# ACI의 패킷 삭제 결함 설명

## 목차

```
소개
관리되는 개체
하드웨어 삭제 카운터 유형
앞으로
SECURITY GROUP DENY
VLAN XLATE MISS
ACL DROP
SUP 리디렉션
오류
버퍼
CLI에서 Drop Stats 보기
<u>관리되는 개체</u>
하드웨어 카운터
리프
스파인
결함
<u>F112425 - 인그레스 삭제 패킷 속도(I2IngrPktsAg15min:dropRate)</u>
F100264 - 인그레스 버퍼 삭제 패킷 속도(eqptIngrDropPkts5min:bufferRate)
F100696 - 인그레스 포워딩 삭제 패킷(eqptIngrDropPkts5min:forwardingRate)
통계 임계값
패킷 전송 속도(eqptIngrDropPkts)
l2IngrPktsAg의 인그레스 삭제 패킷 속도
```

## 소개

이 문서에서는 각 결함 유형 및 이 결함이 표시될 때의 절차에 대해 설명합니다.관리자는 Cisco ACI(Application Centric Infrastructure) 패브릭의 정상적인 운영 중에 특정 유형의 패킷 삭제에 대한 결함을 볼 수 있습니다.

## 관리되는 개체

Cisco ACI에서는 모든 결함이 MO(Managed Objects)에서 제기됩니다. 예를 들어, fault "*F11245 - 인그레스 삭제 패킷 속도(l2IngrPktsAg15min:dropRate)*"는 MO *l2IngrPktsAg15min*의 매개 변수 *dropRate에* 대해 *설명합니다*.

이 섹션에서는 패킷 장애 삭제와 관련된 MO(Managed Object)의 몇 가지 예를 소개합니다.

	예	설명	샘플 매개 변수	점을 MO 내성 어떤 결함이 제기. 었는지
l2인그로그패킷	l2IngrPkts5min l2IngrPkts15분	이는 각 기간 동안 VLAN당 인그 레스 패킷 통계를 나타냅니다.	드롭 속도 플러드 비	vlanCktEp(VLAN)

	l2IngrPkts1h 기타		율 멀티캐스트 속도 유니캐스트 속도	
l2IngrPktsAg	l2IngrPktsAg15분 l2IngrPktsAg1h l2IngrPktsAg1d 기타	이는 EPG, BD, VRF 등당 인그레 스 패킷 통계를 나타냅니다. 예) EPG 통계는 EPG에 속하는 VLAN 통계의 집계를 나타냅니다	늡 속도 플러드 비 율 멀티캐스트 속도 유니캐스트 속도	fvAEPg(EPG) fvAp(애플리케이션 프로파일) fvBD(BD) l3extOut(L3OUT)
에qptIngr삭제패킷	eqptIngrDropPkts15분 eqptIngrDropPkts1h eqptIngrDropPkts1d 기타	이는 각 기간 동안 인터페이스당 인그레스 삭제 패킷 통계를 나타 냅니다.	*1 전달 속 도 *1 오류 비 율 *1 버퍼 속 도	l1physlf(물리적 포 트) pcAggrlf(포트 채님

\*1:SUP\_REDIRECT 패킷이 전달 삭제로 기록되고 있기 때문에 여러 Nexus 9000 플랫폼의 ASIC 제한으로 인해 eqptIngrDropPkts의 이러한 카운터가 잘못 발생할 수 있습니다 .CSCvo68407 <u>참조</u> 및 <u>CSCvn72699</u> 자세한 내용 및 고정 버전.

## 하드웨어 삭제 카운터 유형

ACI 모드에서 실행 중인 Nexus 9000 스위치에는 ASIC에 인그레스 인터페이스 삭제 사유에 대한 3가지 주요 하드웨어 카운터가 있습니다.

I2IngrPkts, I2IngrPktsAg의 dropRate에는 이러한 카운터가 포함됩니다.eqptIngrDropPkts에 대한 위 의 표에 있는 세 개의 매개 변수(forwardingRate, errorRate, bufferRate)는 세 개의 각 인터페이스 카 운터를 나타냅니다.

## 앞으로

전달 삭제는 ASIC의 LookUp 블록(LU)에서 삭제된 패킷입니다.LU 블록에서 패킷 헤더 정보를 기반으로 패킷 포워딩 결정이 수행됩니다.패킷을 삭제하기로 결정하면 Forward Drop이 계산됩 니다.다양한 이유가 있을 수 있지만 주요 이유를 살펴보겠습니다.

### SECURITY\_GROUP\_DENY

통신이 가능하도록 계약이 누락되어 드롭입니다.

패킷이 패브릭에 들어가면 스위치는 소스 및 대상 EPG를 확인하여 이 통신을 허용하는 계약이 있는지 확인합니다. 소스와 대상이 다른 EPG에 있고 이러한 패킷 유형을 허용하는 계약이 없는 경우 스위치는 패킷을 삭제하고 SECURITY\_GROUP\_DENY로 레이블을 지정합니다.이렇게 하면 Forward Drop 카운터가 증가합니다.

