Catalyst 4000/4500 IOS 기반 수퍼바이저 엔진으로 QOS 폴리싱 및 마킹

목차

소개

Policing 기능은 트래픽 레벨이 지정된 프로필(계약) 내에 있는지 확인합니다. 폴리싱 기능을 사용하면 프로필 외 트래픽을 삭제하거나 트래픽을 다른 DSCP(Differential Services Code Point) 값으로 표시하여 계약 서비스 레벨을 적용할 수 있습니다.DSCP는 패킷의 QoS(Quality of Service) 레벨을 측정합니다.DSCP와 함께 IP 우선 순위 및 CoS(Class of Service)를 사용하여 패킷의 QoS 레벨을 전달합니다.

트래픽 셰이핑과 폴리싱을 혼동해서는 안 됩니다. 둘 다 프로필(계약) 내에 트래픽이 유지되도록 보장합니다. 폴리싱은 트래픽을 버퍼링하지 않으므로 전송 지연은 영향을 받지 않습니다.폴리싱은 아웃오브프로파일(out-of-profile) 패킷을 버퍼링하는 대신 패킷을 삭제하거나 다른 QoS 레벨(DSCP 마크 다운)로 표시합니다. 트래픽 셰이핑은 비프로필 트래픽을 버퍼링하고 트래픽 버스트를 완화하지만 지연 및 지연 변형의 영향을 줍니다.셰이핑은 발신 인터페이스에만 적용할 수 있는 반면, 폴리싱은 수신 및 발신 인터페이스 모두에 적용할 수 있습니다.

Supervisor Engine 3, 4 및 2+(지금부터 이 문서에서 SE3, SE4, SE2+)가 포함된 Catalyst 4000/4500은 수신 및 발신 방향의 폴리싱을 지원합니다.트래픽 셰이핑도 지원되지만 이 문서에서는 폴리싱 및 마킹만 처리합니다.마킹은 정책에 따라 패킷 QoS 레벨을 변경하는 프로세스입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

QoS 폴리싱 및 마킹 매개변수

QoS 정책 맵을 정의하고 포트(포트 기반 QoS) 또는 VLAN(VLAN 기반 QoS)에 적용하여 폴리싱을 설정합니다. 폴리서는 속도 및 버스트 매개변수뿐만 아니라 인프로파일 및 아웃오브프로파일 트래픽에 대한 작업에 의해 정의됩니다.

지원되는 폴리서 유형은 두 가지입니다.집계 및 인터페이스별.각 폴리서는 여러 포트 또는 VLAN에 적용할 수 있습니다.

집계 폴리서는 적용된 모든 포트/VLAN에서 트래픽에 적용됩니다.예를 들어, VLAN 1과 3에서 TFTP(Trivial File Transfer Protocol) 트래픽을 1Mbps로 제한하려면 집계 폴리서를 적용합니다. 이러한 폴리서는 VLAN 1과 3에서 1Mbps의 TFTP 트래픽을 함께 허용합니다.인터페이스별 폴리서를 적용하면 VLAN의 TFTP 트래픽이 각각 1Mbps에서 3Mbps로 제한됩니다.

참고: 패킷에 인그레스(ingress) 및 이그레스(egress) 폴리싱이 모두 적용되는 경우 가장 심각한 결정이 적용됩니다.즉, 인그레스(ingress) 폴리서가 패킷을 삭제하도록 지정하고 이그레스(egress) 폴리서가 패킷을 아래로 표시하도록 지정하면 패킷이 삭제됩니다.표 1은 인그레스(ingress) 및 이그레스(egress) 정책 모두에서 처리하는 경우 패킷에 대한 QoS 작업을 요약합니다.

표 1:인그레스 및 이그레스 정책에 따른 QoS 조치

	Ingress policy			
Egress policy	**Transmit**	**Drop**	**Markdown$_i$**	**Mark$_i$**
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

Catalyst 4000 SE3, SE4, SE2+ QoS 하드웨어는 이그레스(egress) 폴리서 이후에 패킷의 실제 표시가 발생하는 방식으로 구현됩니다.즉, 인그레스 정책에서 패킷(폴리서 표시 다운이나 일반 표시)을 언급하더라도 이그레스 정책은 원래 QoS 레벨로 표시된 패킷을 계속 볼 수 있습니다.이그레스(egress) 정책에서는 패킷을 인그레스(ingress) 정책에 의해 표시되지 않은 것처럼 표시합니다.이는 다음을 의미합니다.

