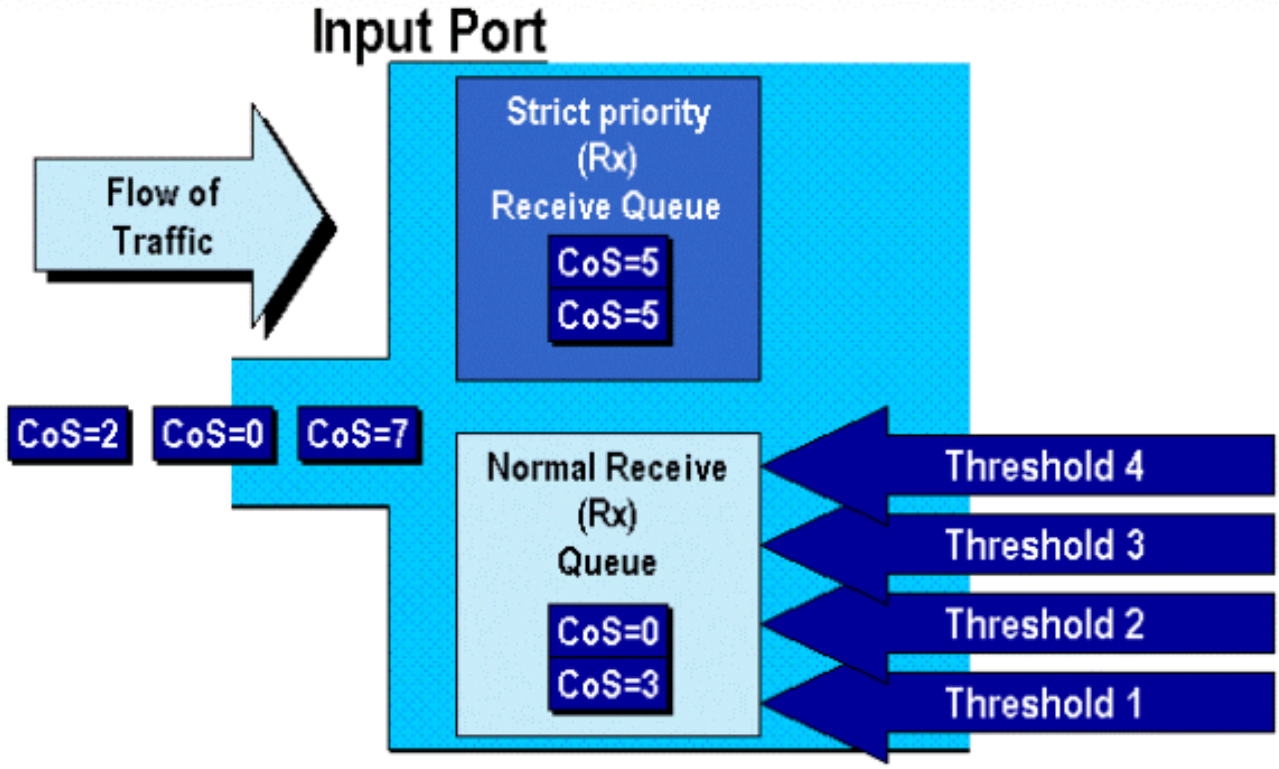
통합 Cisco IOS(기본 모드)

```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

이 명령은 모듈 5의 포트 13에 있는 수신 이더넷 프레임의 CO를 표시가 없는 프레임이 도착하거나 포트가 신뢰할 수 없음으로 설정된 경우 값 4로 설정합니다.

Rx 삭제 임계값 구성

스위치 포트에 대한 인그레스(ingress)에서 프레임은 Rx 대기열에 배치됩니다. 버퍼 오버플로를 방지하기 위해 포트 ASIC는 각 Rx 대기열에 4개의 임계값을 구현하고 이러한 임계값을 사용하여 임계값을 초과하면 삭제될 수 있는 프레임을 식별합니다. 포트 ASIC는 임계값을 초과할 때 삭제할 수 있는 프레임을 식별하기 위해 설정된 COs 값을 사용합니다. 이 기능을 사용하면 혼잡이 발생할 때 우선 순위가 더 높은 프레임이 버퍼에 더 오랫동안 남아 있을 수 있습니다.



위 다이어그램에 표시된 것처럼 프레임이 도달하여 대기열에 배치됩니다. 큐가 채워지기 시작하면 임계값은 포트 ASIC에 의해 모니터링됩니다. 임계값이 위반되면 관리자가 식별한 CO 값이 있는 프레임이 대기열에서 무작위로 삭제됩니다. 1q4t 큐(WS-X6248-RJ45 및 WS-X6348-RJ45 라인 카드에 있음)의 기본 임계값 매핑은 다음과 같습니다.

- 임계값 1은 50%로 설정되고 COs 값 0과 1은 이 임계값에 매핑됩니다.
- 임계값 2는 60%로 설정되고 COs 값 2와 3은 이 임계값에 매핑됩니다.
- threshold 3은 80%로 설정되고 COs 값 4와 5는 이 임계값에 매핑됩니다.
- 임계값 4는 100%로 설정되고 COs 값 6과 7은 이 임계값에 매핑됩니다.

1P1q4t(GE 포트에 있음) 대기열의 경우 기본 매핑은 다음과 같습니다.

- 임계값 1은 50%로 설정되고 COs 값 0과 1은 이 임계값에 매핑됩니다.
- 임계값 2는 60%로 설정되고 COs 값 2와 3은 이 임계값에 매핑됩니다.
- threshold 3은 80%로 설정되고 COs 값 4는 이 임계값에 매핑됩니다.
- 임계값 4는 100%로 설정되고 COs 값 6과 7은 이 임계값에 매핑됩니다.
- COs 값 5가 엄격한 우선 순위 큐에 매핑됩니다.

1p1q0t(WS-X6548-RJ45 라인 카드의 10/100 포트에 있음)의 경우 기본 매핑은 다음과 같습니다.

- COs 5가 있는 프레임은 SP Rx 큐(큐 2)로 이동합니다. 이 경우 SP 수신 대기열 버퍼가 100% 찼을 때만 스위치가 수신 프레임을 삭제합니다.
- CO가 0, 1, 2, 3, 4, 6 또는 7인 프레임은 표준 Rx 큐로 이동합니다. Rx 큐 버퍼가 100% 찼을 때 스위치는 들어오는 프레임을 삭제합니다.

관리자가 이러한 삭제 임계값을 변경할 수 있습니다. 또한 각 임계값에 매핑된 기본 CO 값도 변경할 수 있습니다. 다른 라인 카드는 서로 다른 Rx 대기열 구현을 구현합니다. 대기열 유형의 요약이 아래에 나와 있습니다.

CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

이 명령은 하나의 대기열과 4개의 임계값(1q4t 표시)을 가진 모든 입력 포트에 대한 수신 삭제 임계값을 20%, 40%, 75% 및 100%로 설정합니다.

통합 Cisco IOS(기본 모드)에서 실행된 명령은 아래와 같습니다.

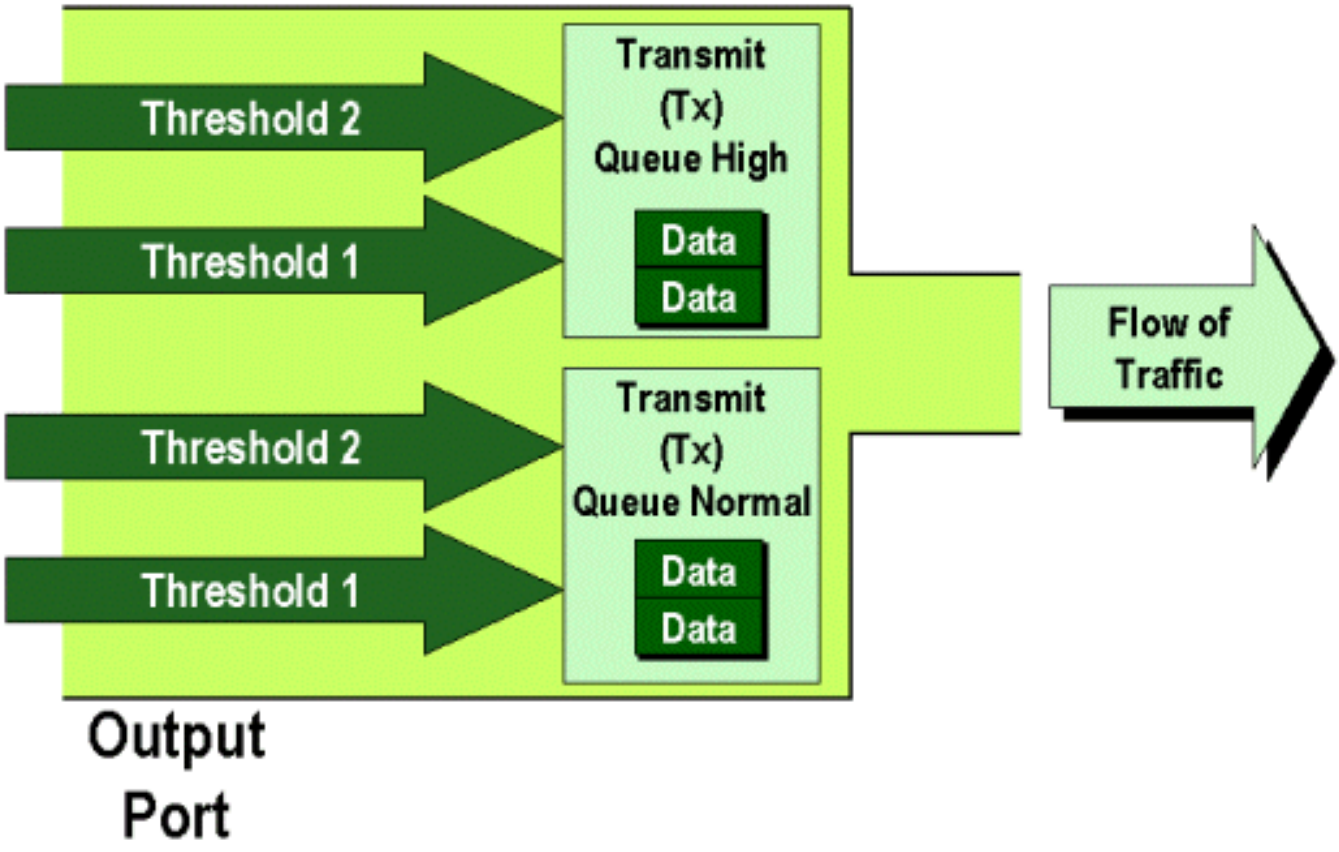
통합 Cisco IOS(기본 모드)