### VLAN\_XLATE\_MISS

부적절한 VLAN으로 인한 삭제.

패킷이 패브릭에 들어가면 스위치는 패킷을 확인하여 포트의 컨피그레이션에서 이 패 킷을 허용하는지 확인합니다. 예를 들어, 프레임은 802.1Q 태그가 10인 패브릭으로 들 어갑니다. 스위치에 VLAN 10이 포트에 있는 경우 콘텐츠를 검사하고 대상 MAC에 따 라 전달을 결정합니다. 그러나 VLAN 10이 포트에 없는 경우 이를 삭제하고 VLAN\_XLATE\_MISS로 레이블을 지정합니다. 이렇게 하면 전달 삭제 카운터가 증가합 니다.

"XLATE" 또는 "Translate"의 이유는 ACI에서 리프 스위치가 802.1Q 캡슐을 가진 프레 임을 가져와 패브릭 내부의 VXLAN 및 기타 표준화에 사용될 새 VLAN으로 변환하기 때문입니다. VLAN이 구축되지 않은 상태로 프레임이 들어오는 경우 "변환"이 실패합 니다.

#### ACL\_DROP

슈퍼캠 때문에 한 방울 떨어졌어요

ACI 스위치의 sup-tcam에는 일반적인 L2/L3 포워딩 결정 위에 적용되는 특수 규칙이 포함되어 있습니다.sup-tcam의 규칙은 기본적으로 제공되며 사용자가 구성할 수 없습 니다.sup-tcam 규칙의 목적은 주로 일부 예외 또는 일부 컨트롤 플레인 트래픽을 처리 하는 데 있으며 사용자가 확인하거나 모니터링하지 않습니다.패킷이 sup-tcam 규칙에 도달하고 규칙이 패킷을 삭제하는 경우 삭제된 패킷은 ACL\_DROP으로 계산되고 Forward Drop 카운터가 증가합니다.이 경우, 일반적으로 패킷이 기본 ACI 포워딩 주체 에 대해 포워딩될 예정임을 의미합니다.

드롭 이름은 ACL\_DROP이지만 이 "ACL"은 독립형 NX-OS 디바이스 또는 기타 라우팅 /스위칭 디바이스에서 구성할 수 있는 일반 액세스 제어 목록과 동일하지 않습니다.

#### SUP\_리디렉션

이것은 한 방울이 아니다.

sup 리디렉션된 패킷(예: CDP/LLDP/UDLD/BFD 등)은 패킷이 올바르게 처리되고 CPU로 전달되는 경우에도 전달 삭제로 계산될 수 있습니다.

이는 N9K-C93180YC-EX와 같은 -EX 플랫폼에서만 발생할 수 있습니다.이러한 항목 은 "삭제"로 계산해서는 안 되지만, -EX 플랫폼의 ASIC 제한 때문입니다.

## 오류

스위치가 전면 패널 인터페이스 중 하나에서 잘못된 프레임을 수신하면 오류로 삭제됩니다. 예 를 들면 FCS 또는 CRC 오류가 있는 프레임이 있습니다. 그러나 정상적인 작동에서는 leaf의 업링크 포트 또는 스파인 포트에서 오류 패킷이 증가하는

그러나 성상적인 작용에서는 leaf의 입링크 포트 또는 스파인 포트에서 오뉴 패킷이 증가하는 것을 볼 수 있습니다. 업링크 리프 포트 또는 스파인 포트를 볼 때 "show interface"를 사용하여 FCS/CRC 오류를 확인하는 것이 가장 좋습니다.

### 버퍼

스위치가 프레임을 수신하고 인그레스 또는 이그레스 중 하나에 사용할 수 있는 버퍼 크레딧이 없는 경우 프레임이 "Buffer"로 삭제됩니다. 이는 일반적으로 네트워크 어딘가에 혼잡을 나타냅 니다. 결함이 표시된 링크는 꽉 찼거나 대상이 포함된 링크가 혼잡할 수 있습니다.

## CLI에서 Drop Stats 보기

## 관리되는 개체

SSH(Secure Shell)를 APIC 중 하나에 연결하고 다음 명령을 실행합니다.

#### apic1# moquery -c l2IngrPktsAg15분

이 클래스는 I2IngrPktsAg15min 클래스에 대한 모든 개체 인스턴스를 제공합니다.

다음은 특정 객체를 쿼리하는 필터를 사용하는 예입니다.이 예에서 필터는 "tn-TENANT1/ap-APP1/epg-EPG1"을 포함하는 특성 **dn**이 있는 객체만 표시합니다.

또한 이 예에서는 egrep를 사용하여 필요한 특성만 표시합니다.

### 출력 1 예:테넌트 TENANT1, 애플리케이션 프로필 APP1, epg EPG1의 EPG 카운터 개체 (l2IngrPktsAg15min)

apicl# moquery -c l2IngrPktsAg15min -f 'l2.IngrPktsAg15min.dn\*"tn-TENANT1/ap-APP1/epg-EPG1"' |
egrep 'dn|drop[P,R]|rep'
dn : uni/tn-TENANT1/ap-APP1/epg-EPG1/CDl2IngrPktsAg15min dropPer : 30 <--- number of drop packet
in the current periodic interval (600sec) dropRate : 0.050000 <--- drop packet rate =
dropPer(30) / periodic interval(600s) repIntvEnd : 2017-03-03T15:39:59.181-08:00 <--- periodic
interval = repIntvEnd - repIntvStart repIntvStart : 2017-03-03T15:29:58.016-08:00 = 15:39 15:29
= 10 min = 600 sec</pre>

또는 객체 dn을 알고 있는 경우 -c 대신 다른 옵션-d를 사용하여 특정 객체를 가져올 수도 있습니다.

#### 출력 2 예:테넌트 TENANT1, 애플리케이션 프로필 APP1, epg EPG2의 EPG 카운터 개체 (l2IngrPktsAg15min)

apicl# moquery -d uni/tn-TENANT1/ap-APP1/epg-EPG2/CDl2IngrPktsAg15min | egrep 'dn|drop[P,R]|rep' dn : uni/tn-jw1/BD-jw1/CDl2IngrPktsAg15min dropPer : 30 dropRate : 0.050000 repIntvEnd : 2017-03-03T15:54:58.021-08:00 repIntvStart : 2017-03-03T15:44:58.020-08:00

## 하드웨어 카운터

결함이 표시되거나 CLI를 사용하여 스위치 포트에서 패킷 삭제를 확인하려면 하드웨어에서 플 랫폼 카운터를 보는 것이 가장 좋습니다.대부분의 경우, 모든 카운터가 show interface를 사용 하여 표시되는 것은 아닙니다. 3가지 주요 삭제 이유는 플랫폼 카운터를 통해서만 볼 수 있습니 다. 이러한 내용을 보려면 다음 단계를 수행합니다.

#### 리프

SSH를 leaf에 연결하고 이 명령을 실행합니다.

#### ACI-LEAF# vsh\_lc

1/31의 출력 예:

ACI-LEAF#	vsh_1	c				
vsh_lc						
module-1#						
module-1#	show	platform inter	nal counte	ers port 31		
Stats for	port	31				
(note: for	ward	drops includes	sup redin	ected packet	s too)	
IF	LPC	ort	Ir	nput		Output
			Packets	Bytes	Packet	s Bytes
eth-1/31	31	Total	400719	286628225	2302918	463380330
		Unicast	306610	269471065	453831	40294786
		Multicast	0	0	1849091	423087288
		Flood	56783	8427482	0	0
		Total Drops	37327		0	
		Buffer	0		0	
		Error	0		0	
		Forward	37327			
		LB	0			
		AFD RED			0	
			snip	-		

## 스파인

박스 유형 스파인(N9K-C9336PQ)의 경우 Leaf와 정확히 동일합니다.

모듈형 스파인(N9K-C9504 등)의 경우 플랫폼 카운터를 보려면 먼저 특정 라인 카드를 연 결해야 합니다. SSH를 스파인에 연결하고 다음 명령을 실행합니다.

ACI-SPINE# vsh

### ACI-SPINE# 연결 모듈 <X>

module-2# show platform internal counters port <Y>.

\* 여기서 X는 보려는 라인 카드의 모듈 번호를 나타냅니다.

Y는 포트 번호를 나타냅니다.

## 이더넷 2/1의 출력 예:

ACI-SPINE# vsh Cisco iNX-OS Debug Shell This shell should only be used for internal commands and exists for legacy reasons. User should use ibash infrastructure as this will be deprecated. ACI-SPINE# ACI-SPINE# attach module 2 Attaching to module 2 ... To exit type 'exit', to abort type '\$.' Last login: Mon Feb 27 18:47:13 UTC 2017 from sup01-ins on pts/1 No directory, logging in with HOME=/ Bad terminal type: "xterm-256color". Will assume vt100. module-2#

module-2#	show	platform inte	rnal count	ers port 1		
Stats for	port	1				
(note: for	ward	drops include	s sup redi	rected packets	s too)	
IF	LPo	rt	I	nput		Output
			Packets	Bytes	Packet	ts Bytes
eth-2/1	1	Total	85632884	32811563575	126611414	25868913406
		Unicast	81449096	32273734109	104024872	23037696345
		Multicast	3759719	487617769	22586542	2831217061
		Flood	0	0	0	0
		Total Drops	0		0	
		Buffer	0		0	
		Error	0		0	
		Forward	0			
		LB	0			
		AFD RED			0	
			- snip			

## 결함

## F112425 - 인그레스 삭제 패킷 속도(I2IngrPktsAg15min:dropRate)

### 설명:

이 결함의 가장 일반적인 이유 중 하나는 레이어 2 패킷이 "Forward Drop" 이유로 삭제되기 때문입니다.다양한 이유가 있지만 가장 일반적인 이유는 다음과 같습니다.

