CatOS 소프트웨어를 실행하는 Catalyst 6500/6000 Series 스위치의 QoS 분류 및 마킹

목차

소개

이 문서에서는 Catalyst 6000 섀시 내에서 패킷이 이동하는 동안 다른 위치에서 패킷의 마킹 및 분류와 관련하여 어떤 일이 발생하는지 살펴봅니다.특별 사례, 제한 사항을 언급하고 짧은 사례 연구를 제공합니다.

이 문서는 QoS(Quality of Service) 또는 마킹과 관련된 모든 Catalyst OS(CatOS) 명령의 전체 목록이 아닙니다.CatOS CLI(command-line interface)에 대한 자세한 내용은 다음 문서를 참조하십시오.

- QoS 구성

참고: 이 문서에서는 IP 트래픽만 고려합니다.

시작하기 전에

표기 규칙

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

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 CatOS 소프트웨어를 실행하는 Catalyst 6000 제품군 스위치와 다음 수퍼바이저 엔진 중 하나를 사용하는 경우에 유효합니다.

- SUP1A + PFC
- SUP1A + PFC + MSFC
- SUP1A + PFC + MSFC2
- SUP2 + PFC2
- SUP2 + PFC2 + MSFC2

그러나 모든 샘플 명령은 소프트웨어 버전 6.3을 실행하는 SUP1A/PFC가 포함된 Catalyst 6506에서 시도되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

용어

다음은 이 문서에서 사용되는 용어 목록입니다.

- DSCP(Differentiated Services Code Point):IP 헤더에 있는 ToS(Type of Service) 바이트의 처음 6비트입니다.DSCP는 IP 패킷에만 있습니다.**참고:** 또한 모든 패킷(IP 또는 비 IP)에 내부 DSCP를 할당하면 이 내부 DSCP 할당은 이 문서의 뒷부분에 자세히 설명되어 있습니다.
- IP 우선 순위:IP 헤더에 있는 ToS 바이트의 처음 3비트입니다.
- CoS(Class of Service):레이어 2(L2)에서 패킷을 표시하는 데 사용할 수 있는 유일한 필드입니다. 다음 3비트로 구성됩니다.IEEE dot1q 패킷에 대한 dot1q 태그의 3개의 dot1p 비트ISL 캡슐화된 패킷의 ISL(Inter-Switch Link) 헤더에 있는 "User Field"라는 세 비트가 있습니다.non-dot1q 또는 ISL 패킷에는 CoS가 없습니다.
- 분류:표시할 트래픽을 선택하는 데 사용되는 프로세스입니다.
- 표시:패킷에서 레이어 3(L3) DSCP 값을 설정하는 프로세스입니다.이 문서에서 마킹 정의는 L2 CoS 값 설정을 포함하도록 확장됩니다.

Catalyst 6000 제품군 스위치는 다음 세 가지 매개변수를 기준으로 분류할 수 있습니다.

- DSCP

- IP 우선 순위
- CoS

Catalyst 6000 제품군 스위치는 다른 장소에서 분류 및 표시를 하고 있습니다.다음은 이러한 다양한 장소에서 발생하는 상황을 보여 주는 것입니다.

- 입력 포트(인그레스 ASIC(Application-Specific Integrated Circuit))
- 스위칭 엔진(PFC(Policy Feature Card))
- 출력 포트(이그레스 ASIC)

QoS 활성화

기본적으로 QoS는 Catalyst 6000 스위치에서 비활성화됩니다.CatOS 명령 **집합** qos enable을 실행하여 QoS를 활성화할 수 **있습니다**.

QoS를 비활성화하면 스위치에서 수행하는 분류 또는 표시가 없으며, 따라서 모든 패킷은 스위치를 입력할 때 가졌던 DSCP/IP 우선 순위를 스위치에 둡니다.

입력 포트 처리

분류와 관련된 인그레스 포트의 기본 컨피그레이션 매개변수는 포트의 신뢰 상태입니다.시스템의 각 포트는 다음 신뢰 상태 중 하나를 가질 수 있습니다.

- 신뢰 IP 우선 순위
- 신뢰 DSCP
- 신뢰 비용
- 신뢰

이 섹션의 나머지 부분에서는 포트 신뢰 상태가 패킷의 최종 분류에 미치는 영향에 대해 설명합니다.다음 CatOS 명령을 사용하여 포트 신뢰 상태를 설정하거나 변경할 수 있습니다.