```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100

!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line
card.
```

관리자가 Rx 삭제 임계값을 활성화해야 합니다. 현재 set **port qos x/y trust trust-COs** 명령을 사용하여 Rx 삭제 임계값을 활성화해야 합니다(*x*는 모듈 번호이고 y는 해당 모듈의 포트임).

TX 삭제 임계값 구성

이그레스 포트에서 포트에는 혼잡 방지 메커니즘의 일부로 사용되는 두 개의 TX 임계값(대기열 1 및 대기열 2)이 있습니다. 대기열 1은 표준 낮은 우선순위 대기열로 표시되고 대기열 2는 표준 높은 우선순위 대기열로 표시됩니다. 사용된 라인 카드에 따라 tail drop 또는 WRED 임계값 관리 알고리즘을 사용합니다. 두 알고리즘 모두 각 TX 대기열에 대해 두 개의 임계값을 사용합니다.



관리자는 다음과 같이 이러한 임계값을 수동으로 설정할 수 있습니다.

CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

이 명령은 대기열 2개와 임계값 2개(2q2t 표시)가 있는 모든 출력 포트에 대해 대기열 1에 대한 TX 삭제 임계값을 40% 및 100%로 설정합니다.

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

이 명령은 하나의 SP 대기열, 두 개의 일반 대기열 및 두 개의 임계값(1p2q2t 표시)을 가진 모든 출력 포트에 대해 대기열 1에 대한 WRED 삭제 임계값을 60% 및 100%로 설정합니다. 대기열 1은 일반 낮은 우선 순위 대기열로 정의되며 우선순위가 가장 낮습니다. 대기열 2는 우선 순위가 높은 일반 대기열이며 대기열 1보다 우선 순위가 높습니다. 대기열 3은 SP 대기열이며 해당 포트의 다른 모든 대기열보다 먼저 처리됩니다.

Integrated Cisco IOS(Native Mode)에서 실행된 동등한 명령은 아래와 같습니다.

통합 Cisco IOS(기본 모드)

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
Cat6500(config-if)#
```

이렇게 하면 1p2q2t 포트의 WRED 삭제 임계값이 TX(threshold 1)의 경우 1~40%, TX(threshold 2)의 경우 100%로 설정됩니다.

Integrated Cisco IOS(기본 모드)에서 필요한 경우 WRED를 비활성화할 수도 있습니다. 이 작업을 수행하는 데 사용되는 방법은 명령의 **n"** 형식을 사용하는 것입니다. WRED를 비활성화하는 예는 다음과 같습니다.

통합 Cisco IOS(기본 모드)

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

MAC 주소를 COs 값에 매핑

전역 포트 정의를 기반으로 CO를 설정하는 것 외에도, 이 스위치를 사용하면 관리자가 대상 MAC 주소 및 VLAN ID를 기반으로 COs 값을 설정할 수 있습니다. 이렇게 하면 특정 타겟으로 향하는 프레임이 미리 결정된 COs 값으로 태깅될 수 있습니다. 이 컨피그레이션은 다음 명령을 실행하여 수행할 수 있습니다.

CatOS

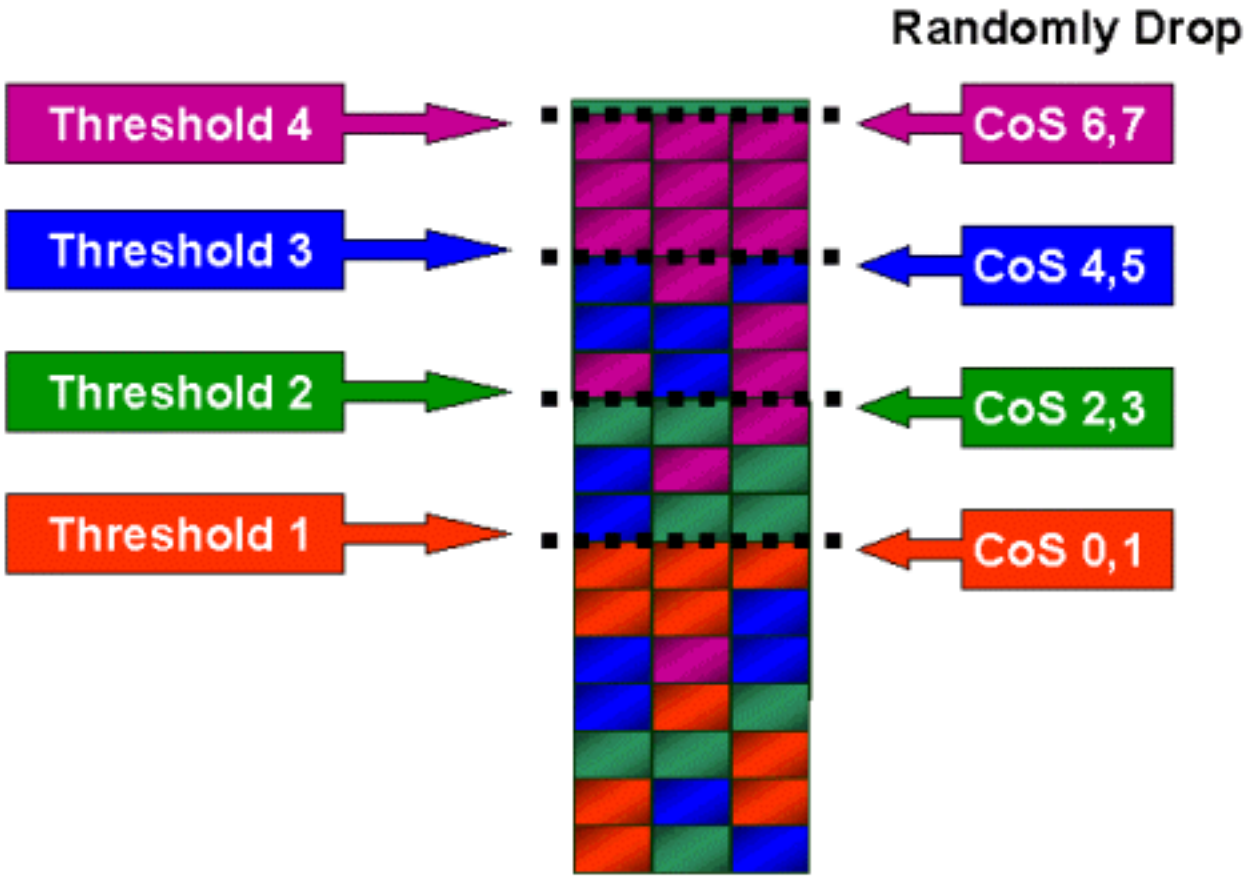
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

이 명령은 대상 MAC 주소가 VLAN 200에서 보낸 00-00-0c-33-2a-4e인 모든 프레임에 대해 CO를 5로 설정합니다.

Integrated Cisco IOS(Native Mode)에는 동일한 명령이 없습니다. 이는 PFC가 없고 Integrated Cisco IOS(Native Mode)가 작동하려면 PFC가 필요한 경우에만 이 명령이 지원되기 때문입니다.

임계값에 CO 매핑

임계값이 구성된 후 관리자는 이러한 임계값에 COs 값을 할당하여 임계값이 초과되면 특정 COs 값이 있는 프레임을 삭제할 수 있습니다. 일반적으로 관리자는 낮은 임계값에 낮은 우선 순위 프레임을 할당하므로 혼잡이 발생할 경우 대기열에서 높은 우선 순위 트래픽을 유지합니다.



위의 그림에는 4개의 임계값이 있는 입력 대기열과 각 임계값에 COs 값이 할당된 방법이 나와 있습니다.

다음 출력은 COs 값을 임계값에 매핑하는 방법을 보여줍니다.

CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

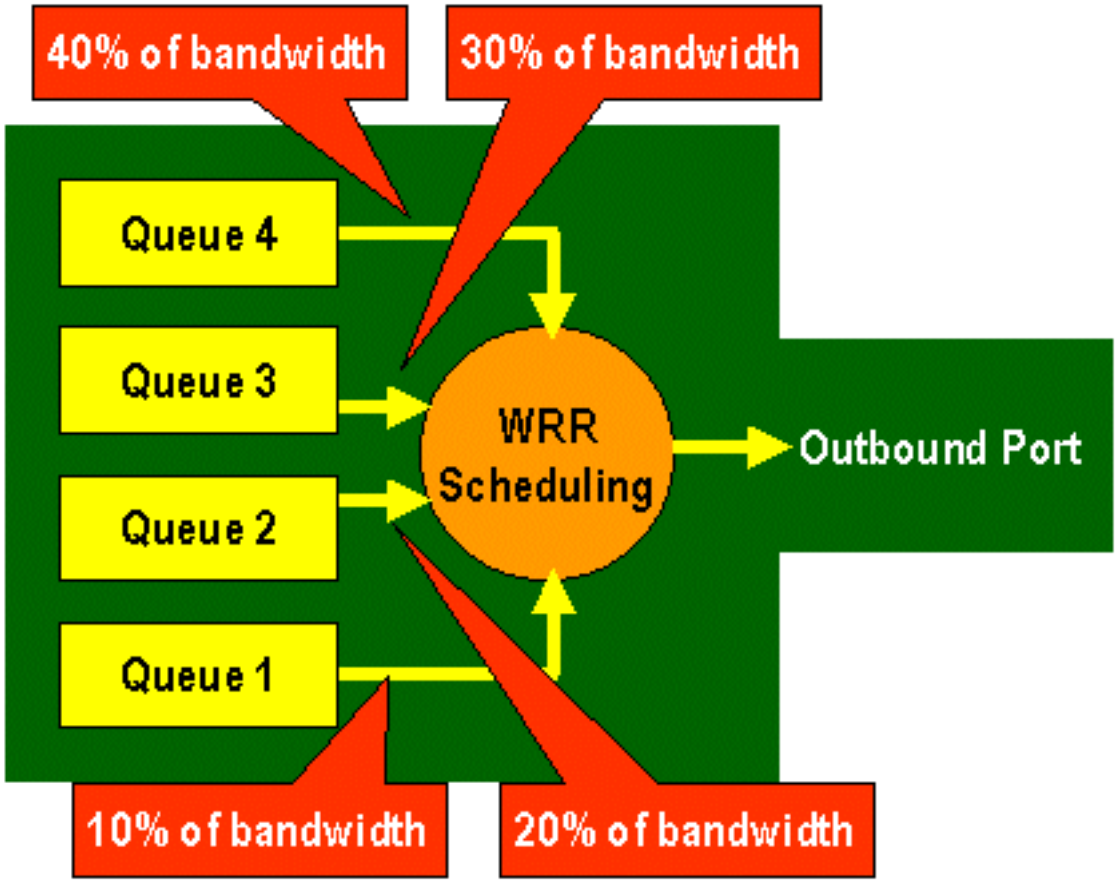
이 명령은 대기열 1, 임계값 1에 0 및 1의 COs 값을 할당합니다. Integrated Cisco IOS(Native Mode)의 해당 명령이 아래에 나와 있습니다.

통합 Cisco IOS(기본 모드)

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

TX 큐의 대역폭 구성

출력 대기열에 프레임이 배치되면 출력 스케줄링 알고리즘을 사용하여 전송됩니다. 출력 스케줄러 프로세스는 WRR을 사용하여 출력 큐에서 프레임을 전송합니다. 사용 중인 라인 카드 하드웨어에 따라 포트당 2개, 3개 또는 4개의 전송 대기열이 있습니다.



WS-X6248 및 WS-X6348 라인 카드(2q2t 큐 구조 포함)에서 WRR 메커니즘에서 스케줄링에 두 개의 TX 큐를 사용합니다. WS-X6548 라인 카드(1p3q1t 큐 구조 포함)에는 4개의 TX 대기열이 있습니다. 이 4개의 TX 대기열 중 3개의 TX 대기열은 WRR 알고리즘에 의해 서비스됩니다(마지막 TX 대기열은 SP 대기열임). GE 라인 카드에는 3개의 TX 대기열이 있습니다(1p2q2t 대기열 구조 사용). 이러한 대기열 중 하나는 SP 대기열이므로 WRR 알고리즘은 두 개의 TX 대기열만 서비스합니다.

일반적으로 관리자는 TX 대기열에 가중치를 할당합니다. WRR은 포트 대기열에 할당된 가중치를 확인하는 방식으로 작동합니다. 이 가중치는 스위치가 내부적으로 사용하여 다음 대기열로 이동하기 전에 전송할 트래픽 양을 결정합니다. 1에서 255 사이의 가중치 값을 각 포트 대기열에 할당할 수 있습니다.

CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

이 명령은 대기열 1과 대기열 2에 가중치 40을 할당하고 대기열 1 및 80을 할당합니다. 이는 두 대

기열 사이에 할당된 대역폭의 2-1 비율(80 ~ 40 = 2 ~ 1)을 의미합니다. 이 명령은 2개의 대기열과 2개의 임계값이 있는 모든 포트에서 적용됩니다.

Integrated Cisco IOS(Native Mode)에서 실행된 동등한 명령은 아래와 같습니다.

통합 Cisco IOS(기본 모드)

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
Cat6500(config-if)#
```

위의 는 두 대기열 간의 3 대 1 비율을 나타냅니다. 이 명령의 Cat IOS 버전은 특정 인터페이스에만 적용됩니다.

COs에 DSCP 매핑

프레임이 이그레스 포트에 배치되면 포트 ASIC은 할당된 CO를 사용하여 혼잡 회피(즉, WRED)를 수행하고 CO를 사용하여 프레임(즉, 프레임 전송)의 일정을 결정합니다. 이때 스위치는 기본 맵을 사용하여 할당된 DSCP를 가져온 다음 다시 COs 값에 매핑합니다. 이 기본 맵은 이 테이블에 표시됩니다.

또는 관리자가 스위치에서 사용할 맵을 만들어 할당된 내부 DSCP 값을 가져오고 프레임에 대한 새 COs 값을 생성할 수 있습니다. CatOS 및 Integrated Cisco IOS(Native Mode)를 사용하여 이를 달성하는 방법의 예는 아래와 같습니다.

CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

위의 명령은 DSCP 값 20부터 30까지 COs 값 5에 매핑하고, DSCP 값 10부터 15까지 3의 CO에 매핑하며, DSCP 값 45부터 52까지 7의 COs 값에 매핑합니다. 다른 모든 DSCP 값은 스위치에서 QoS가 활성화되었을 때 생성된 기본 맵을 사용합니다.

Integrated Cisco IOS(Native Mode)에서 실행된 동등한 명령은 아래와 같습니다.

통합 Cisco IOS(기본 모드)

```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

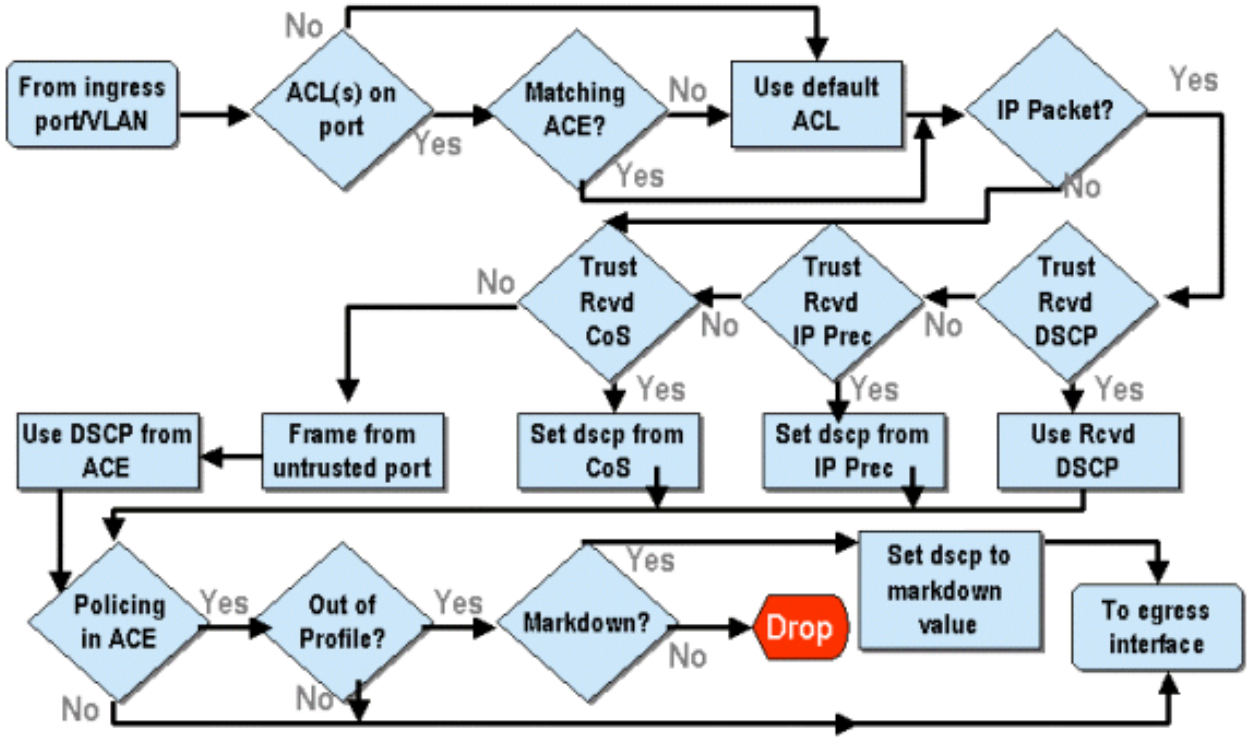
이렇게 하면 DSCP 값이 20, 30, 40, 50, 52, 10 및 1로 COs 값 3으로 설정됩니다.