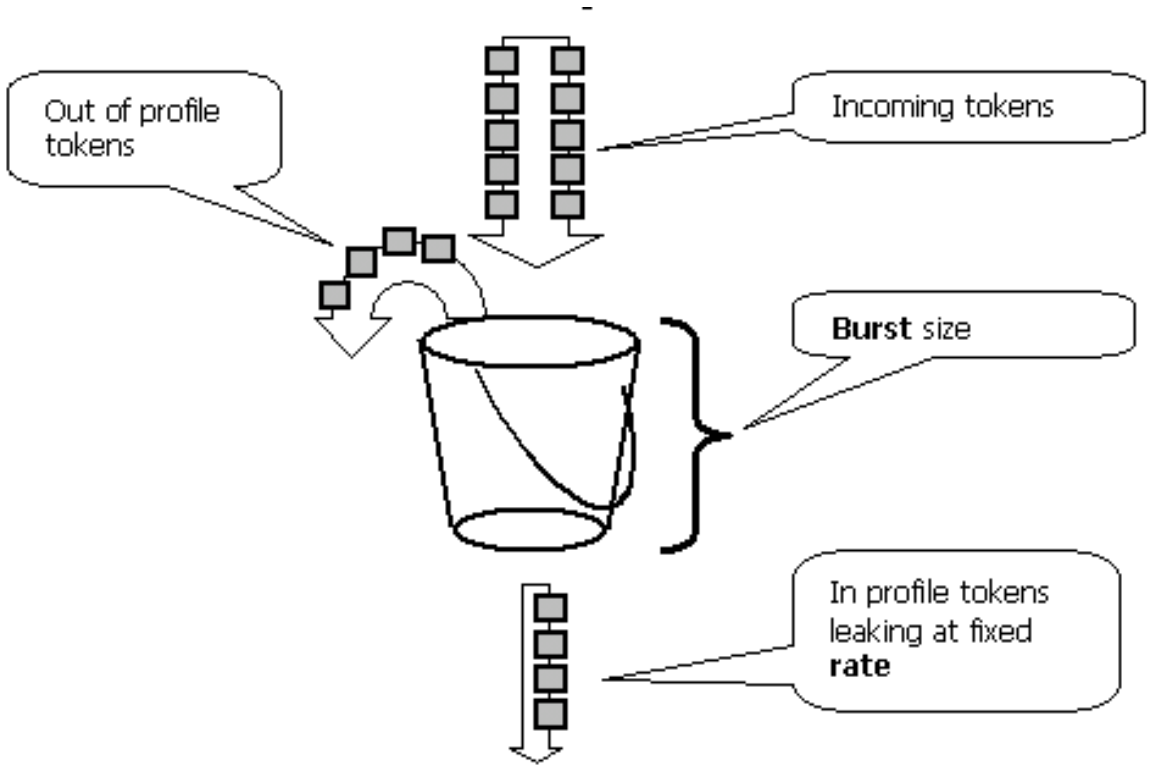
- 이그레스 마킹은 인그레스 마킹을 재정의합니다.
- 이그레스(egress) 정책은 인그레스(ingress) 표시로 변경된 새 QoS 레벨과 일치할 수 없습니다.

기타 중요한 사항은 다음과 같습니다.

- 동일한 정책 내에서 동일한 트래픽 클래스 내에서 표시 및 표시를 할 수 없습니다.
- 집계 폴리서는 방향별로 구성됩니다.즉, 집계 폴리서가 인그레스 및 이그레스 모두에 적용될 경우 입력 및 출력에 각각 하나씩 두 개의 집계 폴리서가 있습니다.
- 정책 내에서 VLAN과 물리적 인터페이스에 집계 폴리서가 적용되면 사실상 VLAN 인터페이스에 대해 하나씩 물리적 인터페이스에 대해 두 개의 집계 폴리서가 적용됩니다.현재, VLAN 인터페이스와 물리적 인터페이스를 전체적으로 폴리싱할 수는 없습니다.

Catalyst 4000 SE3, SE4, SE2+의 폴리싱은 아래의 모델과 같이 Unlequy Bucket 개념을 준수합니다.수신 트래픽 패킷에 해당하는 토큰은 버킷에 배치됩니다(토큰 수 = 패킷 크기). 정기적으로 버킷에서 정의된 토큰 수(구성된 비율에서 파생됨)가 제거됩니다.수신 패킷을 수용하기 위한 버킷에 공

간이 없는 경우 구성된 폴리싱 작업에 따라 패킷은 아웃오브프로파일로 간주되어 삭제되거나 아래로 표시됩니다.



트래픽은 위의 모델에서 나타날 수 있으므로 버킷에서 버퍼링되지 않습니다.실제 트래픽은 버킷을 통해 전혀 이동하지 않습니다.버킷은 패킷이 인프로파일(in-profile)인지 아니면 아웃오브프로파일(out-of-profile)인지 결정하는 데만 사용됩니다.

폴리싱의 정확한 하드웨어 구현은 기능적으로 다르며, 위 모델을 준수합니다.

다음 매개변수는 폴리싱 작업을 제어합니다.

- 속도는 각 간격에서 제거된 토큰 수를 정의합니다.이렇게 하면 폴리싱 비율이 효과적으로 설정됩니다.속도 이하의 모든 트래픽은 인프로파일로 간주됩니다.
- 간격은 버킷에서 토큰이 제거되는 빈도를 정의합니다.간격은 16나노초(16초 *10-9)로 고정됩니다. 간격을 변경할 수 없습니다.
- 버스트는 버킷이 언제든지 보유할 수 있는 토큰의 최대 양을 정의합니다.

Catalyst 6000과 Catalyst 4000 SE3, SE4, SE2+ 간의 버스트 차이점은 이 문서의 끝에 있는 Comparing Policing and Marking on Catalyst 600/4500 IOS Based Supervisor Engine 섹션을 참조하십시오.

폴리서는 임의의 기간(0부터 무한대까지)을 검사할 경우 폴리서가 더 이상 허용하지 않도록 합니다

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

트래픽이 해당 기간 동안 폴리서를 통과했습니다.

Catalyst 4000 SE3, SE4, SE2+ QoS 하드웨어는 폴리싱을 위한 특정 세분성을 가집니다.구성된 속도에 따라, 비율에서 최대 편차는 1.5%입니다.

버스트 속도를 구성할 때 TCP와 같은 일부 프로토콜은 패킷 손실에 반응하는 플로우 제어 메커니즘을 구현한다는 점을 고려해야 합니다.예를 들어, TCP는 손실된 각 패킷에 대해 창을 절반으로 줄

입니다.특정 속도로 폴리싱하면 유효한 링크 사용률이 구성된 속도보다 낮아집니다.더 나은 활용을 위해 버스트를 늘릴 수 있습니다.이러한 트래픽의 좋은 출발점은 버스트를 RTT(Round-Trip Time) 중에 원하는 속도로 보낸 트래픽의 두 배까지 설정하는 것입니다. 동일한 이유로 연결 지향 트래픽으로 폴리서 작업을 벤치마킹하지 않는 것이 좋습니다. 일반적으로 폴리서가 허용한 것보다 성능이 낮기 때문입니다.

참고: 연결 없는 트래픽도 폴리싱에 다르게 반응할 수 있습니다.예를 들어 NFS(Network File System)는 블록을 사용하며, 이는 둘 이상의 UDP(User Datagram Protocol) 패킷으로 구성될 수 있습니다.한 패킷이 삭제되면 여러 패킷(전체 블록)이 재전송될 수 있습니다.

예를 들어, 다음은 폴리싱 속도가 64Kbps이고 TCP RTT가 0.05초인 TCP 세션의 버스트를 계산하는 것입니다.

```
<burst> = 2* <RTT> * <rate> = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800 [bytes]
```

참고: <burst>는 하나의 TCP 세션용이므로 폴리서를 통해 전송되는 예상 세션 수를 평균으로 확장해야 합니다.이것은 예시일 뿐이므로, 각각의 경우 폴리싱 매개변수를 선택하기 위해 트래픽/애플리케이션 요구 사항 및 동작 대 사용 가능한 리소스를 평가해야 합니다.

폴리싱 작업은 패킷을 삭제(drop)하거나 패킷의 DSCP를 변경(마크 다운)하는 것입니다. 패킷을 표시하려면 폴리싱된 DSCP 맵을 수정해야 합니다.기본 폴리싱된 DSCP는 동일한 DSCP에 패킷을 표시합니다. 즉, 마크 다운(no mark down)이 발생하지 않습니다.

참고: 프로파일 이외 패킷이 DSCP로 다운되어 원래 DSCP가 아닌 다른 출력 대기열로 표시될 경우 패킷이 순서가 잘못되어 전송될 수 있습니다.따라서 패킷 순서가 중요한 경우 프로파일 내 패킷과 동일한 출력 대기열에 매핑된 DSCP에 프로파일 외 패킷을 표시하는 것이 좋습니다.

