Catalyst 6500/6000 Series 스위치의 QoS 폴리싱

목차

소개

네트워크의 QoS 폴리싱은 네트워크 트래픽이 지정된 프로파일(계약)에 속하는지 여부를 결정합니다. 이로 인해 프로필 외 트래픽이 다른 차별화된 서비스 코드 포인트(DSCP) 값으로 삭제되거나 표시되지 않아 계약된 서비스 수준을 적용할 수 있습니다.(DSCP는 프레임의 QoS 레벨을 측정하는 측정값입니다.)

트래픽 폴리싱을 트래픽 셰이핑과 혼동하지 마십시오.둘 다 트래픽이 프로필(계약) 내에 있는지 확인합니다. 트래픽을 폴리싱할 때 프로필 외 패킷을 버퍼링하지 않습니다.따라서 전송 지연에는 영향을 미치지 않습니다.트래픽을 삭제하거나 더 낮은 QoS 레벨(DSCP markdown)으로 표시합니다. 반면 트래픽 셰이핑을 사용하면 프로필에서 벗어난 트래픽을 버퍼링하고 트래픽 버스트를 원활하게 처리할 수 있습니다.이는 지연 및 지연 편차에 영향을 줍니다.아웃바운드 인터페이스에서만 트래픽 셰이핑을 적용할 수 있습니다.인바운드 및 아웃바운드 인터페이스 모두에 폴리싱을 적용할 수 있습니다.

Catalyst 6500/6000 PFC(Policy Feature Card) 및 PFC2는 인그레스 폴리싱만 지원합니다.PFC3는 인그레스 및 이그레스 폴리싱을 모두 지원합니다.트래픽 셰이핑은 OSM(Optical Services Module) 및 FlexWAN 모듈과 같은 Catalyst 6500/7600 시리즈의 특정 WAN 모듈에서만 지원됩니다.자세한 내용은 Cisco 7600 Series Router Module 컨피그레이션 노트를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

QoS 폴리싱 매개변수

폴리싱을 설정하려면 폴리서를 정의하고 이를 포트(포트 기반 QoS) 또는 VLAN(VLAN 기반 QoS)에 적용합니다. 각 폴리서는 프로필 내 및 프로필 외 트래픽에 대한 이름, 유형, 속도, 버스트 및 작업을 정의합니다.Supervisor Engine II의 폴리서도 초과 속도 매개변수를 지원합니다.두 가지 유형의 폴리서가 있습니다.마이크로플로우 및 종합

- **Microflow**(마이크로플로우) - 적용된 각 포트/VLAN에 대한 트래픽을 흐름별로 개별적으로 폴리싱합니다.
- **Aggregate**(집계) - 적용된 모든 포트/VLAN에서 트래픽을 폴리싱합니다.

각 폴리서는 여러 포트 또는 VLAN에 적용할 수 있습니다.플로우는 다음 매개변수를 사용하여 정의됩니다.

- 소스 IP 주소
- 대상 IP 주소
- 레이어 4 프로토콜(예: UDP(User Datagram Protocol))
- 소스 포트 번호
- 대상 포트 번호

정의된 특정 매개변수 집합과 일치하는 패킷이 동일한 흐름에 속한다고 말할 수 있습니다.(이는 NetFlow 스위칭에서 사용하는 것과 기본적으로 동일한 플로우 개념입니다.)

예를 들어, VLAN 1 및 VLAN 3에서 TFTP 트래픽을 1Mbps로 제한하도록 마이크로플로우 정책을 구성하면 VLAN 1의 각 플로우에 대해 1Mbps가 허용되고 VLAN 3의 각 플로우에 대해 1Mbps가 허용됩니다. 즉, VLAN 1에 3개의 플로우와 VLAN 3에 4개의 플로우가 있는 경우 마이크로플로우 폴리서는 각 플로우를 1Mbps로 허용합니다.집계 폴리서를 구성할 경우 VLAN 1과 VLAN 3에서 결합된 모든 플로우에 대한 TFTP 트래픽이 1Mbps로 제한됩니다.

집계 폴리서와 마이크로 플로우 폴리서를 모두 적용할 경우 QoS는 항상 폴리서가 지정한 가장 심각한 조치를 취합니다.예를 들어, 한 폴리서가 패킷을 삭제하도록 지정하지만 다른 폴리서가 패킷을 아래로 표시하도록 지정하면 패킷이 삭제됩니다.