PFC를 사용한 분류 및 폴리싱

PFC는 프레임의 분류 및 폴리싱을 지원합니다. 분류는 ACL을 사용하여 DSCP(Priority)로 들어오는 프레임을 할당(표시)할 수 있습니다. 폴리싱을 사용하면 트래픽의 스트림이 특정 양의 대역폭으로 제한될 수 있습니다.

다음 섹션에서는 CatOS와 Integrated Cisco IOS(Native Mode) OS 플랫폼의 관점에서 PFC에 대한

이러한 기능에 대해 설명합니다. PFC에서 적용한 프로세스는 다음 다이어그램에 나와 있습니다.



CatOS를 사용하여 Catalyst 6000 제품군에 폴리싱 구성

폴리싱의 기능은 CatOS용 섹션과 Integrated Cisco IOS(Native Mode)용 두 섹션으로 구분됩니다. 두 가지 모두 동일한 최종 결과를 달성하지만 서로 다른 방식으로 구성 및 구현됩니다.

폴리싱

PFC는 스위치로 들어오는 트래픽을 제한(또는 경찰)할 수 있는 기능을 지원하며, 트래픽 흐름을 미리 정의된 제한 값으로 줄일 수 있습니다. 해당 제한을 초과하는 트래픽은 삭제되거나 프레임의 DSCP 값이 더 낮은 값으로 표시될 수 있습니다.

출력(이그레스) 속도 제한은 현재 PFC1 또는 PFC2에서 지원되지 않습니다. 이 값은 출력(또는 이그레스) 폴리싱을 지원할 2002년 하반기에 계획된 PFC의 새 개정판에 추가됩니다.

이러한 기능의 컨피그레이션은 매우 다르지만 CatOS 및 새로운 Integrated Cisco IOS(Native Mode)에서 폴리싱이 모두 지원됩니다. 다음 섹션에서는 두 OS 플랫폼의 폴리싱 컨피그레이션에 대해 설명합니다.

집계 및 마이크로플로우(CatOS)

집계 및 마이크로플로우는 PFC가 수행하는 폴리싱 범위를 정의하는 데 사용되는 용어입니다.

마이크로플로우는 단일 플로우의 폴리싱을 정의합니다. 플로우는 고유한 SA/DA MAC 주소, SA/DA IP 주소 및 TCP/UDP 포트 번호를 가진 세션에 의해 정의됩니다. VLAN의 포트를 통해 시작되는 새 흐름마다 마이크로플로우를 사용하여 스위치에서 해당 플로우에 대해 수신되는 데이터의 양을 제한할 수 있습니다. 마이크로플로우 정의에서 지정된 속도 제한을 초과하는 패킷은 삭제되거나 DSCP 값이 down으로 표시될 수 있습니다.

마이크로플로우와 마찬가지로, 트래픽을 제한하는 데 집계를 사용할 수 있습니다. 그러나 집계 속도는 지정된 QoS ACL과 일치하는 포트 또는 VLAN의 모든 인바운드 트래픽에 적용됩니다. ACE(Access Control Entry)의 프로필과 일치하는 누적 트래픽의 폴리싱으로 집계를 볼 수 있습니다
.

집계 및 마이크로플로우는 모두 스위치로 수락할 수 있는 트래픽의 양을 정의합니다. 집계 및 마이크로플로우는 포트 또는 VLAN에 동시에 할당할 수 있습니다.

마이크로플로우를 정의할 때 최대 63개의 마이크로플로우를 정의할 수 있으며 최대 1,023개의 집계를 정의할 수 있습니다.

액세스 제어 항목 및 QoS ACL(CatOS)

QoS ACL은 PFC가 수신 프레임을 처리하는 데 사용하는 QoS 규칙 집합을 정의하는 ACE 목록으로 구성됩니다. ACE는 RACL(Router Access Control List)과 유사합니다. ACE는 들어오는 프레임에 대한 분류, 표시 및 폴리싱 기준을 정의합니다. 수신 프레임이 ACE에 설정된 기준과 일치하면 QoS 엔진이 프레임을 처리합니다(ACE에서 간주하는 경우).

모든 QoS 처리는 하드웨어에서 수행되므로 QoS 폴리싱을 활성화해도 스위치 성능에 영향을 주지 않습니다.

PFC2는 현재 최대 500개의 ACL을 지원하며 이러한 ACL은 총 32,000개의 ACE로 구성될 수 있습니다. 실제 ACE 번호는 PFC에서 정의된 다른 서비스 및 사용 가능한 메모리에 따라 달라집니다.

세 가지 유형의 에이스를 정의할 수 있습니다. IP, IPX 및 MAC입니다. IP 및 IPX Ace 모두 L3 헤더 정보를 검사하는 반면 MAC 기반 Ace는 L2 헤더 정보만 검사합니다. 또한 MAC 에이스는 비 IP 및 비 IPX 트래픽에만 적용할 수 있습니다.

폴리싱 규칙 생성

폴리싱 규칙을 생성하는 프로세스에는 집계(또는 마이크로플로우)를 생성한 다음 해당 집계(또는 마이크로플로우)를 ACE에 매핑해야 합니다.

예를 들어, 포트 5/3의 모든 수신 IP 트래픽을 최대 20MB로 제한해야 하는 경우 위에서 언급한 두 단계를 구성해야 합니다.

먼저, 이 예에서는 모든 수신 IP 트래픽을 제한하도록 요청합니다. 이는 집계 폴리서를 정의해야 함을 의미합니다. 예를 들면 다음과 같습니다.

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

테스트 흐름이라는 집계를 만들었습니다. 20000KBPS(20MBPS) 및 버스트 13을 정의합니다. policed-dscp 키워드는 이 정책을 초과하는 모든 데이터에 DSCP markup 맵에 지정된 대로 아래로 표시된 DSCP 값이 있음을 나타냅니다(기본 값이 있거나 관리자가 수정할 수 있음). policed-dscp 키워드를 사용하는 또 다른 방법은 drop 키워드를 사용하는 것입니다. drop 키워드는 모든 out-of-profile 트래픽(할당된 버스트 값 외부에 있는 트래픽)을 삭제합니다.

폴리싱 기능은 버스트를 정의한다는 점에서 Leaky 토큰 버킷 체계에서 작동합니다. 즉, 지정된 (고정) 시간 간격 동안 수락할 초당 데이터 양(비트 수)과 그 다음 속도(해당 버킷을 1초 내에 비울 데이터 양으로 정의됨)입니다. 이 버킷을 오버플로하는 모든 데이터는 삭제되거나 해당 DSCP가 다운된 것으로 표시됩니다. 위에서 언급한 지정된 기간(또는 간격)은 0.00025초(또는 1/4000분의 1)이며 고정되어 있습니다(즉, 이 숫자를 변경하기 위해 어떤 컨피그레이션 명령도 사용할 수 없음).

위의 예에서 숫자 13은 1초의 1/4000초마다 최대 13,000비트의 데이터를 수용할 버킷을 나타냅니다. 이는 초당 52MB(13K * (1 / 0.00025) 또는 13K * 4000)와 관련이 있습니다. 버스트가 항상 데이터를 보낼 속도보다 크거나 같도록 구성되어야 합니다. 즉, 버스트는 지정된 기간 동안 전송하려는 최소 데이터 양보다 크거나 같아야 합니다. 버스트 결과로 속도가 지정된 수치보다 더 낮아지면 속

도 제한이 버스트와 같습니다. 즉, 20MBPS의 속도와 15MBPS로 계산되는 버스트를 정의하면 속도가 15MBPS에 불과합니다. 다음 질문은 왜 13인지 입니다. 버스트는 토큰 버킷의 깊이를 정의합니다. 즉, 초당 1/4000초마다 수신 데이터를 수신하는 데 사용되는 버킷의 깊이를 정의합니다. 따라서 버스트는 초당 20MB보다 크거나 같은 도착 데이터 전송에서 지원되는 숫자일 수 있습니다. 속도 제한 20MB에 사용할 수 있는 최소 버스트는 20000/4000 = 5입니다.

폴리서를 처리할 때 토큰 버킷에 토큰의 완전한 보충을 입력하여 폴리싱 알고리즘이 시작됩니다. 토큰 수는 버스트 값과 같습니다. 버스트 값이 13이면 버킷의 토큰 수는 13,000개입니다. 초당 1/4000분의 1에 대해 폴리싱 알고리즘은 정의된 비율과 동일한 양의 데이터를 4000으로 나눕니다. 전송된 데이터의 모든 비트(이진 숫자)에 대해 버킷에서 하나의 토큰을 사용합니다. 간격이 끝나면 새 토큰 세트로 버킷을 보충합니다. 교체되는 토큰 수는 rate/4000으로 정의됩니다. 위의 예를 참조하여 이를 이해하십시오.

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

100MBPS 포트이며 100MBPS의 일정한 스트림을 포트로 전송한다고 가정합니다. 이는 초당 100,000,000비트의 수신 속도와 같습니다. 이 매개변수는 20000과 버스트 13의 비율입니다. 시간 간격 t0에는 버킷에 토큰(13,000개)의 전체 보충이 있습니다. time interval t0에는 첫 번째 데이터 집합이 포트에 도착하게 됩니다. 이 시간 간격 동안 도착 비율은 100,000,000/4000 = 초당 25,000비트입니다. 토큰 버킷에는 깊이 13,000개의 토큰만 있으므로 이 간격 동안 포트에 도착하는 25,000비트의 13,000비트만 전송될 수 있으며 12,000비트가 삭제됩니다.