Catalyst 4000/4500 IOS 기반 수퍼바이저 엔진에서 지원되는 폴리싱 및 마킹 기능

Catalyst 4000 SE3, SE4, SE2+에서는 인그레스(수신 인터페이스) 및 이그레스(발신 인터페이스) 폴리싱이 모두 지원됩니다.이 스위치는 1024 인그레스 및 1024 이그레스 폴리서를 지원합니다.2개의 인그레스 및 2개의 이그레스 폴리서가 시스템에서 기본 no-policing 동작을 위해 사용됩니다.

정책 내에서 VLAN 및 물리적 인터페이스에 종합 폴리서가 적용되면 추가 하드웨어 폴리서 항목이 사용됩니다.현재, VLAN 인터페이스와 물리적 인터페이스를 전체적으로 폴리싱할 수는 없습니다.이는 향후 소프트웨어 릴리스에서 변경될 수 있습니다.

모든 소프트웨어 버전에는 폴리싱에 대한 지원이 포함됩니다.Catalyst 4000은 클래스당 최대 8개의 유효한 match 문을 지원하며, 정책 맵당 최대 8개의 클래스가 지원됩니다.유효한 일치 문은 다음과 같습니다.

- 액세스 그룹 일치
- ip dscp 일치
- IP 우선 순위 일치
- 모두 일치

참고: 비 IP V4 패킷의 경우 **match ip dscp** 문이 유일한 분류 방법입니다. 단, 패킷이 CoS를 신뢰하는 트렁킹 포트로 들어오는 경우 가능합니다.내부 DSCP가 일치하면 IP뿐만 아니라 모든 패킷에 적용되므로 match ip **match ip** dscp 명령의 키워드 ip에 의해 속지 마십시오.CoS를 신뢰하도록 포트를 구성하면 L2(802.1Q 또는 ISL 태그 지정) 프레임에서 후자가 추출되고 CoS-DSCP QoS 맵을 사용하여 내부 DSCP로 변환됩니다.그런 다음 match ip dscp를 사용하여 정책에서 이 내부 DSCP 값

을 **일치시킬** 수 있습니다.

유효한 정책 작업은 다음과 같습니다.

- 경찰
- ip dscp 설정
- ip 우선 순위 설정
- 신뢰 SCP
- 신뢰 비용

마킹을 사용하면 분류 또는 폴리싱을 기반으로 패킷의 QoS 레벨을 변경할 수 있습니다.분류는 정의된 기준에 따라 QoS 처리를 위해 트래픽을 다른 클래스로 분할합니다.IP 우선 순위 또는 DSCP와 매칭하려면 해당 수신 인터페이스를 신뢰할 수 있는 모드로 설정해야 합니다.이 스위치는 CoS 신뢰, DSCP 신뢰 및 신뢰할 수 없는 인터페이스를 지원합니다.Trust는 패킷의 QoS 수준이 파생될 필드를 지정합니다.

CoS를 신뢰할 경우 QoS 레벨은 ISL 또는 802.1Q 캡슐화된 패킷의 L2 헤더에서 파생됩니다 .DSCP를 신뢰할 경우 스위치는 패킷의 DSCP 필드에서 QoS 레벨을 파생시킵니다.CoS 신뢰는 트렁킹 인터페이스에서만 의미가 있으며 DSCP를 신뢰하는 것은 IP V4 패킷에만 유효합니다.

인터페이스를 신뢰할 수 없는 경우(QoS가 활성화된 경우 기본 상태), 내부 DSCP는 해당 인터페이스에 대해 구성 가능한 기본 CoS 또는 DSCP에서 파생됩니다.기본 CoS 또는 DSCP가 구성되지 않은 경우 기본값은 0(0)입니다. 패킷의 원래 QoS 레벨이 결정되면 내부 DSCP에 매핑됩니다.표시 또는 폴리싱을 통해 내부 DSCP를 유지하거나 변경할 수 있습니다.

패킷이 QoS 처리를 거친 후 내부 DSCP에서 QoS 레벨 필드(IP의 경우 IP DSCP 필드 내, ISL/802.1Q 헤더 내(있는 경우))가 업데이트됩니다.

패킷의 신뢰할 수 있는 QoS 메트릭을 내부 DSCP로 변환하거나 그 반대로 변환하는 데 사용되는 특수 맵이 있습니다.이러한 맵은 다음과 같습니다.

- 폴리싱된 DSCP에 DSCP;패킷을 아래로 표시할 때 폴리싱된 DSCP를 파생시키는 데 사용됩니다.
- DSCP에서 CoS로:내부 DSCP에서 CoS 레벨을 파생시켜 나가는 패킷 ISL/802.1Q 헤더를 업데이트하는 데 사용됩니다.
- DSCP에 대한 CoS:인터페이스가 트러스트 CoS 모드에 있을 때 수신 CoS(ISL/802.1Q 헤더)에서 내부 DSCP를 파생시키는 데 사용됩니다.

인터페이스가 신뢰 CoS 모드에 있을 때 발신 CoS는 항상 수신 CoS와 동일합니다.이는 Catalyst 4000 SE3, SE4, SE2+의 QoS 구현에 한정됩니다.

폴리싱 구성 및 모니터링

IOS에서 폴리싱을 구성하는 절차는 다음과 같습니다.

1. 폴리서 정의
2. 폴리싱을 위한 트래픽을 선택하는 기준을 정의합니다.
3. 클래스를 사용하여 서비스 정책을 정의하고 지정된 클래스에 폴리서를 적용합니다.
4. 포트 또는 VLAN에 서비스 정책 적용

다음 예를 고려하십시오.포트 5/14에 연결된 트래픽 생성기가 포트 111을 대상으로 최대 17Mbps의 UDP 트래픽을 전송합니다. 이 트래픽을 1Mbps로 폴리싱하고 과도한 트래픽을 삭제해야 합니다.

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

포트가 VLAN 기반 QoS 모드에 있지만 해당 VLAN에 서비스 정책이 적용되지 않을 경우 스위치는 물리적 포트에 적용된 서비스 정책(있는 경우)을 따릅니다.이를 통해 포트 기반 및 VLAN 기반 QoS를 결합할 수 있는 추가적인 유연성을 제공합니다.

지원되는 폴리서 유형은 두 가지입니다.명명된 집계 및 인터페이스별명명된 집계 폴리서는 해당 트래픽이 적용되는 모든 인터페이스에서 결합된 트래픽을 폴리싱합니다.위의 예에서는 명명된 폴리서를 사용했습니다.인터페이스별 폴리서는 명명된 폴리서와 달리 적용된 각 인터페이스에서 트래픽을 개별적으로 폴리싱합니다.인터페이스별 폴리서는 정책 맵 컨피그레이션 내에서 정의됩니다.인터페이스별 집계 폴리서와 함께 다음 예를 고려하십시오.

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

다음 명령은 폴리싱 작업을 모니터링하는 데 사용됩니다.

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
```

```
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

counter near class-map은 해당 클래스와 일치하는 패킷 수를 계산하고 있습니다.

다음과 같은 구현 관련 고려 사항에 유의하십시오.

- 클래스별 패킷 카운터가 인터페이스당 카운터가 아닙니다.즉, 서비스 정책 내에서 이 클래스가 적용되는 모든 인터페이스 간에 클래스와 일치하는 모든 패킷을 계산합니다.
- 폴리서는 패킷 카운터를 유지 관리하지 않으며 바이트 카운터만 지원됩니다.
- 제공된 트래픽 또는 폴리서별 발신 트래픽 속도를 확인하는 특정 명령은 없습니다.
- 카운터는 정기적으로 업데이트됩니다.위 명령을 빠르게 연속하여 반복적으로 실행할 경우 카운터가 여전히 나타날 수 있습니다.

마킹 구성 및 모니터링

마킹을 구성하는 절차는 다음과 같습니다.

1. 트래픽 분류 기준(access-list, DSCP, IP 우선순위 등)을 정의합니다.
2. 이전에 정의된 기준을 사용하여 분류할 트래픽 클래스를 정의합니다.
3. 정의된 클래스에 마킹 작업 및/또는 폴리싱 작업을 연결하는 정책 맵을 만듭니다.
4. 해당 인터페이스에서 신뢰 모드를 구성하는 중입니다.
5. 인터페이스에 정책 맵을 적용합니다.

IP 우선 순위 3의 수신 트래픽이 IP 우선 순위 6에 매핑된 192.168.196.3 UDP 포트 777을 호스트하도록 하려면 다음 예를 고려하십시오. 다른 모든 IP 우선 순위 3 트래픽은 1Mbps로 폴리싱되며 초과 트래픽은 IP 우선 순위 2로 아래쪽으로 표시되어야 합니다.

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
```

```
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
qos map dscp policed 24 to dscp 16
!
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

sh **policy interface** 명령은 마킹을 모니터링하는 데 사용됩니다.샘플 출력 및 결과는 위의 폴리싱 컨피그레이션에 설명되어 있습니다.

Catalyst 6000 및 Catalyst 4000/4500 IOS 기반 수퍼바이저 엔진의 폴리싱 및 마킹 비교

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

관련 정보

- QoS 이해 및 구성
- Technical Support - Cisco Systems