Catalyst 3550에서 QoS 폴리싱 및 마킹 이해

목차

소개

폴리싱 기능은 트래픽 레벨이 지정된 프로파일 또는 계약에 속하는지 여부를 결정하며, 프로파일 외부 트래픽을 삭제하거나 다른 DSCP(Differential Services Code Point) 값으로 표시할 수 있습니다.이는 계약된 서비스 레벨을 적용합니다.

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 폴리싱은 혼동되지 않습니다. 둘 다 트래픽이 프로필 또는 계약 내에 있는지 확인합니다.

폴리싱은 트래픽을 버퍼링하지 않으므로 폴리싱은 전송 지연에 영향을 주지 않습니다.폴리싱은 아웃오브프로파일(out-of-profile) 패킷을 버퍼링하는 대신 이를 삭제하거나 다른 QoS 레벨(DSCP markdown)으로 표시합니다.

트래픽 셰이핑은 비프로필 트래픽을 버퍼링하고 트래픽 버스트를 완화하지만 지연 및 지연 변형의 영향을 줍니다.셰이핑은 발신 인터페이스에만 적용할 수 있으며, 폴리싱은 수신 및 발신 인터페이스 모두에 적용할 수 있습니다.

Catalyst 3550은 수신 및 발신 방향 모두에 대한 폴리싱을 지원합니다.트래픽 셰이핑은 지원되지 않습니다.

마킹하면 정책에 따라 패킷 QoS 레벨이 변경됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

하드웨어 및 소프트웨어 버전

Catalyst 3550의 폴리싱 및 마킹은 모든 소프트웨어 버전에서 지원됩니다.최신 컨피그레이션 가이드가 여기에 나와 있습니다.지원되는 모든 기능은 이 설명서를 참조하십시오.

- QoS 구성

QoS 폴리싱 및 마킹 매개변수

폴리싱을 설정하려면 QoS 정책 맵을 정의하고 포트에 적용해야 합니다.포트 기반 QoS라고도 합니다.

참고: VLAN 기반 QoS는 현재 Catalyst 3550에서 지원되지 않습니다.

폴리서는 속도 및 버스트 매개변수와 비프로필 트래픽에 대한 작업에 의해 정의됩니다.

다음의 두 가지 유형의 폴리서가 지원됩니다.

- 집계
- 개별

집계 폴리서는 적용된 모든 인스턴스에서 트래픽에 적용됩니다.개별 폴리서는 적용된 각 인스턴스 전체의 트래픽에 대해 개별적으로 작동합니다.

참고: Catalyst 3550에서는 동일한 정책의 다른 클래스에만 집계 폴리서를 적용할 수 있습니다.여러 인터페이스 또는 정책의 종합 폴리싱은 지원되지 않습니다.

예를 들어, 동일한 정책 맵에서 class customer1 및 class customer2의 트래픽을 1Mbps로 제한하려면 집계 폴리서를 적용합니다.이러한 폴리서는 customer1 및 customer2 클래스에서 1Mbps의 트래픽을 함께 허용합니다.개별 폴리서를 적용할 경우, 폴리서는 클래스 customer1의 트래픽을 1Mbps로, 클래스 customer2의 경우 1Mbps로 제한합니다.따라서 폴리서의 각 인스턴스는 별개입니다.

이 표에는 인그레스 및 이그레스 정책 모두에서 처리하는 경우 패킷에 대한 QoS 작업이 요약되어

있습니다.