지정된 속도는 1/4000번째 간격당 전송된 5,000비트와 같은 초당 20,000,000비트의 전달 속도를 정의합니다. 전송된 5,000비트마다 5,000개의 토큰이 사용됩니다. 시간 간격 T1에 다른 25,000비트의 데이터가 도착하지만 버킷은 12,000비트를 삭제합니다. 버킷은 rate/4000(새 토큰 5,000개)으로 정의된 토큰으로 보충됩니다. 그런 다음 이 알고리즘은 각 간격마다 다른 5,000비트의 데이터(다른 5,000개의 토큰 사용)와 같은 다음 보완 데이터를 전송합니다.

기본적으로 버킷 깊이(정의된 버스트)를 초과하는 데이터는 삭제됩니다. 데이터가 전송된 후(지정된 속도와 일치) 남은 데이터도 삭제되므로 다음 데이터 집합을 가져올 수 있습니다. 불완전한 패킷은 해당 시간 간격 내에 완전히 수신되지 않은 패킷은 삭제되지 않고 포트에 완전히 수신될 때까지 보관됩니다.

이 버스트 번호는 트래픽의 지속적인 흐름을 전제로 합니다. 그러나 실제 네트워크에서는 데이터가 일정하지 않으며 흐름은 전송 시퀀스에 TCP 승인을 통합하는 TCP 윈도우 크기에 따라 결정됩니다. TCP 윈도우 크기의 문제를 고려하려면 버스트 값을 두 배로 하는 것이 좋습니다. 위의 예에서 제안된 값 13은 실제로 26으로 구성됩니다.

또 다른 중요한 점은 시간 간격 0(즉, 폴리싱 주기의 시작)에서 토큰 버킷은 토큰으로 가득 차 있다는 것입니다.

이제 이 종합 정책을 QoS ACE에 통합해야 합니다. ACE는 기준 집합을 수신 프레임에 일치시키기 위해 사양을 만드는 곳입니다. 다음 예를 고려하십시오. 위에 정의된 집계를 모든 IP 트래픽에 적용하되, 서브넷 10.5.x.x에서 소싱되고 서브넷 203.100.45.x로 향하는 트래픽에 특히 적용하고자 합니다. ACE는 다음과 같습니다.

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

위의 명령은 **set qos acl ip** 명령의 사용으로 표시되는 IP ACE를 생성했으며, 이는 이제 test-acl이라는 QoS ACL과 연결됩니다. ACL 테스트 ACL에 생성 및 연결된 후속 ACE는 ACE 목록의 끝에 추가

됩니다. ACE 항목에는 연결된 종합 테스트 흐름이 있습니다. 소스 서브넷이 10.5.0.0이고 대상 서브넷이 203.100.45.0인 모든 TCP 흐름에는 이 정책이 적용됩니다.

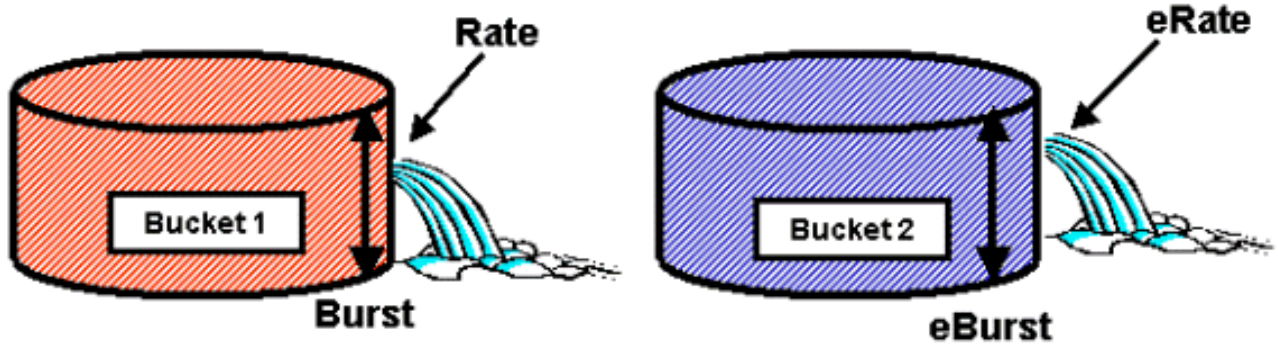
ACL(및 관련 ACE)은 관리자가 사용할 수 있는 매우 세분화된 구성 유연성을 제공합니다. ACL은 하나 이상의 Ace로 구성될 수 있으며 L4 포트 값뿐 아니라 소스 및/또는 목적지 주소도 사용하여 폴리싱해야 하는 특정 흐름을 식별할 수 있습니다.

그러나 폴리싱이 실제로 발생하기 전에 ACL을 물리적 포트 또는 VLAN에 매핑해야 합니다.

PFC2 정책 결정

PFC2의 경우 폴리싱을 위한 이중 누수가 있는 버킷 알고리즘을 도입한 CatOS 7.1과 CatOS 7.2에서 변경이 발생했습니다. 이 새로운 알고리즘을 사용하면 다음과 같은 두 가지 새로운 레벨이 추가됩니다.

1. **일반 폴리싱 수준:** 이는 첫 번째 버켓과 동일하며 버킷의 깊이(버스트)와 버킷에서 데이터를 전송해야 하는 비율(속도)을 지정하는 매개변수를 정의합니다.
2. **초과 폴리싱 수준:** 이는 두 번째 버켓과 동일하며 버킷(eburst)의 깊이 및 버킷에서 데이터를 전송해야 하는 비율(날짜)을 지정하는 매개변수를 정의합니다.



이 프로세스가 작동하는 방법은 데이터가 첫 번째 버킷에 입력되기 시작하는 것입니다. PFC2는 첫 번째 버킷의 깊이(버스트 값)보다 작거나 같은 데이터 수신 스트림을 수용합니다. 첫 번째 버킷에서 오버플로되는 데이터는 다운으로 표시될 수 있으며 두 번째 버킷으로 전달됩니다. 두 번째 버킷은 버킷 1에서 버스트 값보다 작거나 같은 값으로 흐르는 데이터의 수신 속도를 허용할 수 있습니다. 두 번째 버킷의 데이터는 속도 매개변수를 제외한 실제 매개변수에 의해 정의된 비율로 전송됩니다. 두 번째 버킷에서 오버플로되는 데이터도 다운되거나 삭제될 수 있습니다.

이중 이중 이중 이중 버킷 폴리서의 예는 다음과 같습니다.

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst 13 eburst 13
```

이 예에서는 트래픽 속도가 10MBPS를 초과하는 AGG1이라는 집계를 설정하며, 폴리싱된 DSCP 맵에 따라 아래로 표시됩니다. 속도(12MBPS로 설정)를 초과하는 트래픽은 drop 키워드에 따라 삭제됩니다.

DFC 지원 모듈에 종합 폴리서 적용

6000에서 트래픽 포워딩 시 중앙 집중식 포워딩 엔진(PFC)을 사용하는 방식 때문에 비 DFC 라인 카드에 종합 폴리서를 적용할 수 있다는 점에 유의해야 합니다. 중앙 포워딩 엔진을 구현하면 지정된 VLAN에 대한 트래픽 통계를 추적할 수 있습니다. 이 프로세스를 사용하여 VLAN에 종합 정책을 적용할 수 있습니다.

그러나 DFC 지원 라인 카드에서는 포워딩 결정이 해당 라인 카드에 배포됩니다. DFC는 즉시 라인 카드의 포트만 인식하며 다른 라인 카드의 트래픽 이동을 인식하지 못합니다. 따라서 여러 DFC 모

듈에서 멤버 포트가 있는 VLAN에 집계 폴리서가 적용된 경우 폴리서가 일관성 없는 결과를 생성할 수 있습니다. 그 이유는 DFC가 로컬 포트 통계만 추적할 수 있고 다른 라인 카드의 포트 통계를 고려하지 않기 때문입니다. 따라서 DFC 지원 라인 카드에 멤버 포트가 있는 VLAN에 적용된 종합 폴리서는 DFC 라인 카드에만 상주하는 VLAN 포트에 대한 정격 제한에 DFC 폴리싱 트래픽을 생성합니다.

DSCP 마크업 맵(CatOS)

DSCP 마크업 맵은 정책을 정의하여 드롭하는 대신 아웃오브프로파일 트래픽을 축소하는 데 사용됩니다. 프로필 외 트래픽은 정의된 버스트 설정을 초과하는 트래픽으로 정의됩니다.

QoS가 활성화된 경우 기본 DSCP 마크업 맵이 설정됩니다. 이 기본 마크업 맵은 문서 앞에 있는 이 표에 나열됩니다. 관리자는 CLI(Command Line Interface)를 사용하여 set qos policed-dscp-map 명령을 실행하여 기본 **markdown 맵을** 수정할 수 있습니다. 이 예시는 아래와 같습니다.

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

이 예에서는 폴리싱된 DSCP 맵을 수정하여 DSCP 값 20~25가 DSCP 값 7로 표시되고 33~38의 DSCP 값은 DSCP 값 3으로 하향 표시됩니다.

VLAN 및 포트에 정책 매핑(CatOS)

ACL이 구축되면 해당 ACL을 적용하려면 포트 또는 VLAN에 매핑해야 합니다.

많은 사람들이 인식하지 못하는 한 가지 흥미로운 명령은 모든 QoS 포트를 기반으로 하는 기본 QoS 설정입니다. VLAN에 집계(또는 마이크로플로우)를 적용하는 경우 해당 포트가 VLAN 기반 QoS에 대해 구성되지 않은 한 포트에 적용되지 않습니다.

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

포트 기반 QoS를 VLAN 기반 QoS로 변경하면 해당 포트에 할당된 모든 ACL이 즉시 탐지되고 해당 포트에 모든 VLAN 기반 ACL이 할당됩니다.

다음 명령을 실행하여 ACL을 포트(또는 VLAN)에 매핑합니다.

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

ACL을 포트(또는 VLAN)에 매핑한 후에도 ACL이 하드웨어에 커밋될 때까지 ACL이 적용되지 않습니다. 이 내용은 다음 섹션에서 설명합니다. 이 시점에서 ACL은 메모리의 임시 편집 버퍼에 상주합니다. 이 버퍼에서 ACL을 수정할 수 있습니다.

편집버퍼에 있는 커밋되지 않은 ACL을 제거하려면 rollback 명령을 **실행합니다**. 이 명령은 기본적으로 편집 버퍼에서 ACL을 삭제합니다.