일부 플랫폼에서(CSCvo68407 <u>참조)</u>) CPU로 리디렉션해야 하는 L2 패킷(예: CDP/LLDP/UDLD/BFD 등)이 "Forward Drop"으로 기록되고 CPU로 복제되는 데 제한이 있 습니다.이는 이러한 모델에 사용되는 ASIC의 제한 때문입니다.

#### 해결 방법:

위에서 설명한 그 물방울은 순전히 겉에 불과하기 때문에 모범 사례는 Stats Threshold 섹 션에 표시된 대로 결함의 임계값을 늘리는 **것입니다**. 이렇게 하려면 통계 임계값의 지침을 참조하십시오.

## F100264 - 인그레스 버퍼 삭제 패킷 속도(eqptIngrDropPkts5min:bufferRate)

### 설명:

이 결함은 패킷이 포트에서 삭제될 때 "Buffer(버퍼)"라는 이유로 증가할 수 있습니다. 위에 서 언급한 것처럼 일반적으로 인그레스 또는 이그레스 방향의 인터페이스에 혼잡이 있을 때 발생합니다.

#### 해결 방법:

이 결함은 혼잡 때문에 환경에서 실제 삭제된 패킷을 나타냅니다. 삭제된 패킷으로 인해 ACI 패브릭에서 실행되는 애플리케이션에 문제가 발생할 수 있습니다.네트워크 관리자는 패킷 흐름을 격리하고 예기치 않은 트래픽 흐름, 비효율적인 로드 밸런싱 등으로 인한 혼잡 여부를 확인해야 합니다.또는 예상 사용률입니다.

## F100696 - 인그레스 포워딩 삭제 패킷(eqptIngrDropPkts5min:forwardingRate)

**참고:**F11245에 대해 위에서 설명한 것과 같은 ASIC 제한은 이러한 결함을 발생시킬 수 있습니다.자세한 내용은 <u>CSCvo68407</u> 자세한 내용을 확인하십시오.

이 결함은 몇 가지 시나리오로 인해 발생합니다.가장 일반적인 것은 다음과 같습니다.

#### 설명 1) 스파인 삭제

스파인 인터페이스에서 이 결함이 확인되면 알 수 없는 엔드포인트로 향하는 트래픽 때문 일 수 있습니다.

프록시 조회를 위해 ARP 또는 IP 패킷이 스파인에 전달되고 패브릭에서 엔드포인트를 알 수 없는 경우, 특수 간선 패킷이 생성되어 해당 BD(내부) 멀티캐스트 그룹 주소의 모든 leaf로 전송됩니다.그러면 BD(Bridge Domain)의 각 leaf에서 엔드포인트를 검색하기 위한 ARP 요청이 트리거됩니다. 제한 때문에그리고 leaf에서 받은 glean 패킷도 다시 패브릭에 반영되고 leaf에 연결된 스파인 링크에서 전달 드롭을 트리거합니다.이 시나리오의 전달 삭 제는 1세대 스파인 하드웨어에서만 증가합니다.

#### 해결 1)

이 문제는 ACI 패브릭에 불필요한 양의 유니캐스트 트래픽을 전송하는 장치로 인해 발생하 는 것으로 알려져 있으므로, 어떤 디바이스에서 이러한 트래픽을 발생시키고 있는지 파악 하고 방지할 수 있는지 확인해야 합니다.이는 일반적으로 모니터링을 위해 서브넷의 IP 주 소를 스캔하거나 프로브하는 디바이스에서 발생합니다. 이 트래픽을 전송하는 IP를 찾으려 면 fault를 표시하는 스파인 인터페이스에 연결된 leaf에 SSH를 연결합니다.

여기에서 이 명령을 실행하여 glean 패킷을 트리거하는 Source IP Address(sip)를 확인할 수 있습니다.

ACI-LEAF# show ip arp internal event-history event | grep glean | grep sip | more
[116] TID 11304:arp\_handle\_inband\_glean:3035: log\_collect\_arp\_glean;sip = 192.168.21.150;dip
= 192.168.20.100;info = Received glean packet is an IP packet

[116] TID 11304:arp\_handle\_inband\_glean:3035: log\_collect\_arp\_glean;sip = 192.168.21.150;dip = 192.168.20.100;info = Received glean packet is an IP packet

이 예제 출력에서 glean 패킷은 192.168.21.150에 의해 트리거되며 이 작업이 완화될 수 있는지 확인하는 것이 좋습니다.

#### 설명 2) 리프 삭제

리프 인터페이스에서 이 결함이 표시될 경우, 가장 가능성이 높은 원인은 언급된 SECURITY\_GROUP\_DENY 삭제 때문입니다.

#### 해결 방법 2)

ACI leaf는 계약 위반으로 인해 거부된 패킷의 로그를 보관합니다.이 로그는 CPU 리소스를 보호하기 위해 모든 패킷을 캡처하지는 않지만 여전히 방대한 로그를 제공합니다.

필수 로그를 가져오려면 fault가 제기된 인터페이스가 포트 채널의 일부인 경우 이 명령과 grep를 포트 채널에 사용해야 합니다.그렇지 않으면 물리적 인터페이스를 삭제할 수 있습 니다. 이 로그는 계약 삭제의 양에 따라 신속하게 롤오버할 수 있습니다.

ACI-LEAF# show logging ip access-list internal packet-log deny | grep port-channel2 | more [ Sun Feb 19 14:16:12 2017 503637 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD\_VLAN, Vlan-Id: 59, SMac: 0x8c604f0288fc, DMac:0x0022bdf819ff, **SIP: 192.168.21.150, DIP: 192.168.20.3**, SPort: 0, DPort: 0, **Src Intf: port-channel2, Pr oto: 1**, PktLen: 98 [ Sun Feb 19 14:16:12 2017 502547 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD\_VLAN, Vlan-Id: 59, SMac: 0x8c604f0288fc, DMac:0x0022bdf819ff, SIP: 192.168.21.150, DIP: 192.168.20.3, SPort: 0, DPort: 0, Src Intf: port-channel2, Pr oto: 1, PktLen: 98

이 경우 192.168.21.150은 ICMP 메시지(IP 프로토콜 번호 1)를 192.168.20.3으로 전송하 려고 합니다. 그러나 2개의 EPG 간에 ICMP를 허용하는 계약이 없으므로 패킷이 삭제됩니 다. ICMP가 허용되어야 하는 경우 두 EPG 간에 계약을 추가할 수 있습니다.

## 통계 임계값

이 섹션에서는 드롭 카운터에 대해 결함을 일으킬 수 있는 통계 객체에 대한 임계값을 변경하는 방법에 대해 설명합니다.

각 객체(예: I2IngrPkts, eqptIngrDropPkts)의 통계에 대한 임계값은 다양한 객체에 대한 모니터링 정 책을 통해 구성됩니다.

시작 의 표에 설명된 대로, eqptIngrDropPkts는 모니터링 정책을 통해 I1PhysIf 객체와 같이 아래에 서 모니터링됩니다.

## 패킷 전송 속도(eqptIngrDropPkts)

2인분이 있습니다

+ 액세스 정책(외부 장치를 향하는 포트).a.k.전면 패널 포트)

+ 패브릭 정책(LEAF와 SPINE 사이의 포트. a.k.a 패브릭 포트)

Front Panel Ports (ports towards external devices)



Fabric Ports (ports between LEAF and SPINE)



각 포트 객체(I1PhysIf, pcAggrIf)는 위 그림에 표시된 대로 **인터페이스 정책 그룹**을 통해 자체 **모니터링 정책**을 할당할 수 있습니다.

기본적으로 Fabric(패브릭) > Access Policies(액세스 정책) 및 Fabric(패브릭) > Fabric(패브릭) APIC GUI의 Fabric Policies(패브릭 정책)에 **기본 모니터링 정책**이 있습니다.이러한 기본 모니 터링 정책은 각각 모든 포트에 할당됩니다.Access Policies(액세스 정책)의 기본 모니터링 정책 은 전면 패널 포트용이고 패브릭 정책의 기본 모니터링 정책은 패브릭 포트용입니다.

포트당 임계값을 변경해야 하는 경우가 아니면 각 섹션의 기본 모니터링 정책을 직접 수정하여 모든 전면 패널 포트 및/또는 패브릭 포트에 변경 사항을 적용할 수 있습니다.

다음 예는 패브릭 포트(**패브릭 정책**)의 QptIngrDropPkts에서 Forward Drop에 대한 임계값을 변경하는 것입니다. 전면 패널 포트에 대해 **Fabric(패브릭) > Access Policies(액세스 정책)**에서 동일한 작업을 수행하십시오.

1. Fabric(패브릭) >Fabric Policies(패브릭 정책)> Monitoring Policies(모니터링 정책)로 이동합 니다.

2. 마우스 오른쪽 버튼을 클릭하고 "모니터링 정책 생성"을 선택합니다.

(임계값 변경을 모든 패브릭 포트에 적용할 수 있는 경우 새 **포트**를 생성하지 않고 기본값으 로 이동합니다.)

3. 새 모니터링 정책 또는 기본값을 확장하고 통계 수집 정책으로 이동합니다..

4. 오른쪽 창에서 Monitoring Object(모니터링 개체)의 연필 아이콘을 클릭하고 Layer 1 Physical Interface Configuration(I1.PhysIf)을 선택합니다.

(기본 정책을 사용할 경우 이 단계 4를 건너뛸 수 있습니다.)

5. 오른쪽 창의 **Monitoring Object** 드롭다운에서 Layer **1 Physical Interface Configuration** (I1.PhysIf) 및 Stats Type을 선택하고 Ingress Drop Packets를 **선택합니다.** 

ululu cisco	System	Tenants	Fabric	VM Networking	L4-L7 Services	Admin	Operations
		Inventory	Fabric Policies   Acces	ss Policies			
Policies		Stats Col	lection Policies				
Quick Start		Manitaria					
Switch Policies		Objec	Layer 1 Physical Interfa	ce Configuration (I1.Ph 🚽	Stats Type: Ingress Drop	Packets	<u> </u>
Module Policies							
Interface Policies		Cranulada			Adapta Chata		
Pod Policies		Granularity			Admin State		
Global Policies		5 Minute			inherited		
Monitoring Policies							
Common Policy							
▲ L default							
Stats Collecti	on Policies						
Stats Export I	Policies						
Diagnostics P	Policies						
Callhome/SN	MP/Syslog						
Event Severity	y Assignment Policies						
Fault Severity	Assignment Policies						
Fault Lifecycle	e Policies						
Troubleshoot Policie	es						
Geolocation Policies	S						
Analytics Policies							
Tags							
		-					

## 6. 구성 임계값 옆에 있는 +를 클릭합니다.

Inventory   Fabric Policies   Access Policies					
Stats Collection Policies					i
Object: Layer 1 Physical Interface Configuration (I1.Ph - ) Stats	Type: Ingress Drop Packets 🗸 🗸				
				×	+
Granularity	Admin State	History Retention Period	Config Thresholds		
5 Minute	inherited	inherited	0		

## 7. 전달 삭제에 대한 임계값 편집

Thresholds For Collection 5 Minute		×
Config Thresholds		
	×	+
Property	Edit Threshold	
Ingress Buffer Drop Packets rate		
Ingress Forwarding Drop Packets rate		
Ingress Error Drop Packets rate		-
	1	_
	CLOSE	

8. 전달 삭제 속도를 위해 critical, major, minor 및 warning 컨피그레이션에 대한 임계값 증가 를 비활성화하는 것이 좋습니다. Ingress Forwarding Drop Packets rate

	Normal Value:	0		\$						
1	Threshold Direction:	Both	Risin	g Falli	ng					
Rising Tr	hresholds to Config:	Criti Maji Mini War	ical or or ming							
Falling Tr	hresholds to Config:	CHE	CK ALL	UNCHE	CK ALL					
		Maj Min War CHE	or or ming CK ALL	UNCHE	CK ALL					
Rising		Maji Min War CHE	or or ming CK ALL	UNCHE	CK ALL	Falling	3			
Rising	et	Maj Min Min War CHE	or or CK ALL Reset	UNCHE	CK ALL	Falling	Reset		Set	
Rising Se	et 0000	Maj Min Min War CHE	or or ming CK ALL Reset	UNCHE	CK ALL	Falling	Reset	•	Set 0	
Rising Se Critical 10 Major 50	et 0000	CHE	OF OF Ming CK ALL 9000 4900	UNCHE	CK ALL	Falling Warning Minor	Reset	•	Set 0	4
Rising Se Sritical 10 Aajor 50 Alinor 50	et 0000 000	CHE	or or ming CK ALL 9000 4900 490	UNCHE	CK ALL	Falling Warning Minor Major	Reset           0           0           0           0	0 0	<b>Set</b> 0 0	0 0 0

9. 이 새 모니터링 정책을 필요한 포트에 대한 인터페이스 정책 그룹에 적용합니다.따라서 패브 릭 정책에서 인터페이스 프로필, 스위치 프로필 등을 구성하는 것을 잊지 마십시오.

## (기본 정책을 사용할 경우 이 단계 9를 건너뛸 수 있습니다.)

alialia cisco	System	Tenants	Fabric	VM Networking	L4-L7 Services	Admin	Operations	Apps	٩	i
		wentory Fab	ric Policies A	coess Policies						
Policies				a 🛛 Le	eaf Fabric	Port P	olicy Group	- FABRI	C PORT PG	
Quick !	Start Policies						,,		Policy	Fault
<ul> <li>Module</li> <li>Interface</li> </ul>	e Policies ce Policies			0	±		<u>A</u> 4			
Pol	icy Groups FABRIC_PORT	_PG		F	Properties	S Name: F	ABRIC_PORT_PG			
<ul> <li>Pro</li> <li>Los</li> </ul>	tiles Il Fabric Interfa	ce Overrides			D	escription:	optional			
<ul> <li>Pod Pod</li> </ul>	ne Fabric Inter Nicies	face Overrides			Monitori	ing Policy:	FABRIC_PORT	<u>*</u> 6		
<ul> <li>Global</li> <li>Monito</li> </ul>	Policies ring Policies									
<ul> <li>Cor</li> <li>FAE</li> <li>Get</li> </ul>	mmon Policy SRIC_PORT ault		13							

10. 전면 패널 포트(액세스 정책)에 해당하는 경우 이 새 모니터링 정책이 포트 채널 및 물리적

×

포트에 적용될 수 있도록 **레이어 1 물리적 인터페이스 구성(I1.Physlf)**과 반대로 **집계 인터페이** 스(pc.Aggrlf)에 대해 동일한 작업을 수행하십시오.

(기본 정책을 사용할 경우 이 10단계를 건너뛸 수 있습니다.)

## l2IngrPktsAg의 인그레스 삭제 패킷 속도

여기에는 여러 부분이 있습니다.

VLAN or any aggregation of VLAN stats



※ It doesn't have to be one Monitoring Policy. It could be one Monitoring Policy for each.

위 그림에서 알 수 있듯이 l2IngrPktsAg는 많은 개체 아래에서 모니터링됩니다.위 그림에는 일 부 예만 표시되지만 l2IngrPktsAg의 일부 객체는 표시되지 않습니다.그러나 통계 임계값은 모 니터링 정책 및 l1Physlf 또는 pcAggrlf에 eqptIngrDropPkts를 통해 구성됩니다.

각 객체(EPG(fvAEPg), Bridge Domain(fvBD) 등)에 위 그림에 표시된 대로 자체 **모니터링 정책** 을 할당할 수 있습니다.

기본적으로 테넌트의 모든 객체는 달리 구성되지 않은 한 Tenant(테넌트) > common(공통) > Monitoring Policies(모니터링 정책) > default(기본값)에서 기본 Monitoring Policy(모니터링 정책)를 사용합니다.

각 구성 요소별로 임계값을 변경해야 하는 경우가 아니면 공통 테넌트 아래의 기본 모니터링 정 책을 직접 수정하여 모든 관련 구성 요소에 대한 변경 사항을 적용할 수 있습니다.

다음 예는 브리지 도메인의 I2IngrPktsAg15min에서 Ingress Drop Packets Rate에 대한 임계값 을 변경하는 것입니다.

1. Tenant(테넌트) > (테넌트 이름) > Monitoring Policies(모니터링 정책)로 이동합니다.

(기본 모니터링 정책을 사용하거나 새 모니터링 정책을 테넌트 간에 적용해야 하는 경우 테 넌트가 공통이어야 합니다.)

2. 마우스 오른쪽 버튼을 클릭하고 "모니터링 정책 생성"을 선택합니다.

(임계값 변경 사항을 모든 구성 요소에 적용할 수 있는 경우 새 구성 요소를 만드는 대신 기

**본값**으로 이동합니다.)

3. 새 모니터링 정책 또는 기본값을 확장하고 통계 수집 정책으로 이동합니다..

4. 오른쪽 창에서 **모니터링 객체**의 연필 아이콘을 클릭하고 다음을 선택합니다. **브리지 도메인** (fv.BD).

(기본 정책을 사용할 경우 이 단계 4를 건너뛸 수 있습니다.)

5. 오른쪽 창의 Monitoring Object(모니터링 개체) 드롭다운에서 Bridge Domain (fv.BD) and Stats Type(브리지 도메인(fv.BD) 및 Stats Type(통계 유형)을 선택하고 Aggregated ingress packets(집계 인그레스 패킷)를 선택합니다.

alialia cisco	System		Fabric	VM Networking	L4-L7 Services	Admin	Operations	Apps	٩	i	Advanced Mode welcome, admin •
ALL TENANTS		earch: enter nam	e, alias, descr								
Tenant common		⊴ 0	State Co	Ilection Poli	cioc						
Quick Star  A  Tenant co  Applica	t mmon ution Ptofiles		O Monitor Obje	ing Bridge Domain et:	(fv.BD)		💌 🖍 Stats Type:	Aggregated ingress packe	ts 🗸 🖌		
Notwork	rking										× +
🕨 🖿 IP Add	ress Pools		Granularity			Admin State		History Reten	tion Period	Co	onfig Thresholds
L4-L7	Service Paramete	rs	15 Minute			inherited		inherited		+	1
<ul> <li>Securit</li> </ul>	ty Policies										
► m Trouble	shoot Policies										
🔺 💼 Monito	ring Policies										
► 1. TK.	MON										
🔄 🖌 📃 del	ault										
	Stats Collection P	olicies	-								
	Stats Export Polici	05	1								
-	Callhome/SNMP/S	Syslog									
-	Present Presentation Res	Contract Participan									

## 6. 구성 임계값 옆에 있는 +를 클릭합니다.

Stats Collection Policies				i
Object Bridge Domain (fv.BD)	Stats Type: Aggrega	ated ingress packets 🗸 🗸		
•			×	+
Granularity	Admin State	History Retention Period	Config Thresholds	
15 Minute	inherited	inherited	Ð	

## 7. 전달 삭제에 대한 임계값 편집

Config Thresholds		
	×	+
Property Edit Thres	old	
ingress drop packets rate		

8. 전달 삭제 속도를 위해 critical, major, minor 및 warning 컨피그레이션에 대한 임계값 증가를 비활성화하는 것이 좋습니다.