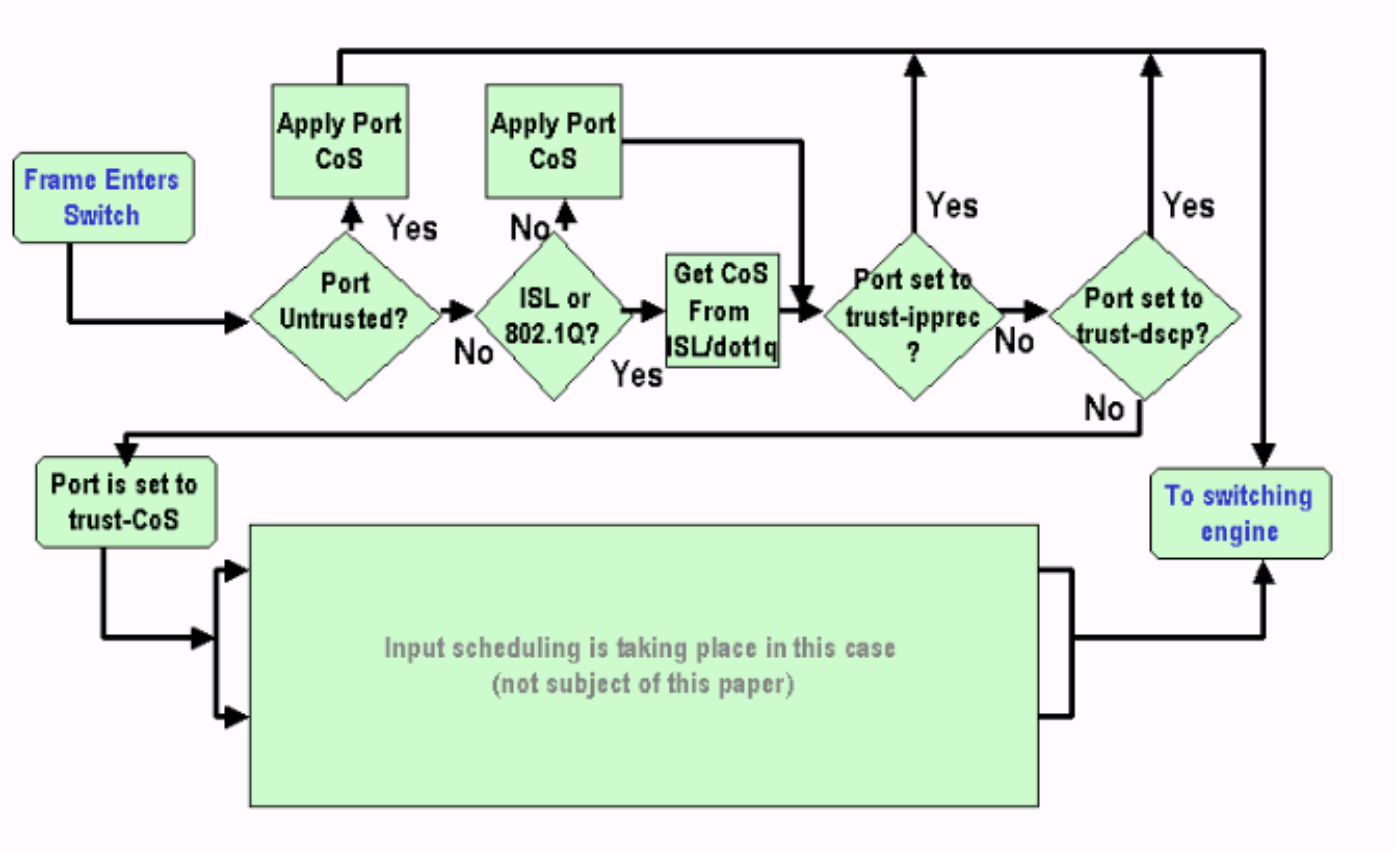
포트 qos *mod/port* trust {untrusted 설정 | trust-cos | trust-ipprec | trust-dscp }

참고: 기본적으로 QoS가 활성화된 경우 모든 포트는 신뢰할 수 없는 상태입니다.

입력 포트 레벨에서 다음 예와 같이 포트당 기본 CoS를 적용할 수도 있습니다.

포트 qos *mod/port* cos-*value 설정*

포트가 신뢰할 수 없는 상태로 설정된 경우, 포트 기본 CoS로 프레임을 표시하고 PFC(스위칭 엔진)에 헤더를 전달합니다. 포트가 신뢰 상태 중 하나로 설정된 경우 기본 포트 CoS를 적용하거나(프레임에 수신 CoS(dot1q 또는 ISL)가 없는 경우) CoS를 그대로 유지하고(dot1q 및 ISL 프레임의 경우) 프레임을 스위칭 엔진에 전달합니다.입력 분류는 다음 순서도에 표시됩니다.



참고: 위 흐름도에 표시된 것처럼 각 프레임에는 실제 CoS를 전달하지 않는 태그 없는 프레임을 포함하여 내부 CoS(수신된 CoS 또는 기본 포트 CoS)가 할당됩니다.이 내부 CoS 및 수신된 DSCP는 특수 패킷 헤더(데이터 버스 헤더라고 함)에 기록되고 데이터 버스를 통해 스위칭 엔진으로 전송됩니다.이는 인그레스 라인 카드에서 발생하며 이 시점에서 이 내부 CoS를 이그레스 ASIC로 전달하여 발신 프레임에 삽입할지 여부는 아직 알려지지 않습니다.이 모든 작업은 PFC가 수행하는 작업에 따라 다르며 다음 섹션에서 자세히 설명합니다.