```
Console> (enable) rollback qos acl test-acl
```

```
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

ACL 커밋(CatOS)

정의한 QoS ACL(위)을 적용하려면 하드웨어에 ACL을 커밋해야 합니다. 커밋하는 프로세스는 ACL을 임시 버퍼에서 PFC 하드웨어로 복사합니다. PFC 메모리에 상주하면 QoS ACL에 정의된 정책을 Aces와 일치하는 모든 트래픽에 적용할 수 있습니다

컨피그레이션을 쉽게 하기 위해 대부분의 관리자는 **commit all** 명령을 실행합니다. 그러나 현재 편집 버퍼에 있을 수 있는 특정 ACL(여러 ACL 중 하나)을 커밋할 수 있습니다. commit 명령의 예는 아래와 같습니다.

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

포트(또는 VLAN)에서 ACL을 제거하려면 다음 명령을 실행하여 해당 ACL을 해당 포트(또는 VLAN)에 연결하는 맵을 지워야 합니다.

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

통합 Cisco IOS(기본 모드)를 사용하여 Catalyst 6000 제품군에서 폴리싱 구성

Integrated Cisco IOS(Native Mode)에서 폴리싱이 지원됩니다. 그러나 정책 맵을 사용하여 폴리싱 기능의 컨피그레이션 및 구현을 수행합니다. 각 정책 맵은 여러 정책 클래스를 사용하여 정책 맵을 구성하며 이러한 정책 클래스는 서로 다른 유형의 트래픽 흐름에 대해 정의할 수 있습니다.

정책 맵 클래스(필터링 시)는 IOS 기반 ACL 및 클래스 일치 문을 사용하여 폴리싱할 트래픽을 식별합니다. 트래픽이 식별되면 정책 클래스는 집계 및 마이크로플로우 폴리서를 사용하여 일치하는 트래픽에 폴리싱 정책을 적용할 수 있습니다.

다음 섹션에서는 Integrated Cisco IOS(Native Mode)에 대한 폴리싱 컨피그레이션에 대해 자세히 설명합니다.

집계 및 마이크로플로우(통합 Cisco IOS(기본 모드))

집계 및 마이크로플로우는 PFC가 수행하는 폴리싱 범위를 정의하는 데 사용되는 용어입니다. CatOS와 마찬가지로 집계 및 마이크로플로우는 통합 Cisco IOS(기본 모드)에서도 사용됩니다.

마이크로플로우는 단일 플로우의 폴리싱을 정의합니다. 플로우는 고유한 SA/DA MAC 주소, SA/DA IP 주소 및 TCP/UDP 포트 번호를 가진 세션에 의해 정의됩니다. VLAN의 포트를 통해 시작되는 새 흐름마다 마이크로플로우를 사용하여 스위치에서 해당 플로우에 대해 수신되는 데이터의 양을 제한할 수 있습니다. 마이크로플로우 정의에서 지정된 속도 제한을 초과하는 패킷은 삭제되거나 DSCP 값이 down으로 표시될 수 있습니다. 마이크로플로우는 정책 맵 클래스의 일부를 형성하는 police flow 명령을 사용하여 적용됩니다.

통합 Cisco IOS(기본 모드)에서 마이크로플로우 폴리싱을 활성화하려면 스위치에서 전역적으로 활성화해야 합니다. 이 작업은 다음 명령을 실행하여 수행할 수 있습니다.

```
Cat6500(config)# mls qos flow-policing
```

L3 스위칭이 아닌 트래픽인 bridged 트래픽에도 Microflow 폴리싱을 적용할 수 있습니다. 스위치가

브리지 트래픽에서 마이크로플로우 폴리싱을 지원하도록 활성화하려면 다음 명령을 실행합니다.

```
Cat6500(config)# mls qos bridged
```

또한 이 명령은 멀티캐스트 트래픽에 대한 마이크로플로우 폴리싱을 활성화합니다. 멀티캐스트 트래픽에 마이크로플로우 폴리서가 적용되어야 하는 경우 이 명령(**mls qos bridged**)을 활성화해야 합니다.

마이크로플로우와 마찬가지로, 트래픽을 제한하는 데 집계를 사용할 수 있습니다. 그러나 집계 속도는 지정된 QoS ACL과 일치하는 포트 또는 VLAN의 모든 인바운드 트래픽에 적용됩니다. 정의된 트래픽 프로필과 일치하는 누적 트래픽의 폴리싱으로 집계를 볼 수 있습니다.

통합 Cisco IOS(기본 모드)에서 다음과 같이 정의할 수 있는 두 가지 형태의 집계가 있습니다.

- 인터페이스별 집계 폴리서
- 명명된 종합 폴리서

인터페이스당 집계는 정책 맵 클래스 내에서 **police** 명령을 실행하여 개별 인터페이스에 적용됩니다. 이러한 맵 클래스는 여러 인터페이스에 적용할 수 있지만 폴리서는 각 인터페이스를 개별적으로 정책합니다. 명명된 집계는 모든 인터페이스의 포트 및 경찰 트래픽 그룹에 누적적으로 적용됩니다. 명명된 집계는 mls qos aggregate policer 명령**을 실행하여** 적용됩니다.

마이크로플로우를 정의할 때 최대 63개의 마이크로플로우를 정의할 수 있으며 최대 1,023개의 집계를 정의할 수 있습니다.

폴리싱 규칙 생성(통합 Cisco IOS(기본 모드))

폴리싱 규칙을 생성하는 프로세스에는 정책 맵을 통해 집계(또는 마이크로플로우)를 생성한 다음 해당 정책 맵을 인터페이스에 연결하는 작업이 수반됩니다.

CatOS에 대해 생성된 동일한 예를 고려하십시오. 포트 5/3의 모든 수신 IP 트래픽을 최대 20MBPS로 제한해야 했습니다.

먼저 정책 맵을 만들어야 합니다. limit-traffic이라는 정책 맵을 만듭니다. 이 작업은 다음과 같이 수행됩니다.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

맵 클래스를 만들기 위한 컨피그레이션 모드에 있음을 반영하도록 스위치 프롬프트가 즉시 변경됩니다. 정책 맵에는 여러 클래스가 포함될 수 있습니다. 각 클래스에는 서로 다른 트래픽 스트림에 적용할 수 있는 별도의 정책 작업 집합이 포함되어 있습니다.

특히 수신 트래픽을 20MBPS로 제한하는 트래픽 클래스를 생성해야 합니다. 이 클래스는 20으로 제한됩니다. 다음은 아래와 같습니다.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
```