Ingress Forwarding Drop Packets rate

Normal Value: 0   Threshold Direction:   Both   Rising   Rising   Major   Major   Minor   Warning   Critical   Major   Minor   Warning   Critical   Major   Major   Set   Reset   Set   Najor   Major	Reast of the only a rate of the operation of the operatio												
Threshold Direction: Boh Rsing Falling   Rising Thresholds to Config: Ortical   Minor Warning   CHECK ALL UNCHECK ALL   Falling Thresholds to Config: Ortical   Minor Minor   Warning CHECK ALL   UNCHECK ALL UNCHECK ALL   Falling Thresholds to Config:   Critical Minor   Minor Minor   Boh Falling Thresholds to Config:   Critical Minor   Minor Minor   Set Reset   Reset Reset   Sinor 9000   Minor 0   Minor 4900   Minor 0   Minor 4900   Minor 0   Major 0   Minor 0   Minor 0   Minor 9   Major 0   Minor 0	Normal Value: 0												
Rising Thresholds to Config: Critical   Minor Warning   CHECK ALL UNCHECK ALL   Falling Thresholds to Config: Critical   Major Major   Minor Minor   Minor Major   Major Major   Major Major		Threshold Direction:	Both	Rising	Falling								
Falling Thresholds to Config: Critical   Major Minor   Warning CHECK ALL   UNCHECK ALL UNCHECK ALL     Falling Thresholds to Config: Critical   Major Nono   Set Reset   Critical 10000   9000 C   Major 9000   Minor 0   Solo 4900   Minor 0   Minor 0   Solo 4900   Major 0   Major 0   10 9   Critical 0   0 0	Risir	ng Thresholds to Config:	Critic Majo Mino Wan	cal xr xr ning CK ALL	UNCHECK ALL								
Rising         Set         Reset         Reset         Set           Critical         10000         0	Fallir	ng Thresholds to Config:	Critic Majo Mino Warr	cal xr xr ning CK ALL	UNCHECK ALL	3							
Set         Reset         Reset         Set           Critical         10000         \$9000         \$Warning         0         \$0         \$\$           Major         5000         \$4900         \$\$         Minor         0         \$\$         \$\$           Minor         500         \$\$         \$\$         \$\$         \$\$         \$\$         \$\$           Warning         10         \$\$         9         \$\$         \$\$         \$\$         \$\$	Rising					Falling							
Critical         10000         0         9000         Warning         0		Set		Reset			Reset	S	et				
Major         5000         4900         Minor         0	Critical	10000	٥	9000		Warning	0	¢ 0		٠			
Minor         500         6         490         0         Major         0         <	Major	5000	٥	4900		Minor	0	• 0		•			
Warning 10 0 9 0 Critical 0 0 0	Minor	500	٥	490	4	Major	0	<u> </u>		٠			
	Warning	10	٥	9		Critical	0	<u> </u>		٠			
SUBMIT									SUBMIT	CANCEL			

9. 임계값을 변경해야 하는 브리지 도메인에 이 새 모니터링 정책을 적용합니다.

## (기본 정책을 사용할 경우 이 단계 9를 건너뛸 수 있습니다.)

CISCO System Tenants	Fabric VM L4-L Fabric Networking Service	.7 Admin Operations	Apps	P	i	Mode welcome, admin +
ALL TENANTS   Add Tenant   Search	enter name, alias, descr   commo	n   TK   infra   AJ   jw1				
Tenant TK Start	Bridge Domain - BD1					i
A B Tenant TK			Policy Operation	al Stats Healt	h Faults	History
Application Profiles     Application			Main	L3 Configurations	Advanced/	Troublesh.
🔺 🚞 Bridge Domains	⊖ <b>±</b>	▲ ▲	0 0 100			
▶ • BD1	Properties		-			
▶	Monitoring Policy	y: TK_MON 🗸 🗗	J			
BD_SG_PBR1	Segmen	n: 15826915				
BD_SG_PBR2	Multicast Addres	s: 225.1.26.128				
<ul> <li>BD_SPAN</li> <li>VREs</li> </ul>	NetFlow Monitor Policie	S:				× +

### 메모

기본 모니터링 정책이 아닌 경우 기본 모니터링 정책에 있는 컨피그레이션이 없을 수 있습니 다.이러한 컨피그레이션을 기본 모니터링 정책과 동일하게 유지해야 하는 경우 사용자는 기본 모니터링 정책 컨피그레이션을 확인하고 기본 모니터링 정책이 아닌 모니터링 정책에 대해 동 일한 정책을 수동으로 구성해야 합니다.

X