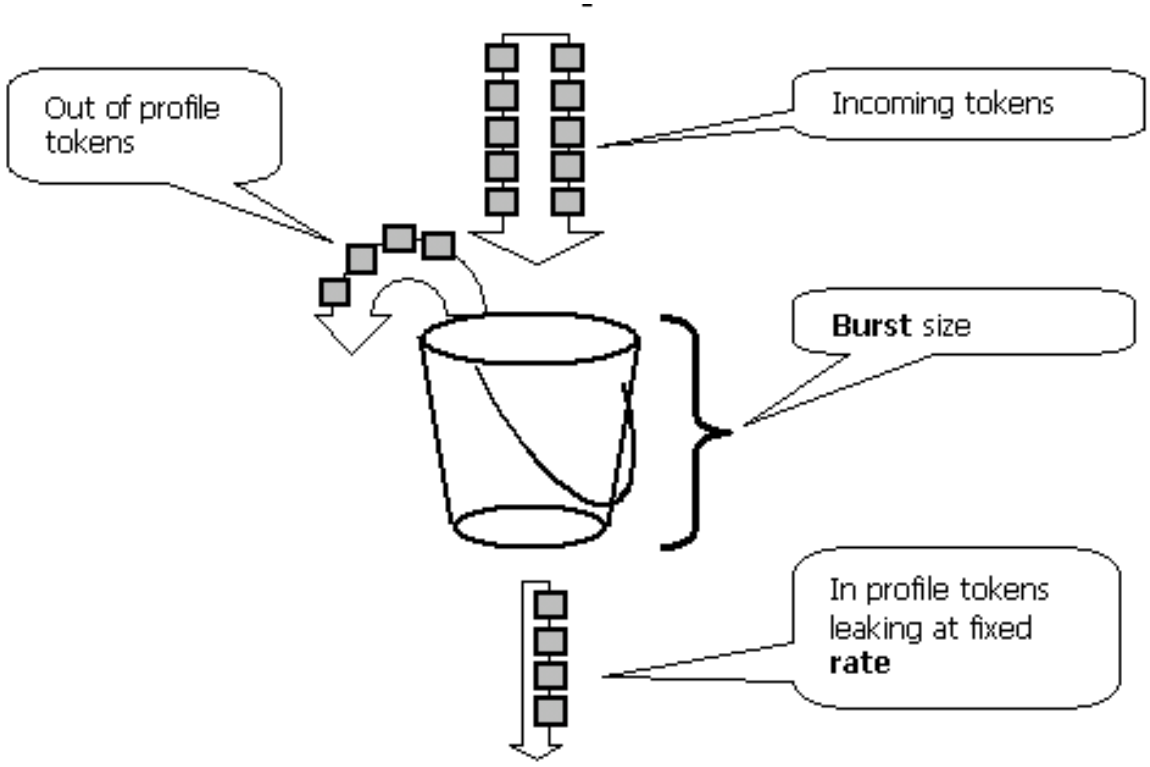
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

참고: 동일한 정책의 동일한 트래픽 클래스 내에서 표시 및 하향 조정이 가능합니다.이 경우 특정 클래스에 대한 모든 트래픽이 먼저 표시됩니다.이미 표시된 트래픽에서 폴리싱 및 마크업이 발생합니다.

Catalyst 3550의 QoS 폴리싱은 이 누수가 있는 버킷 개념을 준수합니다.

수신 트래픽 패킷 크기에 비례하는 토큰 수가 토큰 버킷에 배치됩니다.토큰 수는 패킷의 크기와 같습니다.정기적으로 구성된 비율에서 파생된 정의된 토큰 수가 버킷에서 제거됩니다.수신 패킷을 수용하기 위한 버킷에 공간이 없는 경우 패킷은 아웃오브프로파일로 간주되며 구성된 폴리싱 작업에 따라 삭제되거나 아래로 표시됩니다.

이 개념은 다음 예에 나와 있습니다.



참고: 트래픽은 이 예제에 나타날 수 있으므로 버킷에서 버퍼링되지 않습니다.실제 트래픽은 버킷을 전혀 통과하지 않습니다.버킷은 패킷이 프로필에 있는지 아니면 프로필에서 벗어나는지를 결정하기 위해서만 사용됩니다.

참고: 폴리싱의 하드웨어 구현은 다를 수 있지만 기능상 여전히 이 모델을 준수합니다.

이러한 매개변수는 폴리싱 작업을 제어합니다.

- **속도** - 각 간격에서 제거된 토큰 수를 정의합니다.이렇게 하면 폴리싱 비율이 효과적으로 설정

됩니다.속도 이하의 모든 트래픽은 프로필에서 고려됩니다.지원되는 속도는 8Kbps~2Gbps이며 8Kbps까지 증가합니다.
- **간격** - 버킷에서 토큰이 제거되는 빈도를 정의합니다.간격은 0.125밀리초(또는 초당 8,000회)로 고정됩니다. 이 간격은 변경할 수 없습니다.
- **버스트** - 버킷이 언제든지 보유할 수 있는 토큰의 최대 양을 정의합니다.지원되는 버스트 범위는 8000바이트에서 2000000바이트로, 64바이트로 증가합니다.

참고: 명령줄 도움말 문자열에 큰 범위의 값이 표시되지만 rate-bps 옵션은 구성된 포트 속도를 초과할 수 없으며 burst-byte 옵션은 200000바이트를 초과할 수 없습니다.더 큰 값을 입력하면 인터페이스에 연결할 때 스위치가 정책 맵을 거부합니다.

지정된 트래픽 속도를 유지하려면 버스트가 이 방정식의 합계보다 작아야 합니다.

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

예를 들어, 최소 버스트 값을 계산하여 1Mbps 속도를 유지합니다.속도는 1000Kbps로 정의되므로 필요한 최소 버스트는 이 방정식의 합계입니다.

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

지원되는 최소 버스트 크기는 8000바이트이며, 이는 계산된 최소 버스트보다 큽니다.

참고: 하드웨어 폴리싱 세분화로 인해 정확한 속도와 버스트는 지원되는 가장 가까운 값으로 반올림됩니다.

버스트 속도를 구성할 때 일부 프로토콜은 패킷 손실에 대응하는 메커니즘을 구현한다는 점을 고려해야 합니다.예를 들어, TCP(Transmission Control Protocol)는 손실된 각 패킷에 대해 창을 절반으로 줄입니다.이렇게 하면 TCP가 회선 속도 속도를 가속화하고 폴리서에 의해 조절될 때 TCP 트래픽에서 "톱니" 효과가 발생합니다.톱니 트래픽의 평균 비율을 계산하는 경우 이 속도는 폴리싱된 속도보다 훨씬 낮습니다.그러나 더 효과적으로 활용하려면 버스트를 늘릴 수 있습니다.버스트를 TCP RTT(Round-Trip Time) 중에 원하는 속도로 전송한 트래픽의 양 두 배와 동일하게 설정하는 것이 좋습니다. RTT를 모르는 경우 버스트 매개변수의 값을 두 배로 늘릴 수 있습니다.

같은 이유로 연결 지향 트래픽으로 폴리서 작업을 벤치마킹하지 않는 것이 좋습니다.이 시나리오는 일반적으로 폴리서가 허용한 것보다 낮은 성능을 보여 줍니다.

연결 없는 트래픽도 폴리싱에 다르게 대응할 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 전체 블록까지 많은 패킷이 재전송될 수 있습니다.

이 예에서는 폴리싱 속도가 64Kbps이고 TCP RTT가 0.05초인 경우 TCP 세션에 대한 버스트를 계산합니다.

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

이 예에서 `<burst>` 하나의 TCP 세션용입니다.이 숫자를 폴리서를 통과하는 예상 세션 수를 평균으로 조절합니다.

참고: 이 예시에서는 정책 매개변수를 선택하기 위해 트래픽과 애플리케이션 요구 사항 및 동작 대 사용 가능한 리소스를 평가해야 합니다.

폴리싱 작업은 패킷을 삭제하거나 패킷의 DSCP(markdown)를 변경할 수 있습니다. 패킷을 축소하려면 폴리싱된 DSCP 맵을 수정해야 합니다.기본 폴리싱된 DSCP 맵은 패킷을 동일한 DSCP에 나

타냅니다.따라서 하향 조정이 발생하지 않습니다.

프로파일 이외 패킷이 원래 DSCP와 다른 출력 대기열에 매핑된 DSCP로 다운된 것으로 표시될 경우, 패킷은 주문에서 전송할 수 있습니다.패킷의 순서가 중요한 경우, 프로필 내 패킷과 동일한 출력 대기열에 매핑된 DSCP로 프로파일 외 패킷을 축소합니다.

Catalyst 3550에서 지원되는 폴리싱 및 마킹 기능

이 표에서는 Catalyst 3550에서 지원하는 폴리싱 및 표시 관련 기능에 대한 요약을 방향별로 분류하여 제공합니다.

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

클래스 맵당 하나의 match 문이 지원됩니다.인그레스 정책에 대해 유효한 match 명령문입니다.

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

참고: Catalyst 3550에서는 **match interface** 명령이 지원되지 않으며 클래스 맵에서는 하나의 match 명령만 허용됩니다.따라서 인터페이스를 통해 들어오는 모든 트래픽을 분류하고 단일 폴리서를 사용하여 모든 트래픽을 폴리싱하는 것은 어렵습니다.이 문서의 단일 폴리서 섹션으로 모든 인터페이스 트래픽을 분류하는 방법을 참조하십시오.

이그레스 정책에 대한 유효한 match 문입니다.

- ip dscp 일치

인그레스 정책에 대해 유효한 정책 작업은 다음과 같습니다.

- 경찰
- set ip dscp(표시)
- ip 우선 순위 설정(표시)
- 신뢰 SCP
- 신뢰 ip 우선 순위

- 신뢰 비용

다음 표는 지원되는 인그레스 QoS 정책 매트릭스를 보여줍니다.

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. 이 옵션은 일치 IP 우선 순위도 다룹니다.
2. 이 옵션은 CoS, IP 우선 순위 및 DSCP를 신뢰하는 방법을 다룹니다.
3. 이 옵션은 IP 우선 순위 설정도 다룹니다.

이그레스 정책에 대한 유효한 정책 작업입니다.

- 경찰

다음 표는 지원되는 이그레스 QoS 정책 매트릭스를 보여줍니다.

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

마킹을 사용하면 분류 또는 폴리싱을 기준으로 패킷의 QoS 레벨을 변경할 수 있습니다.분류는 정의된 기준에 따라 QoS 처리를 위해 트래픽을 다른 클래스로 분할합니다.

QoS 처리는 내부 DSCP를 기반으로 합니다.패킷의 QoS 레벨 측정값입니다.내부 DSCP는 트러스트 구성에 따라 파생됩니다.시스템은 신뢰할 수 있는 CoS, DSCP, IP 우선 순위 및 신뢰할 수 없는 인터페이스를 지원합니다.Trust는 각 패킷에 대해 내부 DSCP가 파생되는 필드를 다음과 같이 지정합니다.

- CoS를 신뢰할 경우 QoS 레벨은 ISL(Inter-Switch Link Protocol) 또는 캡슐화된 802.1Q 패킷의 L2(Layer 2) 헤더에서 파생됩니다.
- DSCP 또는 IP 우선 순위를 신뢰하면 시스템은 그에 따라 패킷의 DSCP 또는 IP 우선 순위 필드에서 QoS 레벨을 파생합니다.

CoS를 신뢰하는 것은 트렁킹 인터페이스에서만 의미가 있으며, IP 패킷에 대해서만 DSCP(또는 IP 우선 순위)를 신뢰하는 것이 합리적입니다.

인터페이스를 신뢰할 수 없는 경우 내부 DSCP는 해당 인터페이스의 구성 가능한 기본 CoS에서 파생됩니다.QoS가 활성화된 경우 이 상태가 기본 상태입니다.기본 CoS가 구성되지 않은 경우 기본값은 0입니다.

내부 DSCP가 결정되면 표시 및 폴리싱으로 변경하거나 유지할 수 있습니다.

패킷이 QoS 처리를 거친 후 내부 DSCP에서 해당 QoS 레벨 필드(IP의 IP/DSCP 필드 내, ISL/802.1Q 헤더 내(있는 경우))가 업데이트됩니다.폴리싱과 관련된 다음과 같은 특수한 QoS 맵이 있습니다.

- **DSCP-폴리싱된 DSCP** - 패킷을 축소할 때 폴리싱된 DSCP를 파생시키는 데 사용됩니다.
- **DSCP-to-CoS** - 내부 DSCP에서 CoS 레벨을 파생시켜 나가는 패킷 ISL/802.1Q 헤더를 업데이트하는 데 사용됩니다.
- **CoS-to-DSCP** - 인터페이스가 트러스트 CoS 모드에 있을 때 수신 CoS(ISL/802.1Q 헤더)에서 내부 DSCP를 파생시키는 데 사용됩니다.

다음은 구현별 중요한 고려 사항입니다.

- 인터페이스가 CoS/DSCP 또는 IP 우선 순위와 같은 QoS 메트릭을 신뢰하도록 구성된 경우 인그레스 서비스 정책을 인터페이스에 연결할 수 없습니다.인그레스(ingress)에서 DSCP/IP 우선 순위와 경찰에서 매칭하려면 인터페이스가 아닌 정책 내의 특정 클래스에 대한 신뢰를 구성해야 합니다.DSCP/IP 우선 순위를 기준으로 표시하려면 트러스트를 구성할 필요가 없습니다.
- IP 옵션 및 Ethernet II ARPA(Advanced Research Projects Agency) 캡슐화가 없는 IPv4 트래픽만 하드웨어 및 QoS 관점에서 IP 트래픽으로 간주됩니다.다른 모든 트래픽은 IP가 아닌 것으로 간주되며, IP는 SNAP(SubNetwork Access Protocol) 캡슐화된 IP 및 IPv6과 같은 옵션이 있습니다.
- 비 IP 패킷의 경우 비 IP 트래픽에 대해 DSCP를 확인할 수 없으므로 "match access group"은

유일한 분류 방법입니다.MAC(Media Access Control) ACL(Access List)이 해당 용도로 사용됩니다.패킷은 소스 MAC 주소, 대상 MAC 주소 및 EtherType을 기준으로 매칭할 수 있습니다.IP 트래픽과 MAC ACL을 일치시킬 수 없습니다. 스위치가 IP와 비 IP 트래픽을 구별하기 때문입니다.

폴리싱 구성 및 모니터링

Cisco IOS에서 폴리싱을 구성하려면 다음 단계가 필요합니다.

1. 폴리서 정의(종합 폴리서)
2. 폴리싱을 위한 트래픽을 선택하는 기준 정의
3. 정의된 기준을 사용하여 트래픽을 선택할 클래스 맵을 정의합니다.
4. 클래스를 사용하여 서비스 정책을 정의하고 지정된 클래스에 폴리서를 적용합니다.
5. 포트에 서비스 정책 적용

다음의 두 가지 유형의 폴리서가 지원됩니다.

- 명명된 집계
- 개별

명명된 집계 폴리서는 동일한 정책 내의 모든 클래스에서 조합된 트래픽을 적용되는 위치로 정책합니다.서로 다른 인터페이스 간의 집계 폴리싱은 지원되지 않습니다.

참고: 집계 폴리서는 둘 이상의 정책에 적용할 수 없습니다.이 경우 다음 오류 메시지가 표시됩니다.

```
QoS: Cannot allocate policer for policy map <policy name>
```

다음 예를 고려하십시오.

포트 GigabitEthernet0/3에 연결된 트래픽 생성기가 있으며, 대상 포트 111을 사용하여 약 17Mbps의 UDP 트래픽을 전송합니다. 포트 20의 TCP 트래픽도 있습니다. 이러한 두 트래픽 스트림을 1Mbps로 폴리싱하고 과도한 트래픽을 삭제해야 합니다.다음 예에서는 이 작업을 수행하는 방법을 보여 줍니다.

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
  class cl_udp111
    police aggregate pol_1mbps
  class cl_tcp20
    police aggregate pol_1mbps
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

첫 번째 예에서는 명명된 집계 폴리서를 사용했습니다.개별 폴리서는 명명된 폴리서와 달리 트래픽

이 적용되는 각 클래스에 대해 별도로 트래픽을 정책합니다.개별 폴리서는 정책 맵 컨피그레이션 내에서 정의됩니다.이 예에서는 두 개의 개별 폴리서가 두 개의 트래픽 클래스를 폴리싱합니다 .cl_udp111은 8K 버스트당 1Mbps로 폴리싱되며, cl_tcp20은 32K 버스트당 512Kbps로 폴리싱됩니다.

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

이 명령은 폴리싱 작업을 모니터링하는 데 사용됩니다.

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a        n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

참고: 기본적으로 DSCP당 통계는 없습니다.Catalyst 3550은 최대 8개의 서로 다른 DSCP 값에 대한 인터페이스별 방향 통계 수집을 지원합니다.이는 mls qos monitor 명령을 실행할 때 **구성됩니다** .DSCP 8, 16, 24 및 32에 대한 통계를 모니터링하려면 다음 **인터페이스별** 명령을 실행해야 합니다.

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

참고: mls **qos monitor dscp 8 16 24 32** 명령은 show mls qos int **g0/3 statistics** 명령의 출력을 다음과 같이 변경합니다.

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
```

```
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886      n/a        n/a      0          0
    16: 0              n/a        n/a      0          0          ? per DSCP statistics
    24: 15239542       n/a        n/a      0          0
    32: 539289117      n/a        n/a      536486430  0
Others: 1983055        n/a        n/a      1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

다음은 예제의 필드에 대한 설명입니다.

- **Incoming(수신)** - 각 방향에서 도착하는 패킷 수를 표시합니다.
- **NO_change**—신뢰된 패킷 수를 표시합니다(예: QoS 레벨이 변경되지 않음).
- **Classified**(분류) - 분류 후 이 내부 DSCP에 할당된 패킷 수를 표시합니다.
- **폴리싱됨** - 폴리싱에 의해 중단된 패킷의 수를 표시합니다.DSCP는 하향 조정 전에 표시됩니다 .
- **Dropped(삭제)** - 폴리싱에 의해 삭제된 패킷 수를 표시합니다.

다음과 같은 구현 관련 고려 사항에 유의하십시오.

- mls qos monitor 명령을 실행할 때 8개의 DSCP 값이 구성된 경우 **show mls qos int statistics** 명령을 실행할 때 표시되는 다른 카운터가 부적절한 정보를 표시할 수 있습니다.
- 제공된 트래픽 또는 폴리서별 발신 트래픽 속도를 확인하기 위한 특정 명령은 없습니다.
- 카운터가 하드웨어에서 순차적으로 검색되므로 카운터가 올바르게 추가되지 않을 수 있습니다 .예를 들어, 폴리싱된 패킷, 분류된 패킷 또는 삭제된 패킷의 양은 수신 패킷 수와 약간 다를 수 있습니다.

표시 구성 및 모니터링

마킹을 구성하려면 다음 단계가 필요합니다.

1. 트래픽 분류 기준 정의
2. 이전에 정의된 기준으로 분류할 트래픽 클래스 정의
3. 정의된 클래스에 마킹 작업 및 폴리싱 작업을 연결하는 정책 맵을 만듭니다.
4. 해당 인터페이스를 신뢰 모드로 구성
5. 인터페이스에 정책 맵 적용

이 예에서는 수신 IP 트래픽이 IP 우선순위 6으로 표시되고 폴리싱된 호스트 192.168.192.168에 1Mbps로 연결하고자 합니다.초과 트래픽은 IP 우선 순위 2로 아래쪽으로 표시되어야 합니다.

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all c1_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class c1_2host
```

```
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

마킹을 모니터링하기 위해 동일한 **show mls qos interface statistics** 명령이 실행됩니다.샘플 출력 및 결과는 이 문서의 섹션에 설명되어 있습니다.

단일 폴리서를 사용하여 모든 인터페이스 트래픽을 분류하는 방법

Catalyst 3550에서는 match **interface** 명령이 지원되지 않으며 클래스 맵당 하나의 match 명령만 허용됩니다.뿐만 아니라 Catalyst 3550에서는 MAC ACL과 일치하는 IP 트래픽을 허용하지 않습니다.따라서 IP 트래픽과 비 IP 트래픽은 두 개의 별도의 클래스 맵으로 분류해야 합니다.이렇게 하면 인터페이스로 들어오는 모든 트래픽을 분류하는 것이 어려워지고 단일 폴리서를 사용하여 모든 트래픽을 폴리싱하기가 어려워집니다.여기서 샘플 컨피그레이션을 사용하면 이 작업을 수행할 수 있습니다.이 컨피그레이션에서는 IP 및 비 IP 트래픽이 서로 다른 두 클래스 맵과 일치합니다.그러나 각 트래픽은 두 트래픽 모두에 공통 폴리서를 사용합니다.

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

관련 정보

- Catalyst 3550에서 QoS 구성
- QoS 지원 페이지
- LAN 스위칭 지원 페이지
- LAN 제품 지원 페이지
- 기술 지원 및 문서 – Cisco Systems