PFC(스위칭 엔진)

헤더가 스위칭 엔진에 도달하면 스위칭 엔진 EARL(Encoded Address Recognition Logic)이 각 프레임에 내부 DSCP를 할당합니다.이 내부 DSCP는 PFC가 스위치를 전송할 때 프레임에 할당된 내부 우선 순위입니다.이는 IPv4 헤더의 DSCP가 아닙니다.기존 CoS 또는 ToS 설정에서 파생되며 프레임이 스위치를 종료할 때 CoS 또는 ToS를 재설정하는 데 사용됩니다.이 내부 DSCP는 PFC에 의해 스위치드(또는 라우팅됨)된 모든 프레임에 할당되며 IP가 아닌 프레임에도 할당됩니다.

내부 DSCP에 대한 4개의 가능한 소스

내부 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. 수신 CoS 비트는 스위치로 들어가는 프레임 이전에 이미 설정되었거나 수신 프레임에 CoS가 없는 경우 수신 포트의 기본 CoS에서 설정되었습니다.IP 우선 순위와 마찬가지로 최대 8개의 CoS 값이 있으며 각 값은 64개의 DSCP 값 중 하나에 매핑되어야 합니다.이 맵을 구성하거나, 스위치가 이미 있는 기본 맵을 사용할 수 있습니다.

4. DSCP는 일반적으로 ACL(Access Control List) 항목을 통해 할당된 DSCP 기본값을 사용하여 프레임에 대해 설정할 수 있습니다.

Nos용위의 목록에서 2 및 3은 기본적으로 사용되는 정적 매핑입니다.

- DSCP 파생은 CoS와 DSCP 매핑의 경우 8배입니다.
- DSCP 파생은 IP 우선 순위의 8배이며, IP 우선 순위는 DSCP 매핑에 해당합니다.

이 정적 매핑은 다음 명령을 실행하여 사용자가 재정의할 수 있습니다.

qos ipprec-dscp-map <dscp1> <dscp2> 설정...<dscp8>

qos cos-dscp-map <dscp1> <dscp2> 설정...<dscp8>

CoS(또는 IP 우선 순위)에 대한 매핑에 해당하는 DSCP의 첫 번째 값은 "0"이고, CoS(또는 IP 우선 순위)의 두 번째 값은 "1"이며, 이 패턴을 계속 진행합니다.

내부 DSCP에 사용할 수 있는 4가지 소스 중 어떤 소스가 사용됩니까?

이 섹션에서는 위에서 설명한 네 가지 가능한 소스 중 각 패킷에 사용할 소스를 결정하는 규칙에 대해 설명합니다.다음 매개변수에 따라 다릅니다.

1. 패킷에 어떤 QoS ACL이 적용됩니까?이는 다음 규칙에 의해 결정됩니다.**참고:** 각 패킷은 ACL 항목을 거칩니다.수신 포트 또는 VLAN에 연결된 ACL이 없는 경우 기본 ACL을 적용합니다.수신 포트 또는 VLAN에 연결된 ACL이 있고 트래픽이 ACL의 항목 중 하나와 일치하는 경우 이 항목을 사용합니다.수신 포트 또는 VLAN에 연결된 ACL이 있고 트래픽이 ACL의 항목 중 하나와 일치하지 *않는* 경우 기본 ACL을 사용합니다.
2. 각 항목에는 classification 키워드가 포함되어 있습니다.다음은 가능한 키워드 및 설명 목록입니다.trust-ipprec:내부 DSCP는 포트 신뢰 상태에 관계없이 정적 매핑에 따라 수신 IP 우선 순위에서 파생됩니다.트러스트 DSCP:내부 DSCP는 포트 트러스트 상태에 관계없이 수신된 DSCP에서 파생됩니다.trust-cos:포트 신뢰 상태가 신뢰할 수 있는 경우 내부 DSCP는 정적 매핑에 따라 수신된 CoS에서 파생됩니다(trust-cos, trust-dscp, trust-ipprec). 포트 신뢰 상태가 trust-xx이면 동일한 정적 매핑에 따라 기본 포트 CoS에서 DSCP가 파생됩니다.dscp *xx*:내부 DSCP는 다음 수신 포트 신뢰 상태에 따라 달라집니다.포트를 신뢰할 수 없는 경우 내부 DSCP가 *xx*로 설정됩니다.포트가 trust-dscp이면 내부 DSCP가 수신 패킷에서 수신된 DSCP가 됩니다.포트가 trust-CoS인 경우 내부 DSCP는 수신된 패킷의 CoS에서 파생됩니다.포트가 trust-ipprec인 경우 내부 DSCP는 수신된 패킷의 IP 우선 순위에서 파생됩니다.
3. 각 QoS ACL은 포트 또는 VLAN에 적용할 수 있지만, 고려해야 할 추가 컨피그레이션 매개변수가 있습니다.ACL 포트 유형.포트는 VLAN 기반 또는 포트 기반으로 구성할 수 있습니다.다음은 두 가지 구성 유형에 대한 설명입니다.VLAN 기반으로 구성된 포트는 포트가 속한 VLAN에 적용된 ACL만 찾습니다.포트에 연결된 ACL이 있으면 해당 포트에서 들어오는 패킷에 대해 ACL이 무시됩니다.VLAN에 속한 포트가 포트 기반으로 구성된 경우, 해당 VLAN에 연결된 ACL이 있더라도 해당 포트에서 들어오는 트래픽에 대해서는 고려되지 않습니다.