```
Cat6500(config-pmap-c)#
```

이제 맵 클래스 컨피그레이션에 있음을 반영하도록 프롬프트가 다시 변경됩니다(프롬프트 끝에 -c와 함께 표시됨). 특정 수신 트래픽과 일치하도록 속도 제한을 적용하려면 ACL을 구성하고 클래스 이름에 적용할 수 있습니다. 네트워크 10.10.1.x에서 소싱된 트래픽에 20MBPS 제한을 적용하려면 다음 ACL을 실행합니다.

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

다음과 같이 클래스 이름에 이 ACL을 추가할 수 있습니다.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

클래스 맵을 정의한 후에는 해당 클래스에 대한 개별 폴리서를 정의할 수 있습니다. police 키워드를 사용하여 집계나 마이크로플로우를 생성할 수 있습니다(police flow 키워드를 사용하여). 아래 그림과 같이 집계를 생성합니다.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

위의 class 문(**police** 명령)은 52MBPS(13000 x 4000 = 52MB)의 버스트를 통해 2000k(20MBPS)의 속도 제한을 설정합니다. 트래픽이 프로필과 일치하고 정격 한도 내에 있는 경우, 작업은 confirm-action 문으로 설정하여 인프로파일 트래픽을 전송하는 것입니다. 트래픽이 프로파일링되지 않은 경우(예: 20MB 제한 위의 예) exceed-action 문은 트래픽을 삭제하도록 설정됩니다(예: 20MB를 초과하는 모든 트래픽은 삭제됨).

마이크로플로우를 구성할 때 유사한 작업이 수행됩니다. 지정된 클래스 맵과 일치하는 포트로 들어오는 모든 흐름을 각각 200K로 제한하려면 해당 플로우의 컨피그레이션은 다음과 유사합니다.

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

DSCP 마크업 맵

DSCP 마크업 맵은 정책을 정의하여 드롭하는 대신 아웃오브프로파일 트래픽을 축소하는 데 사용됩니다. 프로필 외 트래픽은 정의된 버스트 설정을 초과하는 트래픽으로 정의됩니다.

QoS가 활성화되면 기본 DSCP 마크업 맵이 설정됩니다. 이 기본 마크업 맵은 이 테이블에 나열됩니다. 관리자는 CLI를 사용하여 set qos policed-dscp-**map** 명령을 실행하여 기본 **markdown 맵을 수정할 수 있습니다**. 이 예시는 아래와 같습니다.

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

이 예에서는 DSCP 값 32가 DSCP 값 16으로 축소되는 기본 폴리싱된 DSCP 맵의 수정을 정의합니다. 이 폴리서가 정의된 포트의 경우 지정된 버스트를 초과하는 데이터 블록의 일부인 이 DSCP 값을 가진 수신 데이터에는 DSCP 값이 16으로 표시됩니다.

VLAN 및 포트에 정책 매핑(통합 Cisco IOS(기본 모드))

정책이 구축되면 해당 정책을 적용하려면 포트 또는 VLAN에 매핑해야 합니다. CatOS의 커밋 프로세스와 달리 Integrated Cisco IOS(Native Mode)에는 동일한 프로세스가 없습니다. 정책이 인터페이스에 매핑되면 해당 정책이 적용됩니다. 위 정책을 인터페이스에 매핑하려면 다음 명령을 실행합니다.

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

정책이 VLAN에 매핑된 경우, VLAN 정책을 적용할 VLAN의 각 포트에 대해 mls qos vlan **기반** 명령을 실행하여 QoS가 VLAN임을 인터페이스에 알려야 합니다.

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

인터페이스 3/5가 VLAN 100의 일부라고 가정할 때 VLAN 100에 적용된 limit-traffic이라는 정책이 인터페이스 3/5에도 적용됩니다.

CatOS를 사용하여 Catalyst 6000 제품군에 분류 구성

PFC는 L2, L3 및 L4 헤더 정보를 볼 수 있는 ACL을 사용하여 데이터를 분류하는 기능을 지원합니다. SupI 또는 IA(PFC 제외)의 경우, 분류는 포트에서 trust 키워드를 사용하는 것으로 제한됩니다.

다음 섹션에서는 CatOS의 분류를 위해 PFC에서 사용하는 QoS 컨피그레이션 구성 요소에 대해 설명합니다.

COs-DSCP 매핑(CatOS)

스위치로의 인그레스(ingress)에서 프레임은 스위치에서 DSCP 값을 설정합니다. 포트가 신뢰할 수 있는 상태이고 관리자가 trust-COs 키워드를 사용한 경우 프레임에 설정된 COs 값을 사용하여 프레임에 설정된 DSCP 값을 확인합니다. 앞에서 언급했듯이 스위치에서는 내부 DSCP 값에 따라 스위치를 전송할 때 프레임에 서비스 수준을 할당할 수 있습니다.

일부 이전 10/100 모듈(WS-X6248 및 WS-X6348)에서 이 키워드는 지원되지 않습니다. 이러한 모듈의 경우 ACL을 사용하여 수신 데이터에 COs 설정을 적용하는 것이 좋습니다.

QoS가 활성화되면 스위치가 기본 맵을 생성합니다. 이 맵은 COs 값에 따라 설정될 DSCP 값을 식별하는 데 사용됩니다. 이러한 맵은 문서 앞에 있는 이 표에 나열되어 있습니다. 또는 관리자가 고유

한 맵을 설정할 수 있습니다. 이 예시는 아래와 같습니다.

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```

위의 명령은 다음 맵을 설정합니다.

COs	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

위의 맵이 실제 네트워크에서 사용되지는 않지만, 이 명령을 사용하여 무엇을 달성할 수 있는지 파악하는 데 도움이 됩니다.

DSCP 매핑에 대한 IP 우선 순위(CatOS)

DSCP 맵과 마찬가지로 프레임에는 들어오는 패킷 IP 우선순위 설정에서 DSCP 값을 결정할 수 있습니다. 이 문제는 관리자가 포트를 신뢰하도록 설정하고 trust-ipprec 키워드를 사용한 경우에만 발생합니다.

QoS가 활성화되면 스위치가 기본 맵을 생성합니다. 이 맵은 이 문서 앞에 있는 이 표에서 참조됩니다. 이 맵은 IP 우선 순위 값을 기반으로 설정할 DSCP 값을 식별하는 데 사용됩니다. 또는 관리자가 고유한 맵을 설정할 수 있습니다. 이 예제는 다음과 같습니다.

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```

위의 명령은 다음 맵을 설정합니다.

IP 우선 순위	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

위의 맵이 실제 네트워크에서 사용되지는 않지만, 이 명령을 사용하여 무엇을 달성할 수 있는지 파악하는 데 도움이 됩니다.

분류(CatOS)

프레임을 PFC에 전달하여 처리하면 분류 프로세스가 프레임에서 수행됩니다. PFC는 미리 구성된 ACL(또는 기본 ACL)을 사용하여 프레임에 DSCP를 할당합니다. ACE 내에서 4개의 키워드 중 하나를 사용하여 DSCP 값을 할당합니다. 다음과 같습니다.

1. TRUST-DSCP(IP ACL만 해당)
2. TRUST-IPPREC(IP ACL'=s만 해당)
3. TRUST-COS(PFC2의 IPX 및 MAC을 제외한 모든 ACL)
4. DSCP

TRUST-DSCP 키워드는 PFC에 도착하는 프레임에 스위치에 들어가기 전에 DSCP 값이 이미 설정되어 있다고 가정합니다. 스위치에서 이 DSCP 값을 유지합니다.

TRUST-IPPREC를 사용하면 PFC는 ToS 필드에 있는 기존 IP 우선순위 값에서 DSCP 값을 파생시킵니다. PFC는 DSCP 맵에 IP 우선 순위를 사용하여 올바른 DSCP를 할당합니다. 스위치에서 QoS가 활성화된 경우 기본 맵이 생성됩니다. 또는 관리자가 생성한 맵을 사용하여 DSCP 값을 파생시킬 수 있습니다.

TRUST-IPPREC와 마찬가지로 TRUS-COS 키워드는 PFC에 프레임 헤더의 CO에서 DSCP 값을 파생시키도록 지시합니다. DSCP 맵에는 PFC가 DSCP를 파생시키는 데 도움이 되는 CO가 있습니다(관리자가 할당한 기본 중 하나).

DSCP 키워드는 신뢰할 수 없는 포트에서 프레임이 도착하면 사용됩니다. 이는 DSCP를 파생시키는 흥미로운 상황을 나타냅니다. 이 시점에서 set qos acl 문에 구성된 DSCP를 사용하여 DSCP를 파생합니다. 그러나 ACE에 설정된 분류 기준에 따라 트래픽에 대한 DSCP를 파생시키는 데 ACL을 사용할 수 있는 시점입니다. 즉, ACE에서는 트래픽을 식별하기 위해 IP 소스 및 목적지 주소, TCP/UDP 포트 번호, ICMP 코드, IGMP 유형, IPX 네트워크 및 프로토콜 번호, MAC 소스 및 목적지 주소, 이더넷 유형(비 IP 및 비 IPX 트래픽에만 해당)과 같은 분류 기준을 사용할 수 있습니다. 즉, FTP 트래픽을 통한 HTTP 트래픽을 나타내기 위해 특정 DSCP 값을 할당하도록 ACE를 구성할 수 있습니다.

다음 예를 고려하십시오.