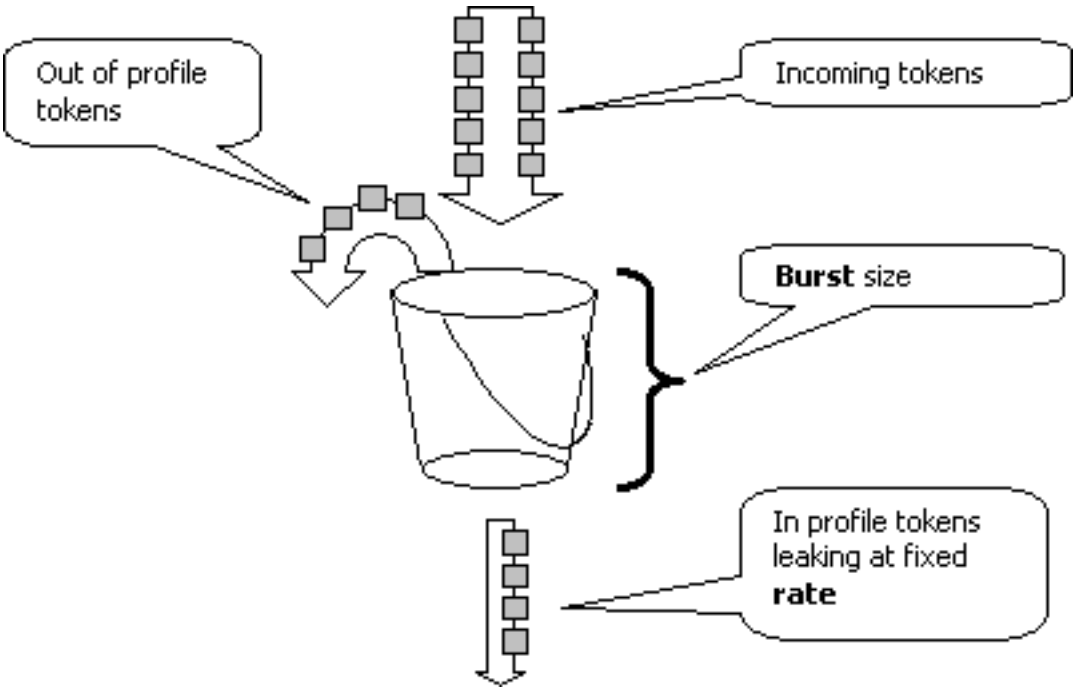
기본적으로 마이크로플로우 폴리서는 라우팅된(레이어 3 [L3]) 트래픽에서만 작동합니다.또한 트래픽을 브리지하려면(L2[Layer 2]) bridged microflow 폴리싱을 활성화해야 합니다.Supervisor Engine II에서는 L3 마이크로플로우 폴리싱에도 bridged microflow 폴리싱을 활성화해야 합니다.

폴리싱은 프로토콜을 인식합니다.모든 트래픽은 다음 세 가지 유형으로 구분됩니다.

- IP
- IPX(Internetwork Packet Exchange)
- 기타

"Leaky bucket" 개념에 따라 Catalyst 6500/6000에서 폴리싱이 구현됩니다.인바운드 트래픽 패킷에

해당하는 토큰이 버킷에 배치됩니다.(각 토큰은 비트를 나타내므로 큰 패킷은 작은 패킷보다 더 많은 토큰으로 표시됩니다.) 일정한 간격으로 정의된 수의 토큰이 버킷에서 제거되어 이동 중에 전송됩니다.인바운드 패킷을 수용하기 위한 버킷에 공간이 없는 경우 패킷은 out-of-profile으로 간주됩니다.구성된 폴리싱 작업에 따라 드롭되거나 다운된 것으로 표시됩니다.



참고: 트래픽은 위의 이미지에 나타날 수 있으므로 버킷에 버퍼링되지 않습니다.실제 트래픽은 전혀 버킷을 통과하지 못합니다.버킷은 패킷이 in-profile 또는 out-of-profile인지 결정하는 데만 사용됩니다.

매개변수 계산

다음과 같은 여러 매개 변수가 토큰 버킷의 작업을 제어합니다.

- **속도** - 각 간격에서 제거된 토큰 수를 정의합니다.이렇게 하면 폴리싱 비율이 효과적으로 설정됩니다.속도 이하의 모든 트래픽은 인프로파일로 간주됩니다.
- **간격** - 버킷에서 토큰이 제거되는 빈도를 정의합니다.간격은 0.00025초로 고정되므로 초당 4,000회 버킷에서 토큰이 제거됩니다.간격을 변경할 수 없습니다.
- **버스트** - 버킷이 한 번에 보유할 수 있는 최대 토큰 수를 정의합니다.지정된 트래픽 속도를 유지하려면 버스트가 해당 간격의 속도 값보다 작아야 합니다.또 다른 고려 사항은 최대 크기의 패킷이 버킷에 맞아야 한다는 것입니다.

버스트 매개변수를 확인하려면 다음 방정식을 사용합니다.

- 버스트 = (Rate [bps]) * 0.00025 [sec/interval]) *또는*(최대 패킷 크기[bits]) 중 더 큰 값.

예를 들어, 이더넷 네트워크에서 1Mbps 속도를 유지하는 데 필요한 최소 버스트 값을 계산하려는 경우 속도가 1Mbps로 정의되고 최대 이더넷 패킷 크기는 1518바이트입니다.방정식은 다음과 같습니다.

- 버스트 = (1,000,000bps * 0.0025) *또는* (1518바이트 * 8비트/바이트) = 250 *또는* 12144.

더 큰 결과는 12144이며, 13kbps까지 회전합니다.

참고: Cisco IOS® Software에서 폴리싱 속도는 Catalyst OS(CatOS)의 kbps와 달리 bps(비트/초)로 정의됩니다. 또한 Cisco IOS Software에서는 버스트 속도가 CatOS의 킬로비트 속도와 반대로 바이

트 단위로 정의됩니다.

참고: 하드웨어 폴리싱 세분화로 인해 정확한 속도와 버스트는 지원되는 가장 가까운 값으로 반올림됩니다.버스트 값이 최대 크기 패킷보다 작지 않아야 합니다.그렇지 않으면 버스트 크기보다 큰 모든 패킷이 삭제됩니다.

예를 들어 Cisco IOS Software에서 버스트를 1518로 설정하려고 하면 1000으로 반올림됩니다.이로 인해 1000바이트보다 큰 모든 프레임이 삭제됩니다.해결책은 버스트를 2000으로 구성하는 것입니다.

버스트 속도를 구성할 때 일부 프로토콜(예: TCP)은 패킷 손실에 반응하는 흐름 제어 메커니즘을 구현한다는 점을 고려하십시오.예를 들어, TCP는 손실된 각 패킷에 대해 윈도우링을 절반으로 줄입니다.따라서 특정 속도로 폴리싱하면 유효한 링크 사용률이 구성된 속도보다 낮습니다.버스트를 증가시켜 활용도를 높일 수 있습니다.이러한 트래픽의 좋은 시작은 버스트 크기를 두 배로 늘리는 것입니다.(이 예에서는 버스트 크기가 13kbps에서 26kbps로 증가합니다.) 그런 다음 성능을 모니터링하고 필요에 따라 추가 조정을 수행합니다.

같은 이유로 연결 지향 트래픽을 사용하여 폴리서 작업을 벤치마킹하지 않는 것이 좋습니다.이는 일반적으로 폴리서가 허용하는 것보다 낮은 성능을 보여줍니다.

경찰 활동

Introduction(소개)에서 언급했듯이, 폴리서는 프로파일 이외 패킷에 다음 두 가지 작업 중 하나를 수행할 수 있습니다.

- 패킷 삭제(컨피그레이션의 `drop` 매개변수)
- 패킷을 더 낮은 DSCP로 표시(컨피그레이션 `policed-dscp` 매개변수)

패킷을 축소하려면 폴리싱된 DSCP 맵을 수정해야 합니다.폴리싱된 DSCP는 기본적으로 동일한 DSCP에 패킷을 명시하도록 설정되어 있습니다. (마크 다운 없음)

참고: "out-of-profile" 패킷이 원래 DSCP와 다른 출력 대기열에 매핑되는 DSCP로 다운된 경우 일부 패킷은 주문에서 전송될 수 있습니다.따라서 패킷의 순서가 중요한 경우 프로필의 수신 패킷과 동일한 출력 대기열에 매핑된 DSCP에 프로파일 외 패킷을 표시하는 것이 좋습니다.

초과 속도를 지원하는 Supervisor Engine II에서는 다음 두 가지 트리거가 가능합니다.

- 트래픽이 정상 속도를 초과하는 경우
- 트래픽이 초과 속도를 초과하는 경우

초과 속도의 적용 사례 중 하나는 정상적인 속도를 초과하는 패킷을 표시하고 초과 속도를 초과하는 패킷을 삭제하는 것입니다.

Catalyst 6500/6000에서 지원되는 폴리싱 기능

소개에 설명된 대로 Supervisor Engine 1a의 PFC1 및 Supervisor Engine 2의 PFC2는 인그레스(인바운드 인터페이스) 폴리싱만 지원합니다.Supervisor Engine 720의 PFC3은 인그레스(ingress) 및 이그레스(아웃바운드 인터페이스) 폴리싱을 모두 지원합니다.

Catalyst 6500/6000은 최대 63개의 마이크로플로우 폴리서와 최대 1,023개의 종합 폴리서를 지원합니다.

Supervisor Engine 1a는 CatOS 버전 5.3(1) 및 Cisco IOS Software 릴리스 12.0(7)XE부터 인그레

스 폴리싱을 지원합니다.

참고: Supervisor Engine 1a를 사용한 폴리싱에는 PFC 또는 PFC2 부속 카드가 필요합니다.

Supervisor Engine 2는 CatOS 버전 6.1(1) 및 Cisco IOS Software 릴리스 12.1(5c)EX부터 인그레스 폴리싱을 지원합니다.Supervisor Engine II는 초과 속도 폴리싱 매개변수를 지원합니다.

DFC(Distributed Forwarding Card)를 사용하는 컨피그레이션은 포트 기반 폴리싱만 지원합니다.또한 집계 폴리서는 시스템별로 계산하지 않고 포워딩 엔진별로 트래픽만 계산합니다.DFC와 PFC는 모두 포워딩 엔진입니다.모듈(라인 카드)에 DFC가 없으면 PFC를 포워딩 엔진으로 사용합니다.

Supervisor Engine 720용 폴리싱 기능 업데이트

참고: Catalyst 6500/6000 QoS 폴리싱에 익숙하지 않은 경우 이 문서의 Catalyst 6500/6000 섹션에서 지원하는 QoS 폴리싱 매개변수 및 폴리싱 기능을 읽으십시오.

Supervisor Engine 720은 다음과 같은 새로운 QoS 폴리싱 기능을 도입했습니다.

- **이그레스 폴리싱**.Supervisor 720은 포트 또는 VLAN 인터페이스에서 인그레스 폴리싱을 지원합니다.포트 또는 L3 라우팅 인터페이스에서 이그레스(egress) 폴리싱을 지원합니다(Cisco IOS System Software의 경우). VLAN의 모든 포트는 포트 QoS 모드(포트 기반 QoS 또는 VLAN 기반 QoS)에 관계없이 이그레스(egress)에서 폴리싱됩니다. 이그레스(egress)에서는 Microflow 폴리싱이 지원되지 않습니다.샘플 컨피그레이션은 CatOS 소프트웨어의 Configure and Monitor Policing 섹션 및 Cisco IOS Software 섹션의 Configure and Monitor Policing 섹션에서 제공됩니다.
- **사용자별 마이크로플로우 폴리싱**.Supervisor 720은 사용자별 마이크로플로우 폴리싱이라고 하는 마이크로플로우 폴리싱의 개선을 지원합니다.이 기능은 Cisco IOS System Software에서만 지원됩니다.지정된 인터페이스 뒤에 있는 각 사용자(IP 주소별)에 대해 특정 대역폭을 제공할 수 있습니다. 이는 서비스 정책 내에 흐름 마스크를 지정하여 수행됩니다.플로우 마스크는 플로우를 구분하는 데 사용되는 정보를 정의합니다.예를 들어 소스 전용 플로우 마스크를 지정하면 하나의 IP 주소에서 오는 모든 트래픽은 하나의 흐름으로 간주됩니다.이 기술을 사용하여 일부 인터페이스(해당 서비스 정책을 구성한 경우)에서 사용자당 트래픽을 폴리싱할 수 있습니다.다른 인터페이스에서 기본 플로우 마스크를 계속 사용합니다.지정된 시간에 시스템에서 최대 2개의 서로 다른 QoS 플로우 마스크를 활성화할 수 있습니다.하나의 플로우 마스크와 하나의 클래스만 연결할 수 있습니다.정책은 최대 두 개의 서로 다른 플로우 마스크를 가질 수 있습니다.

Supervisor Engine 720에서 폴리싱의 또 다른 중요한 변경 사항은 프레임의 L2 길이로 트래픽을 계산할 수 있다는 것입니다.이는 L3 길이로 IP 및 IPX 프레임을 계산하는 Supervisor Engine 2 및 Supervisor Engine 1과 다릅니다.일부 애플리케이션의 경우 L2 및 L3 길이가 일치하지 않을 수 있습니다.한 가지 예는 큰 L2 프레임 내에 있는 작은 L3 패킷입니다.이 경우 Supervisor Engine 720은 Supervisor Engine 1 및 Supervisor Engine 2에 비해 약간 다른 폴리싱된 트래픽 속도를 표시할 수 있습니다.

CatOS 소프트웨어에서 폴리싱 구성 및 모니터링

CatOS에 대한 폴리싱 컨피그레이션은 다음 세 가지 주요 단계로 구성됩니다.

1. 폴리서(정상 트래픽 속도, 초과 속도(해당되는 경우), 버스트 및 폴리싱 작업)를 정의합니다.
2. 경찰에 대한 트래픽을 선택하고 이 ACL에 폴리서를 첨부하기 위해 QoS ACL을 생성합니다.
3. 필요한 포트 또는 VLAN에 QoS ACL을 적용합니다.

이 예에서는 포트 2/8에서 모든 트래픽을 UDP 포트 111로 폴리싱하는 방법을 보여줍니다.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
switch port.
```

다음 예는 같습니다.그러나 이 예에서는 VLAN에 정책을 연결합니다.포트 2/8은 VLAN 20에 속함.

참고: 포트 QoS를 VLAN 모드로 변경해야 합니다.set port **qos** 명령으로 수행합니다.

이 정책은 VLAN 기반 QoS에 대해 구성된 VLAN의 모든 포트에서 트래픽을 평가합니다.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
to VLAN 20.
```

다음으로, DSCP 32로 프로파일 외 패킷을 삭제하는 대신 DSCP가 0인 것으로 표시합니다(최선형).

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

이 예에서는 Supervisor Engine 720에 대해서만 이그레스 폴리싱을 위한 컨피그레이션을 보여 줍니다.VLAN 3~10Mbps 집계에서 모든 발신 IP 트래픽을 감시하는 방법을 보여 줍니다.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
egress_10mbps rate 10000 burst 20 drop !--- This defines
a policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip egress_pol
trust-ipprec aggregate egress_10mbps ip any any !---
This creates the QoS ACL to select traffic and attaches
!--- the policer to the QoS ACL. commit qos acl all !---
This compiles the QoS ACL. set qos acl map egress_pol 3
output !--- This maps the QoS ACL to VLAN 3 in the
output direction.
```

show qos **maps runtime policed-dscp-map을 사용하여** 현재 폴리싱된 DSCP 맵을 확인합니다.

show qos **policer runtime {policer_*name* 사용 | all}** - 폴리서의 매개변수를 확인합니다.폴리서가 연결된 QoS ACL도 볼 수 있습니다.

참고: Supervisor Engine 1과 1a에서는 개별 종합 폴리서에 대한 폴리싱 통계를 가질 수 없습니다.시스템별 폴리싱 통계를 보려면 다음 명령을 사용합니다.

```
Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0
```

마이크로플로우 폴리싱 통계를 확인하려면 다음 명령을 사용합니다.

```
Cat6k> (enable) show mls entry qos short
Destination-IP  Source-IP Port  DstPrt SrcPrt Uptime  Age
--------------- --------------- ----- ------ ------ -------- --------

IP bridged entries:
239.77.77.77 192.168.10.200UDP   63 6300:22:02 00:00:00
Stat-Pkts : 165360
Stat-Bytes : 7606560
Excd-Pkts : 492240
Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP  888 77700:05:38 00:00:00
Stat-Pkts : 42372
Stat-Bytes : 1949112
Excd-Pkts : 126128
Stat-Bkts : 1628

Only out of the profile MLS entries are displayed
Cat6k> (enable)
```

Supervisor Engine II를 사용하면 show qos statistics aggregate-policer 명령을 사용하여 폴리서 단위로 집계 폴리싱 통계를 볼 수 있습니다.

이 예에서는 트래픽 생성기가 포트 2/8에 연결되어 있습니다. 대상 포트 111을 사용하여 17Mbps의 UDP 트래픽을 전송합니다. 폴리서가 트래픽의 16/17을 떨어뜨릴 것으로 예상되므로 1Mbps는 다음 작업을 거쳐야 합니다.

```
Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ ------------- ------------- -------------
udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ ------------- ------------- -------------
udp_1mbps58250497331989733198
```

참고: 허용된 패킷이 65씩 증가했고 초과 패킷이 1090년까지 증가했음을 알 수 있습니다.즉, 폴리서가 1090개의 패킷을 삭제하고 65개의 패킷을 통과하도록 허용했음을 의미합니다.65 / (1090 + 65) = 0.056 또는 약 1/17로 계산할 수 있습니다. 따라서 폴리서가 올바르게 작동합니다.

Cisco IOS Software에서 폴리싱 구성 및 모니터링

Cisco IOS Software에서 폴리싱을 위한 컨피그레이션에는 다음 단계가 포함됩니다.

1. 폴리서를 정의합니다.
2. 경찰로 가는 트래픽을 선택하는 ACL을 생성합니다.
3. ACL 및/또는 DSCP/IP 우선 순위를 가진 트래픽을 선택하려면 클래스 맵을 정의합니다.
4. 클래스를 사용하는 서비스 정책을 정의하고 정책을 지정된 클래스에 적용합니다.
5. 포트 또는 VLAN에 서비스 정책을 적용합니다.

CatOS 소프트웨어에서 폴리싱 구성 및 모니터링 섹션에서 제공되는 예와 동일하지만 현재 Cisco IOS Software에서는 동일한 예를 고려하십시오.이 예에서는 포트 2/8에 연결된 트래픽 생성기가 있습니다. 대상 포트 111을 사용하여 17Mbps의 UDP 트래픽을 전송합니다.

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

Cisco IOS Software에는 두 가지 유형의 집계 폴리서가 있습니다.**이름**과 **인터페이스별**.명명된 종합 폴리서는 해당 정책이 적용되는 모든 인터페이스에서 결합된 트래픽을 정책합니다.위 예제에 사용된 유형입니다.인터페이스별 폴리서는 트래픽이 적용되는 각 인바운드 인터페이스에서 트래픽을 개별적으로 정책합니다.인터페이스별 폴리서는 정책 맵 컨피그레이션 내에서 정의됩니다.인터페이

스별 집계 폴리서가 있는 이 예를 고려해 보십시오.

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit udp any
any eq 111 !--- This defines the ACL to select traffic.
class-map match-all udp_qos match access-group 111 !---
This defines the traffic class to police. policy-map
udp_policy class udp_qos !--- This defines the QoS
policy that attaches the policer to the traffic class.
police 1000000 2000 2000 conform-action transmit exceed-
action drop !--- This creates a per-interface aggregate
!--- policer and applies it to the traffic class.
interface GigabitEthernet2/8 switchport service-policy
input udp_policy !--- This applies the QoS policy to an
interface.
```

Microsoft Flow Policer는 인터페이스별 집계 폴리서와 마찬가지로 정책 맵 컨피그레이션 내에서 정의됩니다.아래 예에서는 VLAN 2로 들어오는 호스트 192.168.2.2의 모든 플로우가 100kbps로 폴리싱됩니다.192.168.2.2의 모든 트래픽은 폴리싱되어 총 500kbps로 전송됩니다.VLAN 2에는 인터페이스 fa4/11 및 fa4/12가 포함됩니다.