다음은 IP 트래픽을 표시하기 위한 QoS ACL을 생성하는 구문입니다.

qos acl ip *acl_name* **[dscp xx 설정 | trust-cos | trust-dscp | trust-ipprec]** *acl 항목 규칙*

다음 ACL은 호스트 1.1.1.1으로 전달된 모든 IP 트래픽을 DSCP가 "40"인 상태로 표시하고 다른 모든 IP 트래픽에 대해 trust-dscp를 표시합니다.

qos acl TEST_ACL dscp 40 ip any host 1.1.1.1 설정

qos acl TEST_ACL trust-dscp ip any 설정

ACL이 생성되면 이를 포트 또는 VLAN에 매핑해야 합니다. 다음 명령을 실행하여 이 작업을 수행할 수 있습니다.

qos acl 맵 acl_*name* 설정 [모듈/포트 | VLAN]

기본적으로 각 포트는 ACL에 대한 포트 기반이므로 VLAN에 ACL을 연결하려면 이 VLAN의 포트를 vlan 기반으로 구성해야 합니다.이 작업은 다음 명령을 실행하여 수행할 수 있습니다.

포트 qos *모듈/포트* vlan 기반 설정

다음 명령을 실행하여 포트 기반 모드로 되돌릴 수도 있습니다.

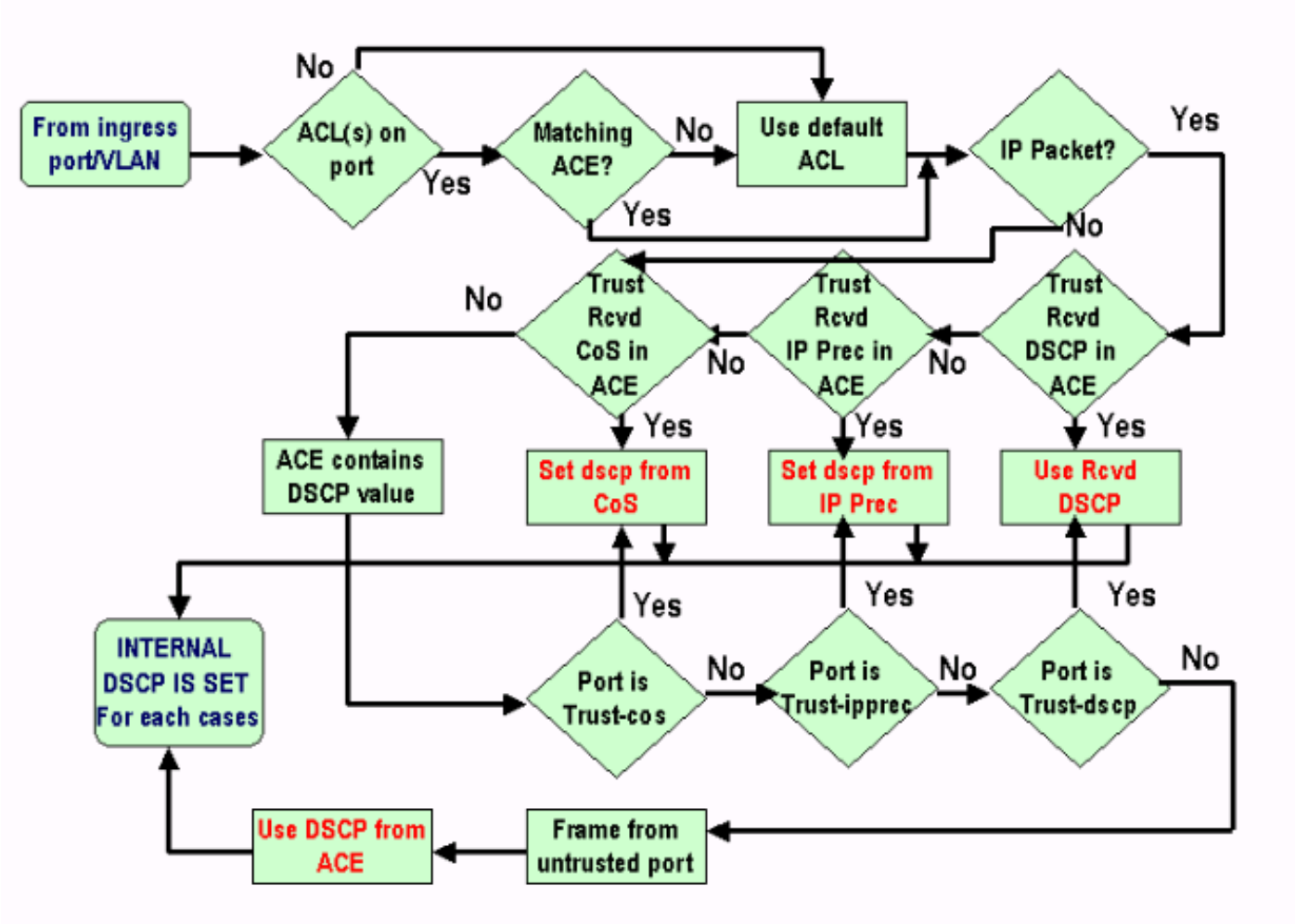
포트 qos *모듈/포트* 포트 기반 설정

요약:내부 DSCP는 어떻게 선택됩니까?

내부 DSCP는 다음 요소에 따라 달라집니다.

- 포트 신뢰 상태
- 포트에 연결된 ACL
- 기본 ACL
- ACL과 관련하여 VLAN 기반 또는 포트 기반

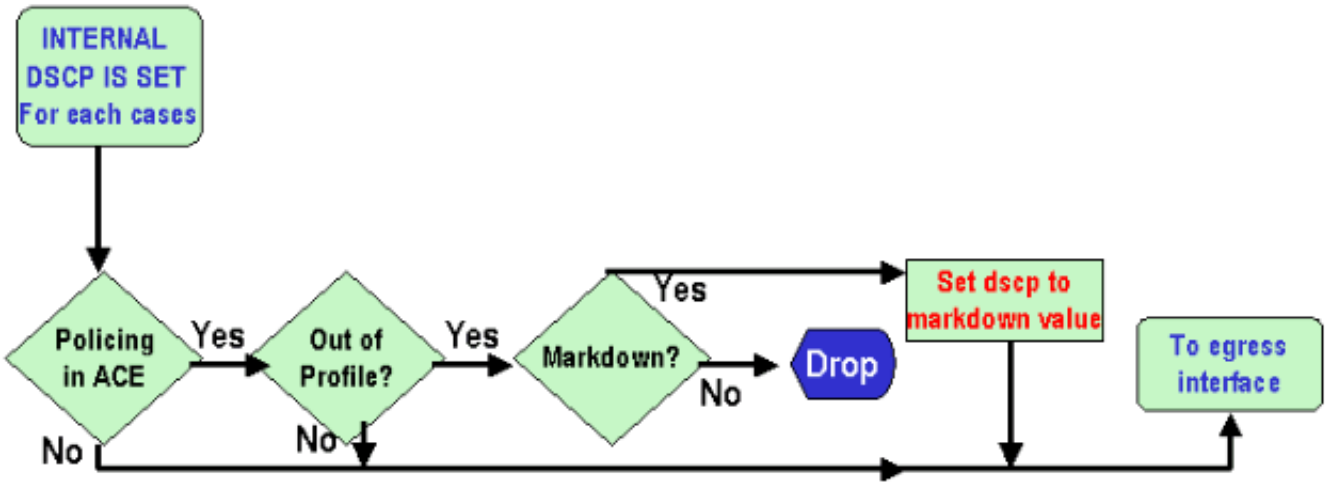
다음 순서도에 따라 내부 DSCP를 선택하는 방법이 요약되어 있습니다.



PFC는 폴리싱을 수행할 수도 있습니다.결국 내부 DSCP가 표시되지 않을 수 있습니다.폴리싱에 대한 자세한 내용은 다음 문서를 참조하십시오.

- Catalyst 6000의 QoS 폴리싱

다음 순서도는 폴리서가 적용되는 방법을 보여줍니다.



출력 포트 처리

이그레스 포트 레벨에서 분류를 변경하기 위해 수행할 수 있는 작업은 없지만 이 섹션에서는 다음 규칙에 따라 패킷을 표시합니다.

- 패킷이 IPv4 패킷인 경우 스위칭 엔진에서 할당한 내부 DSCP를 IPv4 헤더의 ToS 바이트로 복사합니다.
- 출력 포트가 ISL 또는 dot1q 캡슐화를 위해 구성된 경우 내부 DSCP에서 파생된 CoS 를 사용하여 ISL 또는 dot1q 프레임에 복사합니다.

참고: CoS는 다음 명령을 실행하는 사용자가 구성한 정적에 따라 내부 DSCP에서 파생됩니다.

참고: qos dscp-cos-map dscp_*list:cos_value* 설정

참고: 기본 구성은 다음과 같습니다.기본적으로 CoS는 DSCP의 정수 부분으로 8로 나누어집니다.

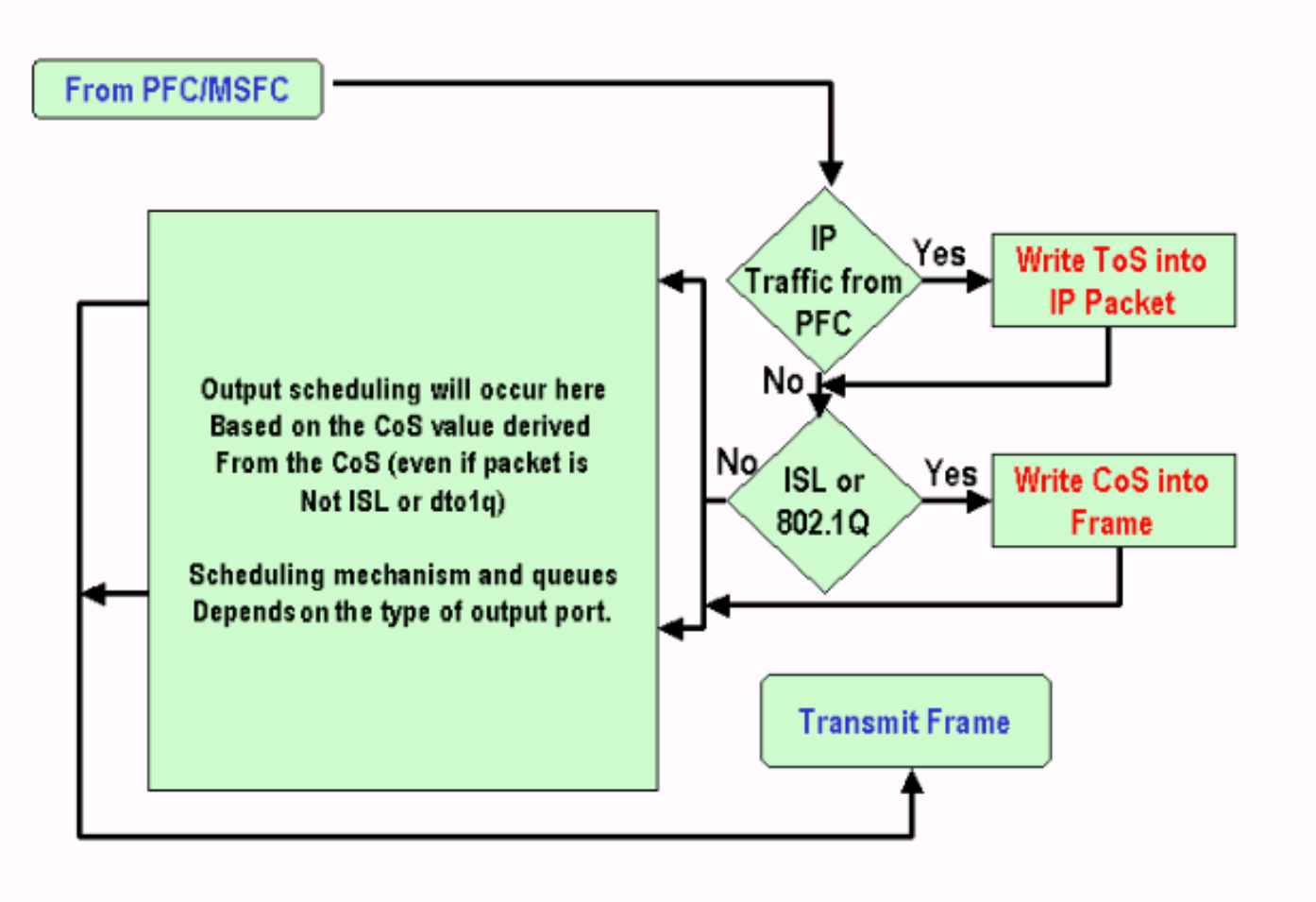
```
set qos dscp-cos-map 0-7:0
set qos dscp-cos-map 8-15:1
set qos dscp-cos-map 16-23:2
set qos dscp-cos-map 24-31:3
set qos dscp-cos-map 32-39:4
set qos dscp-cos-map 40-47:5
set qos dscp-cos-map 48-55:6
set qos dscp-cos-map 56-63:7
```

DSCP가 IP 헤더에 기록되고 CoS가 DSCP에서 파생되면 패킷은 CoS(패킷이 dot1q 또는 ISL이 아닌 경우에도)를 기반으로 출력 스케줄링을 위해 출력 대기열 중 하나로 전송됩니다. 출력 대기열 예약에 대한 자세한 내용은 다음 문서를 참조하십시오.

- Catalyst 6000 Series 스위치의 QoS:CatOS 소프트웨어를 사용하여 PFC 또는 PFC 2를 사용하

는 Catalyst 6000의 출력 스케줄링

다음 플로우 차트는 출력 포트의 마킹과 관련된 패킷 처리를 요약합니다.



메모 및 제한 사항

기본 ACL

기본적으로 기본 ACL은 "dscp 0"을 classification 키워드로 사용합니다.즉, QoS가 활성화된 경우 신뢰할 수 없는 포트를 통해 스위치에 들어오는 모든 트래픽은 DSCP가 "0"으로 표시됩니다.다음 명령을 실행하여 IP에 대한 기본 ACL을 확인할 수 있습니다.

```
Boris-1> (enable) show qos acl  info default-action  ip
set qos acl default-action
-------------------------
ip dscp 0
```

다음 명령을 실행하여 기본 ACL을 변경할 수도 있습니다.

qos acl default action ip [dscp xx 설정 | trust-CoS | trust-dscp | trust-ipprec]

ACL 항목 제한 사항에 대한 trust-cos

항목 내에서 trust-CoS 키워드를 사용할 때 표시되는 추가 제한이 있습니다.수신 신뢰 상태가 신뢰할 수 없는 경우에만 CoS를 엔트리에서 신뢰할 수 있습니다.trust-CoS로 항목을 구성하려고 하면 다음 경고가 표시됩니다.

```
Telix  (enable) set qos acl ip test_2 trust-CoS ip any any
Warning: ACL trust-CoS should only be used with ports that are also configured with port
trust=trust-CoS
test_2 editbuffer modified. Use 'commit' command to apply changes.
```

이 제한은 이전에 Input Port Handling(입력 포트 처리) 섹션에서 확인한 결과 발생합니다.해당 섹션의 순서도에 나와 있는 것처럼, 포트를 신뢰할 수 없는 경우 프레임에는 기본 포트 CoS가 즉시 할당됩니다.따라서 들어오는 CoS는 보존되지 않고 스위칭 엔진으로 전송되지 않으므로 특정 ACL에서도 CoS를 신뢰할 수 없습니다.

WS-X6248-xx, WS-X6224-xx 및 WS-X6348-xx 라인 카드의 제한 사항

이 섹션에서는 다음 라인 카드에만 적용됩니다.

- WS-X6224-100FX-MT:CATALYST 6000 24 PORT 100 FX MULTIMODE
- WS-X6248-RJ-45:CATALYST 6000 48-PORT 10/100 RJ-45 MODULE
- WS-X6248-전화:CATALYST 6000 48-PORT 10/100 TELCO MODULE
- WS-X6248A-RJ-45:CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6248A-TEL:CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6324-100FX-MM:CATALYST 6000 24-PORT 100FX, ENH QOS, MT
- WS-X6324-100FX-SM:CATALYST 6000 24-PORT 100FX, ENH QOS, MT
- WS-X6348-RJ-45:CATALYST 6000 48-PORT 10/100, ENHANCED QO
- WS-X6348-RJ21V:CATALYST 6000 48-PORT 10/100, 인라인 전원
- WS-X6348-RJ45V:CATALYST 6000 48-PORT 10/100, ENH QOS, INLI NE POWER

그러나 이러한 라인 카드에는 몇 가지 추가 제한 사항이 있습니다.

- 포트 레벨에서는 trust-dscp 또는 trust-ipprec를 사용할 수 없습니다.
- 포트 레벨에서 포트 신뢰 상태가 trust-CoS인 경우 다음 문이 적용됩니다.입력 예약에 대한 수신 임계값을 사용할 수 있습니다.또한 수신 패킷의 CoS는 버스에 액세스하기 위해 패킷의 우선순위를 지정하는 데 사용됩니다.CoS는 신뢰할 수 없으며 내부 DSCP를 파생하는 데 사용되지 않습니다. 해당 트래픽에 대한 ACL을 trust-cos로 구성하지 않는 한.또한 라인 카드가 포트에서 cos를 신뢰하는 것만으로는 충분하지 않으며, 해당 트래픽에 대해 trust-cos가 있는 ACL도 있어야 합니다.
- 포트 신뢰 상태가 신뢰할 수 없는 경우 표준 경우와 같이 일반 표시가 발생합니다. 이는 트래픽에 적용된 ACL에 따라 달라집니다.

이러한 포트 중 하나에서 신뢰 상태를 구성하려고 하면 다음 경고 메시지 중 하나가 표시됩니다.

```
telix (enable) set port qos 3/24 trust trust-ipprec
Trust type trust-ipprec not supported on this port.

telix (enable) set port qos 8/4 trust trust-dscp
Trust type trust-dscp not supported on this port.

telix (enable) set port qos 3/24 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/24.
Port  3/24 qos set to untrusted.
```

분류 요약

아래 표에는 다음과 같이 분류된 결과 DSCP가 나와 있습니다.

- 수신 포트 트러스트 상태입니다.
- 적용된 ACL 내의 classification 키워드입니다.

WS-X62*xx* 및 WS-X63*xx*를 제외한 모든 포트에 대한 일반 테이블 요약

ACL 키워드 포트 신뢰 상태	dscp xx	신뢰 DSCP	트러스트 IPC	신뢰-CoS
신뢰할 수 없음	xx(1)	Rx dscp	Rx ipprec에서 파생됨	0
신뢰 DSCP	Rx-dscp	Rx dscp	Rx ipprec에서 파생됨	Rx CoS 또는 포트 CoS에서 파생됨
트러스트 IPC	Rx ipprec에서 파생됨	Rx dscp	Rx ipprec에서 파생됨	Rx CoS 또는 포트 CoS에서 파생됨
신뢰-CoS	Rx cos 또는 포트 CoS에서 파생됨	Rx dscp	Rx ipprec에서 파생됨	Rx CoS 또는 포트 CoS에서 파생됨

(1) 이것이 프레임의 새 표시를 만드는 유일한 방법입니다.

WS-X62*xx* 또는 WS-X63*xx*의 표 요약

ACL 키워드 포트 신뢰 상태	dscp xx	신뢰 DSCP	트러스트 IPC	신뢰-CoS
신뢰할 수 없음	xx	Rx dscp	Rx ipprec에서 파생됨	0
신뢰 DSCP	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음
트러스트 IPC	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음
신뢰-CoS	xx	Rx dscp	Rx ipprec에서 파생됨	Rx CoS 또는 포트 CoS에서 파생됨(2)

(2) 이는 62xx 또는 63*xx* 라인 카드에서 들어오는 트래픽에 대해 수신 CoS를 보존하는 유일한 방법입니다.

구성 모니터링 및 확인

포트 컨피그레이션 확인

포트 설정 및 컨피그레이션은 다음 명령을 실행하여 확인할 수 있습니다.

show port qos *module/port*

이 명령을 실행하여 다른 매개변수 중에서 다음 분류 매개변수를 확인할 수 있습니다.

- 포트 기반 또는 VLAN 기반
- 신뢰 포트 유형
- 포트에 연결된 ACL

다음은 분류와 관련된 중요 필드가 강조 표시된 이 명령 출력의 샘플입니다.

```
tamer (enable) show port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.


Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 1/1    port-based     port-based      COPS           local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 1/1     1p2q2t       1p1q4t     untrusted     untrusted      0       0

(*)Runtime trust type set to untrusted.

Config:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                           IP

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                            IP
```

참고: 각 필드에 대해 구성된 매개변수와 런타임 매개변수가 있습니다.패킷에 적용될 것은 런타임 매개변수입니다.

ACL 확인

다음 명령을 실행하여 이전 명령에서 적용 및 확인한 ACL을 확인할 수 있습니다.

show qos acl info runtime *acl_name*

```
tamer (enable) show qos acl info run test_2
set qos acl IP test_2
-----------------------------------------
1. dscp 32 ip any host 1.1.1.1
2. trust-dscp any
```

샘플 사례 연구

다음 예는 네트워크에 나타날 수 있는 일반적인 사례의 샘플 컨피그레이션입니다.

사례 1:에지에서 표시

많은 사용자가 슬롯 2에 연결되어 있는 액세스 스위치로 사용되는 Catalyst 6000을 구성한다고 가정합니다(슬롯 2, 즉 WS-X6348 라인 카드(10/100M). 사용자는 다음을 전송할 수 있습니다.

- 일반 데이터 트래픽:이는 항상 VLAN 100에 있으며 DSCP가 "0"이어야 합니다.
- IP 전화의 음성 트래픽:이는 항상 음성 보조 VLAN 101에 있으며 DSCP가 "40"이어야 합니다.
- 미션 크리티컬 애플리케이션 트래픽:이 트래픽은 VLAN 100에서도 제공되며 서버 10.10.10.20으로 전송됩니다. 이 트래픽은 "32"의 DSCP를 가져와야 합니다.

이 트래픽 중 어느 것도 애플리케이션에 의해 표시되지 않으므로 포트를 신뢰할 수 없는 상태로 유지하고 트래픽을 분류하도록 특정 ACL을 구성합니다.하나의 ACL이 VLAN 100에 적용되고 하나의 ACL이 VLAN 101에 적용됩니다. 또한 모든 포트를 VLAN 기반으로 구성해야 합니다.다음은 결과 구성의 예입니다.

```
set qos enable
set port qos 2/1-48 vlan-based
!--- Not needed, as it is the default. set port qos 2/1-48 trust untrusted set qos acl ip
Data_vlan dscp 32 ip any host 10.10.10.20 !--- Not needed, because if it is not present you
would !--- use the default ACL which has the same effect. Set qos acl ip Data_vlan dscp 0 ip any
any set qos acl ip Voice_vlan dscp 40 ip any any commit qos acl all set qos acl map Data_vlan
100 set qos acl map Voice_vlan 101
```

사례 2:기가비트 인터페이스만으로 코어 신뢰

슬롯 1과 슬롯 2에 기가비트 인터페이스만 있는 코어 Catalyst 6000을 구성하고 있다고 가정합니다(섀시에 62xx 또는 63xx 라인 카드 없음). 이전에 액세스 스위치에서 트래픽을 올바르게 표시했으므로 리마킹을 할 필요가 없지만 수신 DSCP를 신뢰해야 합니다.모든 포트가 trust-dscp로 표시되고 다음 정도면 충분하므로 가장 쉬운 경우입니다.

```
set qos enable
set port qos 1/1-2 trust trust-dscp
set port qos 2/1-16 trust trust-dscp
...
```

사례 3:섀시에 62xx 또는 63xx 포트가 있는 코어 신뢰

WS-X6416-GBIC 라인 카드의 기가비트 링크(슬롯 2)와 WS-X6348 라인 카드(슬롯 3)의 10/100 링크를 사용하여 코어/디스트리뷰션 디바이스를 구성한다고 가정합니다. 또한 액세스 스위치 레벨에서 이전에 표시되었으므로 모든 수신 트래픽을 신뢰해야 합니다.6348 라인 카드에서 trust-dscp를 사용할 수 없으므로 이 경우 가장 쉬운 방법은 모든 포트를 신뢰할 수 없는 상태로 유지하고 기본 ACL을 trust-dscp로 변경하는 것입니다.

```
set qos enable
set port qos 2/1-16 trust untrusted
set port qos 3/1-48 trust untrusted
set qos acl default-action ip trust-dscp
```

관련 정보

- LAN 제품 지원

- LAN 스위칭 기술 지원
- Technical Support - Cisco Systems