```
Console> (enable) set port qos 3/5 trust untrusted
```

포트를 신뢰할 수 없는 상태로 설정하면 PFC가 ACE를 사용하여 프레임에 대한 DSCP를 파생하도록 지시합니다. ACE가 분류 기준으로 구성된 경우 해당 포트의 개별 플로우는 다른 우선 순위로 분류될 수 있습니다. 다음 예제는 다음과 같습니다.

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

이 예제에서는 두 개의 ACE 문을 사용합니다. 첫 번째 는 포트 번호가 80(80 = HTTP)이고 DSCP 값이 32인 TCP 흐름(소스 및 대상 트래픽을 식별하는 데 any 키워드가 사용됨)을 식별합니다. 두 번째 ACE는 임의의 호스트에서 소싱되고 TCP 포트 번호가 21(FTP)인 호스트로 향하는 트래픽을 식별하여 DSCP 값 16을 할당합니다.

통합 Cisco IOS(기본 모드)를 사용하여 Catalyst 6000 제품군에 분류 구성

다음 섹션에서는 Integrated Cisco IOS(Native Mode)를 사용하여 PFC에서 분류를 지원하는 데 사용되는 QoS 구성 요소에 대해 설명합니다.

COs to DSCP 매핑(통합 Cisco IOS(기본 모드))

스위치로의 인그레스(ingress)에서 프레임은 스위치에서 DSCP 값을 설정합니다. 포트가 신뢰할 수 있는 상태이고 관리자가 mls qos trust-COs 키워드(GE 포트 또는 WS-X6548 라인 카드의 10/100 포트)를 사용한 경우 프레임에 설정된 COs 값을 사용하여 프레임에 설정된 DSCP 값을 확인합니다. 앞에서 언급했듯이 스위치에서는 내부 DSCP 값에 따라 스위치를 전송할 때 프레임에 서비스 수준을 할당할 수 있습니다.

QoS가 활성화되면 스위치가 기본 맵을 생성합니다. 기본 설정은 이 표를 참조하십시오. 이 맵은 COs 값에 따라 설정될 DSCP 값을 식별하는 데 사용됩니다. 또는 관리자가 고유한 맵을 설정할 수 있습니다. 이 예시는 아래와 같습니다.

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

위의 명령은 다음 맵을 설정합니다.

COs	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

위의 맵이 실제 네트워크에서 사용되지는 않지만, 이 명령을 사용하여 무엇을 달성할 수 있는지 파악하는 데 도움이 됩니다.

DSCP 매핑에 대한 IP 우선 순위(통합 Cisco IOS(기본 모드))

DSCP 맵과 마찬가지로 프레임에는 들어오는 패킷 IP 우선순위 설정에서 DSCP 값을 결정할 수 있습니다. 이 문제는 관리자가 포트를 신뢰하도록 설정하고 mls qos trust-ipprec 키워드를 사용한 경우에만 발생합니다. 이 키워드는 WS-X6548 라인 카드의 GE 포트 및 10/100 포트에서만 지원됩니다. WS-X6348 및 WS-X6248 라인 카드의 10/100 포트의 경우 ACL을 사용하여 수신 데이터에 IP 우선 순위 트러스트를 할당해야 합니다.

QoS가 활성화되면 스위치가 기본 맵을 생성합니다. 기본 설정은 이 표를 참조하십시오. 이 맵은 IP 우선 순위 값을 기반으로 설정할 DSCP 값을 식별하는 데 사용됩니다. 또는 관리자가 고유한 맵을 설정할 수 있습니다. 이 예시는 아래와 같습니다.

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

위의 명령은 다음 맵을 설정합니다.

IP 우선 순위	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

위의 맵이 실제 네트워크에서 사용되지는 않지만, 이 명령을 사용하여 무엇을 달성할 수 있는지 파악하는 데 도움이 됩니다.

분류(통합 Cisco IOS(기본 모드))

프레임이 PFC에 전달되면 분류 프로세스를 수행하여 들어오는 프레임에 새 우선순위를 지정할 수 있습니다. 여기서 주의할 점은 이 작업은 프레임이 신뢰할 수 없는 포트에서 온 경우 또는 프레임이 신뢰할 수 없는 것으로 분류된 경우에만 수행할 수 있다는 것입니다.

정책 맵 클래스 작업을 사용하여 다음을 수행할 수 있습니다.

1. 신뢰 회사
2. 신뢰 IP 우선 순위
3. 신뢰 DSCP
4. 신뢰 없음

TRUST DSCP 키워드는 PFC에 도착하는 프레임에 스위치에 들어가기 전에 DSCP 값이 이미 설정되어 있다고 가정합니다. 스위치에서 이 DSCP 값을 유지합니다.

TRUST IP-PRECEDENCE를 사용하면 PFC는 ToS 필드에 있는 기존 IP 우선순위 값에서 DSCP 값을 파생시킵니다. PFC는 DSCP 맵에 IP 우선 순위를 사용하여 올바른 DSCP를 할당합니다. 스위치에서 QoS가 활성화된 경우 기본 맵이 생성됩니다. 또는 관리자가 생성한 맵을 사용하여 DSCP 값을 파생시킬 수 있습니다.

TRUST IP-PRECEDENCE와 마찬가지로 TRUST COs 키워드는 PFC에 프레임 헤더의 CO에서

DSCP 값을 파생시키도록 지시합니다. DSCP 맵에는 PFC가 DSCP를 파생시키는 데 도움이 되는 CO가 있습니다(관리자가 할당한 기본 중 하나).

다음은 기존 우선순위(DSCP, IP 우선순위 또는 COs)에서 DSCP를 파생시키는 예입니다.

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

위의 클래스 맵은 이더넷 헤더의 CO에서 DSCP 값을 파생시킵니다.

키워드의 NO TRUST 형식은 신뢰할 수 없는 포트에서 프레임이 도착하면 사용됩니다. 이렇게 하면 폴리싱을 수행하는 동안 프레임에 DSCP 값이 할당됩니다.

다음 정책 정의를 사용하여 PFC에 들어오는 다른 흐름에 새 우선순위(DSCP)를 할당할 수 있는 방법의 다음 예를 고려하십시오.

```
Cat6500(config)# access-list 102 permit tcp any any eq http
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-
c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

위의 예는 다음과 같습니다.

1. 포트로 들어오는 http 흐름을 식별하기 위해 생성되는 ACL입니다.
2. new-dscp-for-flow라는 정책 맵입니다.
3. 이 클래스 맵에서 작업을 수행할 트래픽을 식별하기 위해 액세스 목록 102를 사용하는 클래스 맵(이름 테스트)입니다.
4. 클래스 맵 테스트는 수신 프레임의 신뢰 상태를 신뢰할 수 없음으로 설정하고 해당 흐름에 DSCP 24를 할당합니다.
5. 이 클래스 맵은 모든 http 흐름의 집계를 최대 1MB로 제한합니다.

COPS(Common Open Policy Server)

COPS는 Catalyst 6000 제품군이 원격 호스트에서 QoS를 구성할 수 있도록 하는 프로토콜입니다. 현재 COPS는 CatOS를 사용해서만 지원되며 QoS에 대한 인터세브 아키텍처의 일부입니다. Integrated Cisco IOS(Native Mode)를 사용할 경우 현재 COPS에 대한 지원(이 문서의 날짜 기준)이 없습니다. COPS 프로토콜은 QoS 컨피그레이션 정보를 스위치에 전달하지만 QoS 컨피그레이션 정보의 소스가 아닙니다. COPS 프로토콜을 사용하려면 외부 QoS 관리자가 스위치에 대한 QoS 컨피그레이션을 호스팅해야 합니다. 외부 QoS 관리자는 COPS 프로토콜을 사용하여 스위치로 이러한 컨피그레이션을 하향 푸시합니다. Cisco의 QPM(QoS Policy Manager)은 외부 QoS Manager의 예입니다.

이 문서에서는 QPM의 작업을 설명하려는 것이 아니라 QPM을 사용하여 외부 QoS 컨피그레이션

을 지원하는 스위치에 필요한 컨피그레이션을 설명합니다.

COPS 컨피그레이션

기본적으로 COPS 지원은 비활성화되어 있습니다. 스위치에서 COPS를 사용하려면 활성화해야 합니다. 이 작업은 다음 명령을 실행하여 수행할 수 있습니다.

```
Console> (enable) set qos policy-source cops
!-- QoS policy source for the switch set to COPS. Console> (enable)
```

이 명령이 시작되면 특정 기본 QoS 컨피그레이션 값이 COPS 서버에서 제공됩니다. 여기에는 다음이 포함됩니다.

1. CO에서 대기열 매핑
2. 입력 및 출력 대기열 임계값 할당
3. WRR 대역폭 할당
4. 모든 종합 및 마이크로플로우 정책
5. 이그레스 트래픽에 대한 DSCP-COs 맵
6. ACL
7. 기본 포트 COs 할당

COPS를 사용하여 QoS 컨피그레이션을 수행할 때 이러한 컨피그레이션의 애플리케이션이 다른 방식으로 적용되는지 이해하는 것이 중요합니다. 포트를 직접 구성하는 대신 COPS를 사용하여 포트 ASIC를 구성합니다. 포트 ASIC는 일반적으로 포트 그룹을 제어하므로 COPS 컨피그레이션이 여러 포트에 동시에 적용됩니다.

구성된 포트 ASIC는 GE ASIC입니다. GE 라인 카드에는 GE당 4개의 포트(포트 1-4, 5-8, 9-12, 13-16)가 있습니다. 이러한 라인 카드에서 COPS 컨피그레이션은 각 포트 그룹에 영향을 미칩니다. 10/100 라인 카드(이 문서에서 앞서 설명한 대로)에는 ASIC의 두 그룹, GE와 10/100 ASIC가 있습니다. 10/100 ASIC 4개에 대해 하나의 GE ASIC가 존재합니다. 각 10/100 ASIC는 10/100 포트 12개를 지원합니다. 경찰이 GE ASIC를 구성합니다. 따라서 COPS를 통해 10/100 라인 카드에 QoS 컨피그레이션을 적용할 때 컨피그레이션은 48개의 10/100 포트 모두에 적용됩니다.

set qos policy-**source cops** 명령을 실행하여 COPS 지원을 활성화하면 스위치 섀시의 모든 ASIC에 COS를 통한 QoS 컨피그레이션이 적용됩니다. 특정 ASIC에 COPS 컨피그레이션을 적용할 수 있습니다. 이 작업은 다음 명령을 사용하여 수행할 수 있습니다.

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```

위의 명령 애플리케이션에서 이 명령이 GE 모듈에서 실행된 4개의 포트가 명령의 영향을 받았음을 확인할 수 있습니다.

정책 결정 지점 서버 및 도메인 이름

PDPS(Policy Decision Point Servers)는 스위치에 푸시된 QoS 컨피그레이션 세부사항을 저장하는 데 사용되는 외부 정책 관리자입니다. 스위치에서 COPS가 활성화된 경우 스위치에 QoS 컨피그레이션 세부사항을 제공할 외부 관리자의 IP 주소로 스위치를 구성해야 합니다. 이는 SNMP가 활성화되고 SNMP 관리자 IP 주소가 정의된 경우와 유사합니다.

외부 PDPS를 식별하는 명령은 다음을 사용하여 수행합니다.

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```
위 명령은 디바이스 192.168.1.1을 기본 결정 지점 서버로 식별합니다.

스위치가 PDPS와 통신할 때 PDPS에 정의된 도메인의 일부여야 합니다. PDPS는 정의된 도메인의 일부를 구성하는 스위치에만 통신하므로, 해당 도메인이 속한 COPS 도메인을 식별하도록 스위치를 구성해야 합니다. 이 작업은 다음 명령을 실행하여 수행됩니다.

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```
위의 명령은 remote-cat6k라는 이름의 도메인에 속하도록 구성된 스위치로 표시합니다. 이 도메인은 QPM에서 정의되어야 하며 해당 도메인에 스위치를 추가해야 합니다.

관련 정보

- 스위치 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems