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 1 permit 192.168.2.2
!--- This defines the access list to select traffic from
host 192.168.2.2. class-map match-all host_2_2 match
access-group 1 !--- This defines the traffic class to
police. policy-map host class host_2_2 !--- This defines
the QoS policy. police flow 100000 2000 conform-action
transmit exceed-action drop !--- This defines a
microflow policer. For the calculation of rate and !---
burst, refer to Calculate Parameters. police 500000 2000
2000 conform-action transmit exceed-action drop !---
This defines the aggregate policer to limit !--- traffic
from the host to 500 kbps aggregate. interface fa4/11
mls qos vlan-based interface fa4/12 mls qos vlan-based
!--- This configures interfaces in VLAN 2 for VLAN-based
QoS. interface vlan 2 service-policy input host !---
This applies the QoS policy to VLAN 2.
```

아래 예는 Supervisor Engine 720에 대한 이그레스 폴리싱을 위한 컨피그레이션을 보여줍니다. Gigabit Ethernet 8/6~100kbps 인터페이스에서 모든 아웃바운드 트래픽의 폴리싱을 설정합니다.

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select traffic. All IP
traffic is subject to policing. class-map match-all
cl_out match access-group 111 !--- This defines the
traffic class to police. policy-map pol_out class cl_out
police 100000 3000 3000 conform-action transmit exceed-
action drop !--- This creates a policer and attaches it
to the traffic class. interface GigabitEthernet8/6 ip
address 3.3.3.3 255.255.255.0 service-policy output
```

```
pol_out !--- This attaches the policy to an interface.
```

아래 예는 Supervisor Engine 720에 대한 사용자별 폴리싱에 대한 컨피그레이션을 보여줍니다. 포트 1/1 뒤에 있는 사용자가 인터넷으로 들어오는 트래픽은 사용자당 1Mbps로 폴리싱됩니다.인터넷에서 사용자에게 보내는 트래픽은 사용자당 5Mbps로 폴리싱됩니다.

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select user traffic. class-
map match-all cl_out match access-group 111 !--- This
defines the traffic class for policing. policy-map
pol_out class cl_out police flow mask src-only 1000000
32000 conform-act transmit exceed-act drop
!--- Only the source IP address is considered for flow
creation !--- on interfaces with this policy attached.
interface gigabit 1/1 !--- 1/1 is the uplink toward the
users. service-policy input pol_out !--- Traffic comes
in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
dest-only 5000000 32000 conform-act transmit exceed-act
drop
!--- Only the destination IP address is considered for
flow creation !--- on interfaces with this policy
attached. interface gigabit 1/2 !--- 1/2 is the uplink
to the Internet. service-policy input pol_in
```

폴리싱을 모니터링하려면 다음 명령을 사용할 수 있습니다.

```
bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS global counters:
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0

bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127451  2129602


bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127755  2134670
```

참고: 허용된 패킷은 304개 증가했으며 초과 패킷은 5068년까지 증가했습니다.즉, 폴리서가

5068개의 패킷을 삭제하고 304개의 패킷을 통과하도록 허용했음을 의미합니다.입력 속도가 17Mbps인 경우 폴리서가 트래픽의 1/17을 통과해야 합니다.삭제된 패킷과 전달된 패킷을 비교하면 다음과 같은 경우가 있습니다.304 / (304 + 5068) = 0.057 또는 약 1/17입니다. 하드웨어 폴리싱 세분화로 인해 일부 사소한 변형이 가능합니다.

마이크로플로우 폴리싱 통계의 경우 show mls **ip detail** 명령을 사용합니다.

```
Orion# show mls ip detail
IP Destination IP Source        Protocol L4 Ports     Vlan Xtag L3-protocol
--------------+---------------+--------+-------------+----+----+-----------+
192.168.3.33192.168.2.2udp555 / 5550   1ip
192.168.3.3192.168.2.2udp63 / 630   1ip

[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes
--------------+-------------+-------+--------------+-----------------+------------+
Fa4/11 - ----ARPA3    0030.7137.1000  0000.3333.3333314548
Fa4/11 - ----ARPA3    0030.7137.1000  0000.2222.2222314824

Packets     Age   Last SeenQoS      Police Count ThresholdLeak
------------+-----+---------+-----------+------------+---------+-----------+
6838     36   18:50:090x80  34619762*2^5 3*2^0
6844     36   18:50:090x80  34669562*2^5 3*2^0

Drop Bucket  Use-Tbl Use-Enable
----+-------+-------+----------+
YES   1968     NONO
YES   1937     NONO
```

참고: Police `Count` 필드에는 플로우당 폴리싱된 패킷 수가 표시됩니다.

관련 정보

- QoS 구성
- Catalyst 6000 제품군 스위치의 서비스 품질 이해
- LAN 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems