ACI中的資料包丟棄故障說明

目錄

簡介

受管理的物件

硬體丟棄計數器型別

- 轉寄
- 錯誤
- 緩衝區

在CLI中檢視丟棄統計資訊

- 受管理的物件
- 硬體計數器
- 分葉
- 骨幹

故障

- F112425 -ingress drop packets rate (l2IngrPktsAg15min：dropRate)
- F100264 -入口緩衝區丟棄資料包速率(eqptIngrDropPkts5min：bufferRate)
- F100696 -入口轉發丟棄資料包(eqptIngrDropPkts5min：forwardingRate)

統計閾值

- eqptIngrDropPkts中的轉發丟棄資料包速率
- l2IngrPktsAg中的入口丟棄資料包速率

簡介

本文檔介紹了每種故障型別，以及發生此故障時的操作步驟。在思科以應用為中心的基礎設施(ACI)交換矩陣的正常運行期間，管理員可能會發現某些型別的資料包丟棄故障。

受管理的物件

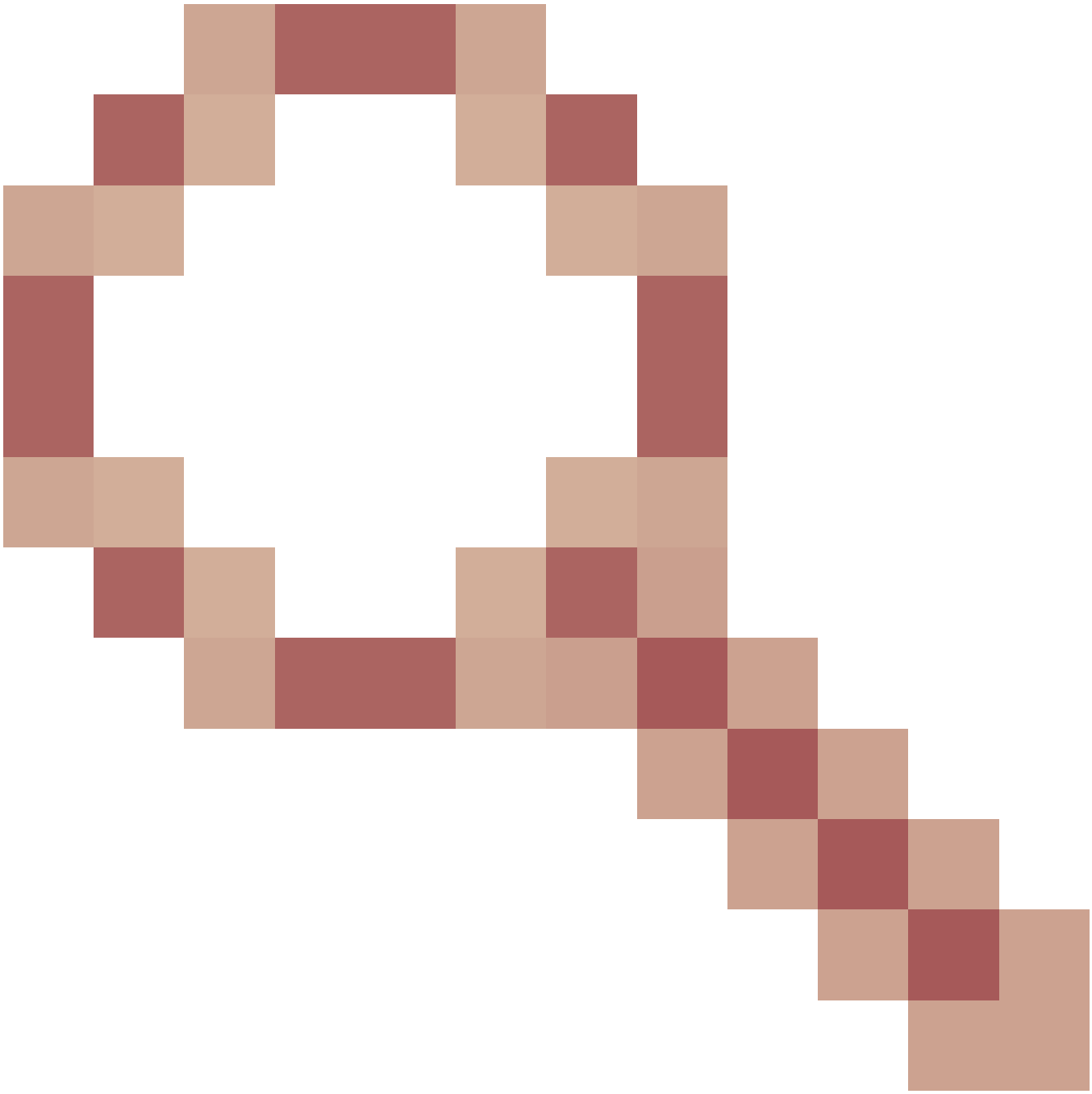
在思科ACI中，所有故障均在託管對象(MO)下引發。例如，錯誤「F11245 -入口丟棄資料包速率(l2IngrPktsAg15min：dropRate)」與MO l2IngrPktsAg15min中的引數dropRate有關。

本節介紹一些與丟棄資料包故障相關的示例託管對象(MO)。

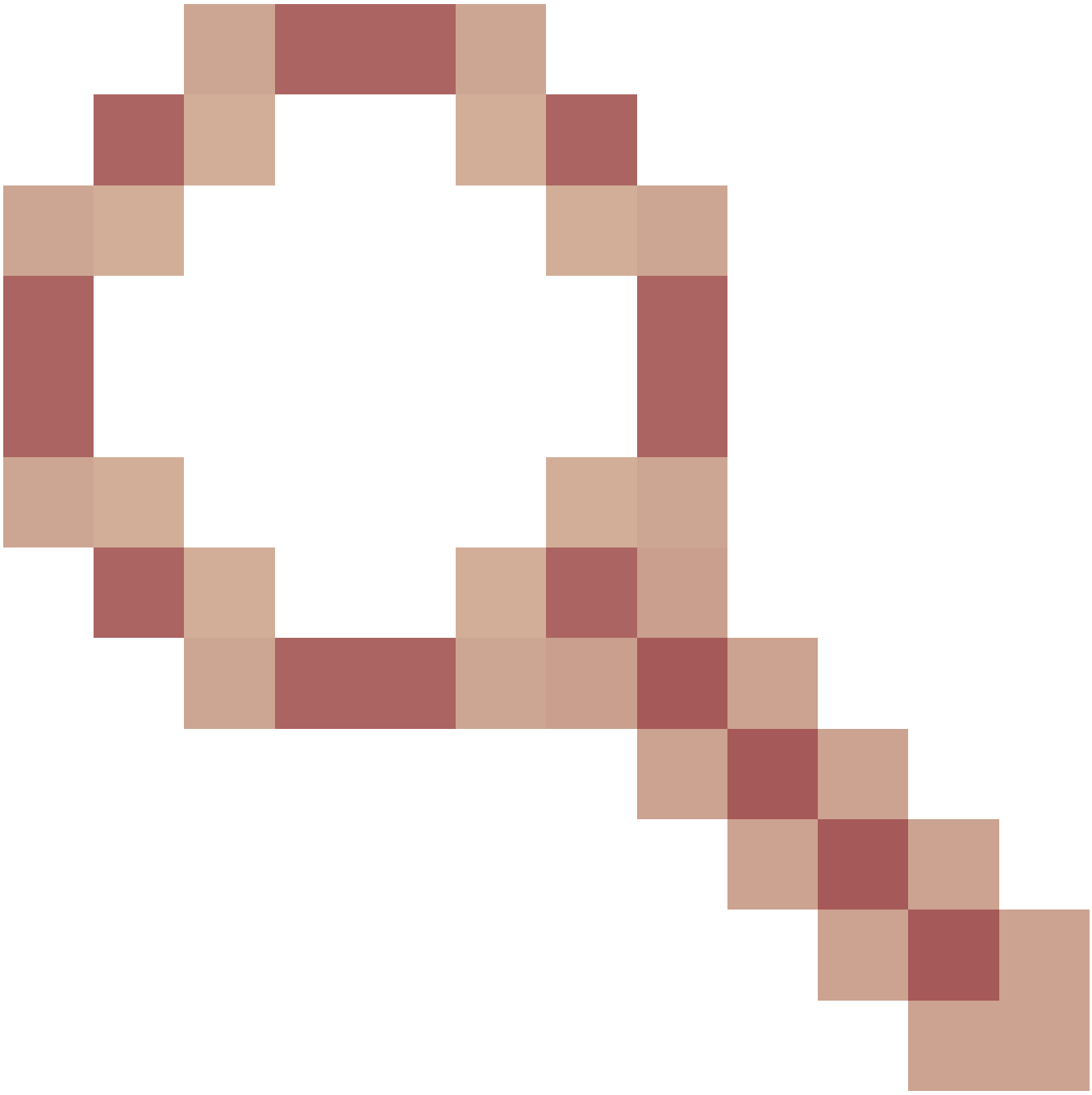
	範例	說明	範例引數	MO示例 出現哪些故障
l2IngrPkts	l2IngrPkts5min l2IngrPkts15min	這表示每個週期內每個VLAN的入口資料包統計資訊	dropRate floodRate	vlanCktEp (VLAN)

	l2IngrPkts1h 等等……		multicastRate unicastRate	
l2IngrPktsAg	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d 等等……	這表示每個EPG、BD、VRF等的入口資料包統計資訊。 例如) EPG統計資訊表示屬於EPG的VLAN統計資訊的聚合	dropRate floodRate multicastRate unicastRate	fvAEPg (EPG) fvAp（應用配置檔案） fvBD (BD) l3extOut (L3OUT)
eqptIngrDropPkts	eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d 等等……	這表示每個介面在每個時間段內的入口丟棄資料包統計資訊	*1 forwardingRate *1 errorRate *1 bufferRate	l1PhysIf（物理埠） pcAggrIf（埠通道）

*1 ：由於多個Nexus 9000平台中的ASIC限制，eqptIngrDropPkts中的這些計數器可能會錯誤地提升，因為SUP_REDIRECT資料包會作為轉發丟棄進行記錄。有關更多詳細資訊及固定版本，請參閱CSCvo68407



和CSCvn72699



。

硬體丟棄計數器型別

在以ACI模式運行的Nexus 9000交換機上，有3個主要硬體計數器表示ASIC上的入口介面丟棄原因。

l2IngrPkts， l2IngrPktsAg中的dropRate包含這些計數器。上表中eqptIngrDropPkts的三個引數(forwardingRate、errorRate、bufferRate)分別代表三個介面計數器。

轉寄

轉發丟棄，是在ASIC的查詢塊(LU)上丟棄的資料包。在LU塊中，基於資料包報頭資訊做出資料包轉發決策。如果決定丟棄資料包，則會計算轉發丟棄。發生這種情況的原因有很多，但讓我們談談主要原因：

SECURITY_GROUP_DENY

由於缺少允許通訊的合約而減少。

當資料包進入交換矩陣時，交換機會檢視源EPG和目的EPG，檢視是否存在允許此通訊的合約。 如果源和目標位於不同的EPG中，並且沒有允許此資料包型別的合約，則交換機將丟棄該資料包並將其標籤為SECURITY_GROUP_DENY。這會增加Forward Drop計數器。

VLAN_XLATE_MISS

由於VLAN不當而丟棄的。

封包進入光纖時，交換器會檢視封包，判斷連線埠上的組態是否允許此封包。 例如，幀以802.1Q標籤10進入交換矩陣。如果交換機在埠上有VLAN 10，它將檢查內容並根據目標MAC做出轉發決策。但是，如果VLAN 10不在埠上，它將丟棄該幀並將其標籤為VLAN_XLATE_MISS。這將增加Forward Drop計數器。

「XLATE」或「Translate」的原因是，在ACI中，枝葉交換機將採用具有802.1Q封裝的幀，並將其轉換為新的VLAN，用於交換矩陣內的VXLAN和其他規範化。 如果幀中有一個VLAN未部署，「轉換」將失敗。

ACL_DROP

因為sup-tcam。

aci交換機中的sup-tcam包含要在正常L2/L3轉發決策基礎上應用的特殊規則。sup-tcam中的規則是內建的，不能由使用者配置。Sup-tcam規則的目的主要是處理某些例外或控制平面流量，而不是由使用者檢查或監控。當資料包符合sup-tcam規則且規則是丟棄資料包時，丟棄的資料包將計為ACL_DROP，它將遞增Forward Drop計數器。發生這種情況時，通常意味著資料包將根據基本ACI轉發主體進行轉發。

請注意，即使丟棄名稱是ACL_DROP，此「ACL」與可在獨立NX-OS裝置或任何其他路由/交換裝置上配置的正常訪問控制清單也不相同。

SUP_REDIRECT

這不是一滴水。

即使資料包被正確處理並轉發到CPU，Sup重定向的資料包（例如CDP/LLDP/UDLD/BFD等）也可能被算作轉發丟棄。

這發生在-EX、-FX和-FX2平台中，例如N9K-C93180YC-EX或N9K-C93180YC-FX。這些不應計為「丟棄」，但這是因為-EX/-FX/-FX2平台中的ASIC限制。

錯誤

當交換機在其中一個前面板介面上收到無效幀時，該幀將被作為錯誤丟棄。 例如，幀中存在

FCS或CRC錯誤。在檢視上行鏈路/下行鏈路枝葉埠或主幹埠時，最好使用「show interface」檢查FCS/CRC錯誤。
但是，在正常操作下，預計會看到錯誤資料包在枝葉的上行/下行鏈路埠或主幹埠上遞增，因為此計數器還包括系統修剪的幀，這些幀不會從介面傳送出去。
示例：路由資料包、相同介面廣播/泛洪幀的TTL故障。

緩衝區

當交換機接收到幀時，沒有可用於入口或出口的緩衝區信用，該幀將帶有「Buffer」一起丟棄。 這通常提示網路中的某個位置擁塞。 表示故障的鏈路可能已滿，或者包含目的地的鏈路可能擁塞。

在CLI中檢視丟棄統計資訊

受管理的物件

將安全外殼(SSH)連線到其中一個APIC並運行以下命令。

```
apic1# moquery -c l2IngrPktsAg15min
```

這將提供此類別l2IngrPktsAg15min的所有物件實體。

以下是具有用於查詢特定對象的篩選器的示例。在本示例中，過濾器是隻顯示屬性為dn的對象，包括「tn-TENANT1/ap-APP1/epg-EPG1」（ DNS為「epg」）。

此範例也使用egrep僅顯示必要的屬性。

示例輸出1：租戶TENANT1、應用配置檔案APP1、epg EPG1的EPG計數器對象(l2IngrPktsAg15min)。

```
apic1# moquery -c l2IngrPktsAg15min -f 'l2.IngrPktsAg15min.dn*"tn-TENANT1/ap-APP1/epg-EPG1"' | egrep 'dn

dn               : uni/tn-TENANT1/ap-APP1/epg-EPG1/CDl2IngrPktsAg15min
dropPer          : 30                                <--- number of drop packet in the current periodic in
dropRate         : 0.050000                          <--- drop packet rate = dropPer(30) / periodic interv
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
```

或者，如果您知道對象dn，則可以使用其他選項-d代替-c來獲取特定對象。

示例輸出2：租戶TENANT1、應用配置檔案APP1、epg EPG2的EPG計數器對象(l2IngrPktsAg15min)。

```
apic1# 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
```

硬體計數器

如果發現故障，或者希望使用CLI檢查交換機埠上的資料包丟棄，則最好透過檢視硬體中的平台計數器來檢查。大多數計數器（但不是所有計數器）是使用show interface顯示的。 三個主要丟棄原因只能使用平台計數器檢視。 要檢視這些資訊，請執行以下步驟：

分葉

透過SSH連線到枝葉並運行以下命令。

ACI-LEAF# vsh_lc
module-1# show platform internal counters port <X>
* 其中X代表連線埠號碼

Etherent 1/31的示例輸出：

<#root>

```
ACI-LEAF#
```

vsh_lc

```
vsh_lc
module-1#
module-1#
```

show platform internal counters port 31

```
Stats for port 31
(note: forward drops includes sup redirected packets too)
IF          LPort                    Input                         Output
                                Packets       Bytes           Packets    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 -----
```

骨幹

對於箱型主幹(N9K-C9336PQ)，它與Leaf完全相同。

對於模組化主幹（N9K-C9504等……），您必須首先連線特定的板卡，然後才能檢視平台計數器。 使用SSH連線到主幹，然後運行以下命令

ACI-SPINE# vsh

ACI-SPINE#連線模組<X>

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

* 其中X代表您想要檢視的線路卡模組編號

Y代表連線埠號碼

Ethernet 2/1的示例輸出：

<#root>

```
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 internal counters port 1

Stats for port 1
(note: forward drops includes sup redirected packets too)
IF          LPort                    Input                        Output
                                Packets       Bytes          Packets    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
```

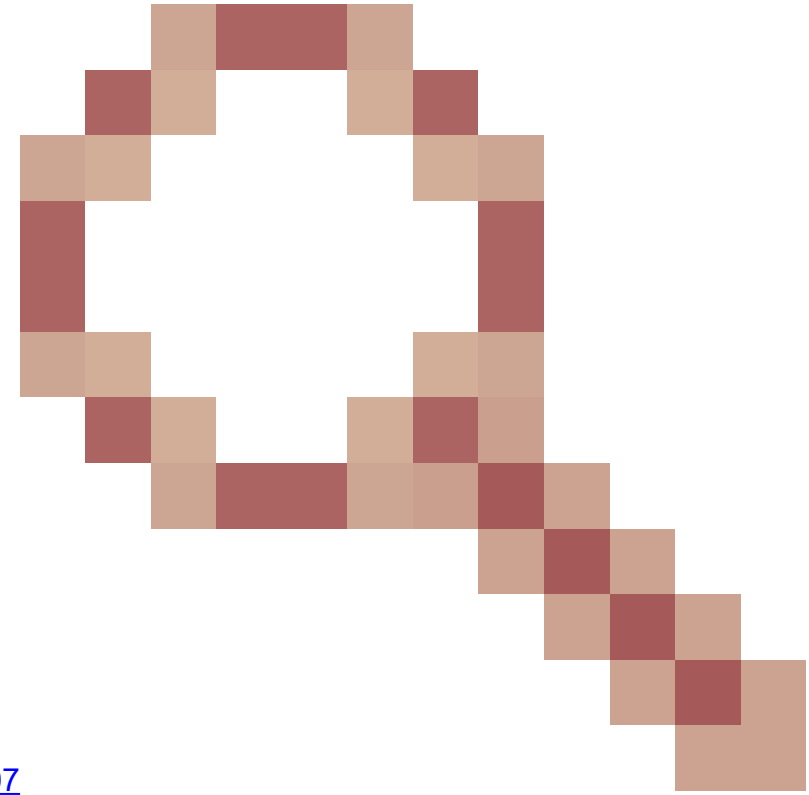
```
Forward          0

                   LB                0
                   AFD RED                                  0
                        ----- snip -----
```

故障

F112425 -入口捨棄封包速率(l2IngrPktsAg15min：dropRate)

說明:

此故障的常見原因之一是第2層資料包由於「Forward Drop」原因而被丟棄。原因有很多，但最常見的是：



在某些平台上(請參閱CSCvo68407)，需要重定向到CPU（即CDP/LLDP/UDLD/BFD等）的L2資料包將被記錄為「轉發丟棄」並複製到CPU存在限制。這是因為這些型號中使用的ASIC的限制。

解析度：

上述的丟包只是表面現象，因此最佳實踐建議是增加故障閾值，如統計閾值部分中所示。要執行此操作，請參閱統計閾值中的說明。

F100264 -入口緩衝區丟棄資料包速率(eqptIngrDropPkts5min：bufferRate)

說明:

當埠上的資料包由於「緩衝區」而被丟棄時，此故障可能會增加。如上所述，當介面在入口或出口方向出現擁塞時，通常會發生此故障。

解析度：

此故障代表因擁塞而實際丟棄的環境中資料包。 丟棄的資料包可能導致ACI交換矩陣中運行的應用程式出現問題。網路管理員應該隔離資料包流，並確定擁塞是由未預期的流量流、低效的負載均衡等造成的，還是由這些埠上的預期使用率造成的。

F100696 -入口轉發丟棄資料包(eqptIngrDropPkts5min：forwardingRate)

註：上述F11245的ASIC限制也會導致這些故障增加。有關詳細資訊，請參閱CSCvo68407。

此故障由幾種情況引起。最常見的是：

描述1)脊柱脫落

如果在主幹介面上發現此故障，則可能是由於發往未知終端的流量所致。

當將ARP或IP資料包轉發到主幹以進行代理查詢時，交換矩陣中的終端未知，將生成一個特殊的收集資料包，並將其傳送到相應BD（內部）組播組地址上的所有枝葉。這將觸發來自網橋域(BD)中每個枝葉的ARP請求以發現終端。 由於限制，枝葉接收的收集資料包也會再次反射回交換矩陣，並觸發連線到枝葉的主幹鏈路上的轉發丟棄。此方案中的轉發丟棄僅在第1代主乾硬體上遞增。

決議1)

由於已知問題是由向ACI交換矩陣傳送不必要數量的未知單播流量導致的，因此需要確定導致此問題的裝置，並檢視是否可以阻止此問題。這通常是由於裝置出於監控目的掃描或探測子網上的IP地址所致。 為了找出傳送此流量的IP地址，請將SSH連線到主幹介面上出現故障的枝葉上。

您可以在此處執行此指令，以檢視觸發收集封包的來源IP位址(sip)：

<#root>

```
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.
```

在此示例輸出中，收集的資料包由192.168.21.150觸發，建議檢視能否緩解此情況。

說明2)枝葉丟棄

如果在枝葉介面上發現此故障，最可能的原因是上面提到的SECURITY_GROUP_DENY丟棄。

決議2)

ACI枝葉會儲存因違反合約而被拒絕的資料包日誌。此日誌不會捕獲所有資料包以保護CPU資源，但它仍然為您提供大量日誌。

要獲取所需的日誌，如果發生故障的介面是埠通道的一部分，則需要使用此命令和grep來獲取埠通道。否則，可能會損壞物理介面。

此日誌可根據合約丟棄量快速累計。

<#root>

```
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,

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,
oto: 1, PktLen: 98
```

在此案例中，192.168.21.150正在嘗試將ICMP訊息（IP通訊協定編號1）傳送到192.168.20.3。但是，2個EPG之間沒有允許ICMP的合約，因此封包被捨棄。 如果應允許ICMP，則可以在兩個EPG之間增加合約。

統計閾值

本節介紹如何更改可能引發丟棄計數器故障的統計對象的閾值。

每個物件的統計值（例如l2IngrPkts、eqptIngrDropPkts）的臨界值是透過監控原則針對各種物件設定的。

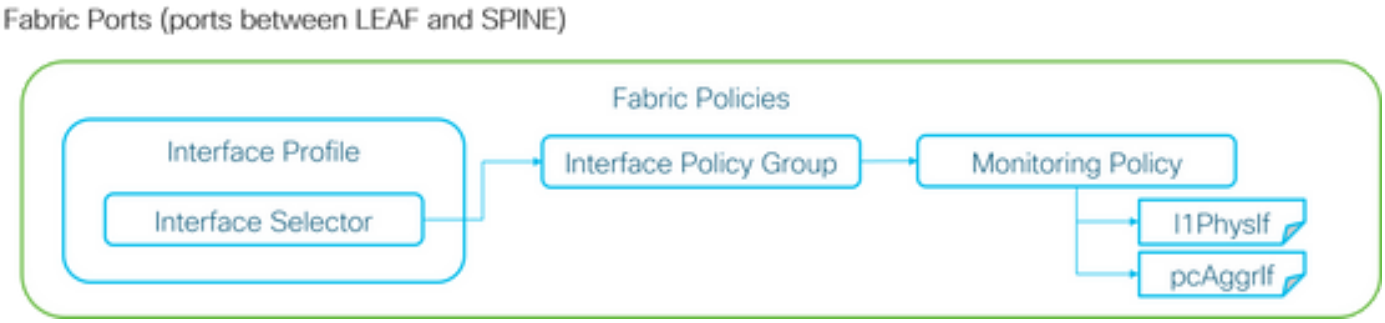
如開始處的表格中所述，eqptIngrDropPkts會透過監視原則在l1PhysIf物件下受到監視。

eqptIngrDropPkts中的轉發丟棄資料包速率

這個有兩個部分。

+存取原則（連線埠朝向外部裝置。亦即前面板連線埠）

+交換矩陣策略（枝葉和主幹之間的埠。又稱a交換矩陣埠）



透過介面策略組可以為每個埠對象(l1PhysIf、pcAggrIf)分配自己的監控策略，如上圖所示。

預設情況下，APIC GUI中的Fabric > Access Policies和Fabric > Fabric Policies下都存在預設監控策略。這些預設監控策略分別分配給所有埠。訪問策略下的預設監控策略用於前面板埠，交換矩陣策略下的預設監控策略用於交換矩陣埠。

除非需要更改每個埠的閾值，否則可以直接修改每個部分中的預設監控策略，以將更改應用於所有前面板埠和/或交換矩陣埠。

以下示例更改交換矩陣埠上eqptIngrDropPkts中的轉發丟棄閾值(交換矩陣策略)。請對前面板埠執行Fabric > Access Policies下的相同操作。

1. 導航到交換矩陣>交換矩陣策略>監控策略。

2. 按一下滑鼠右鍵並選取「建立監督原則」。

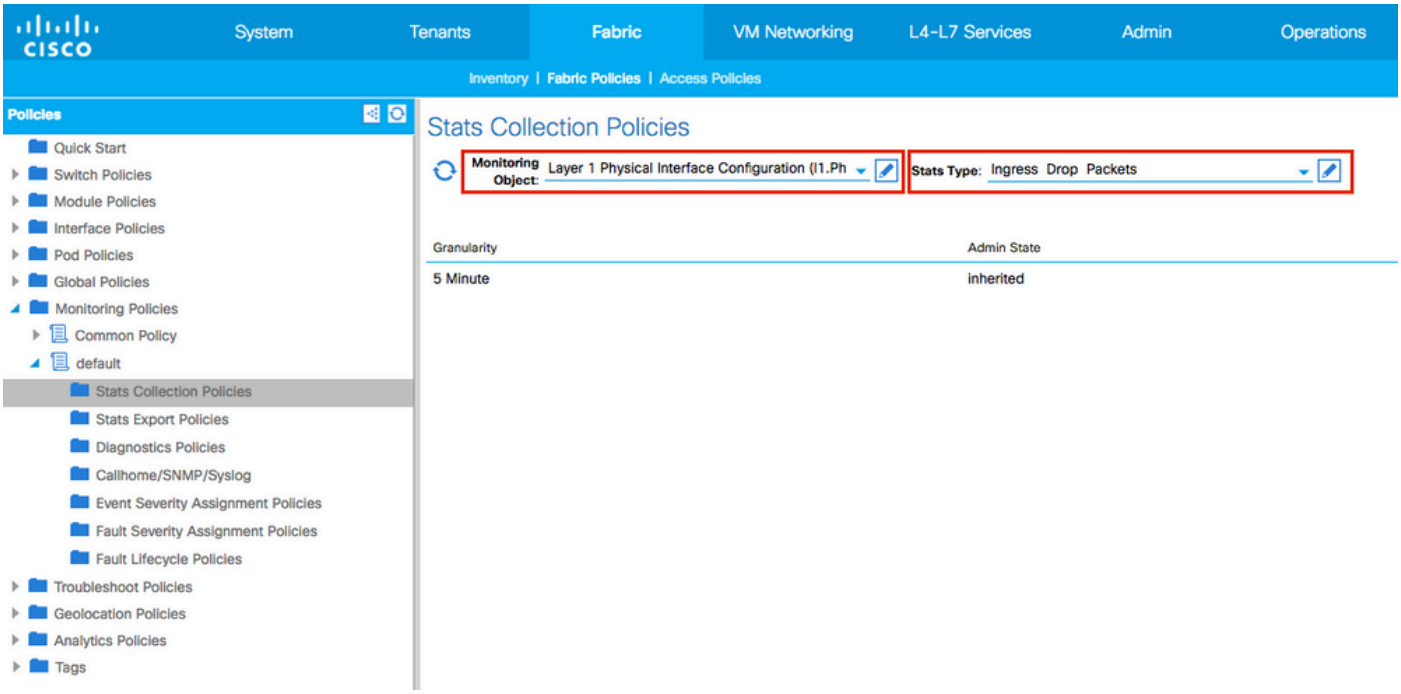
(如果閾值更改可以應用於所有交換矩陣埠，請導航到default，而不是建立一個新埠)

3. 展開新的「監控政策」或預設值，然後定位至統計資料收集政策。

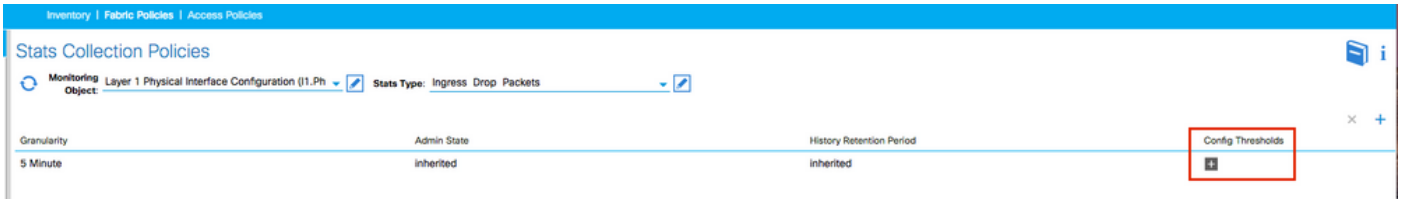
4. 按一下右窗格中監控對象的鉛筆圖示，選擇第1層物理介面配置(l1.PhysIf)。

（使用預設策略時，可以跳過此步驟4）

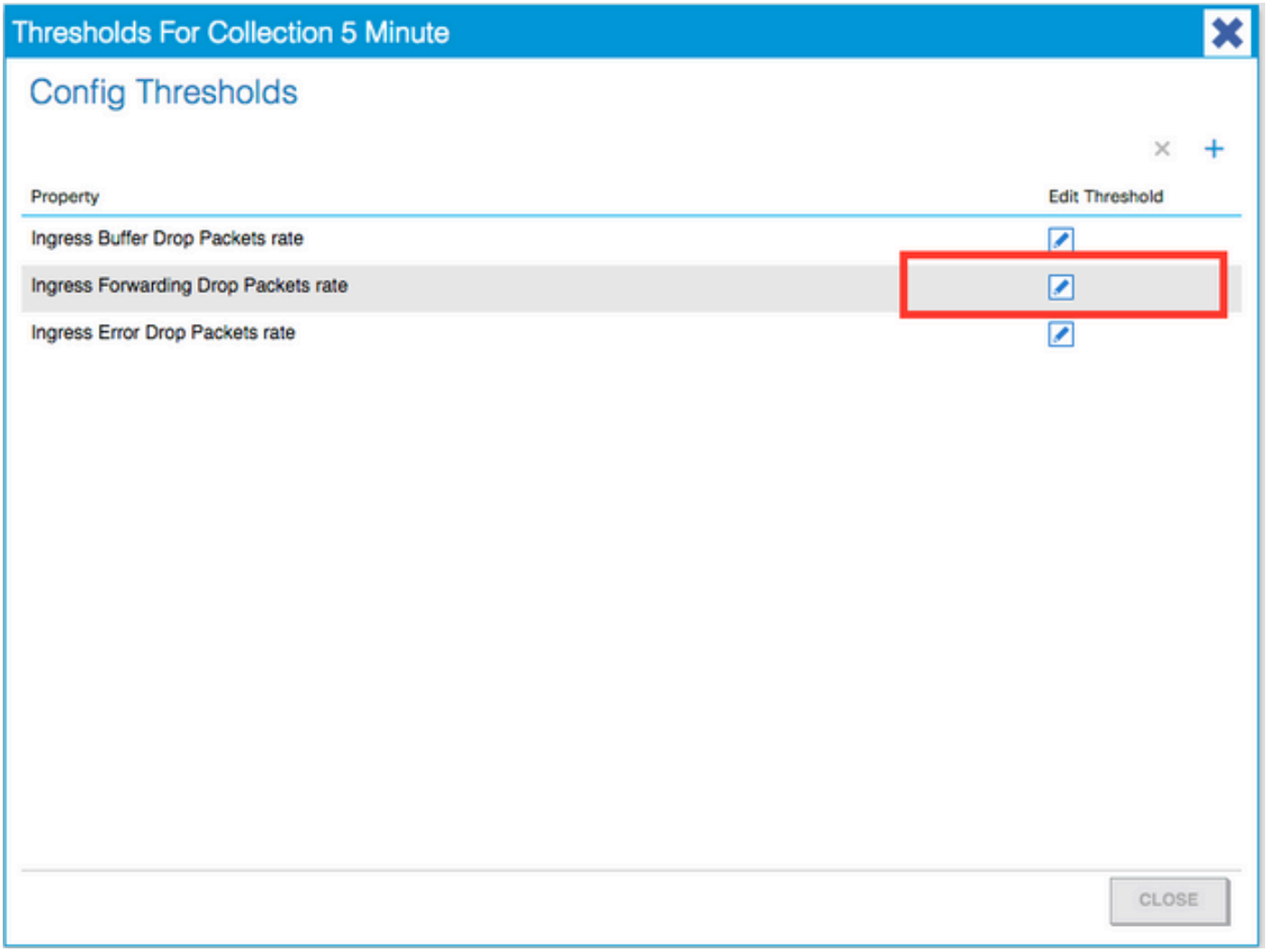
5. 從右側窗格中的Monitoring Object下拉選單中選擇Layer 1 Physical Interface Configuration (l1.PhysIf)和Stats Type，然後選擇Ingress Drop Packets



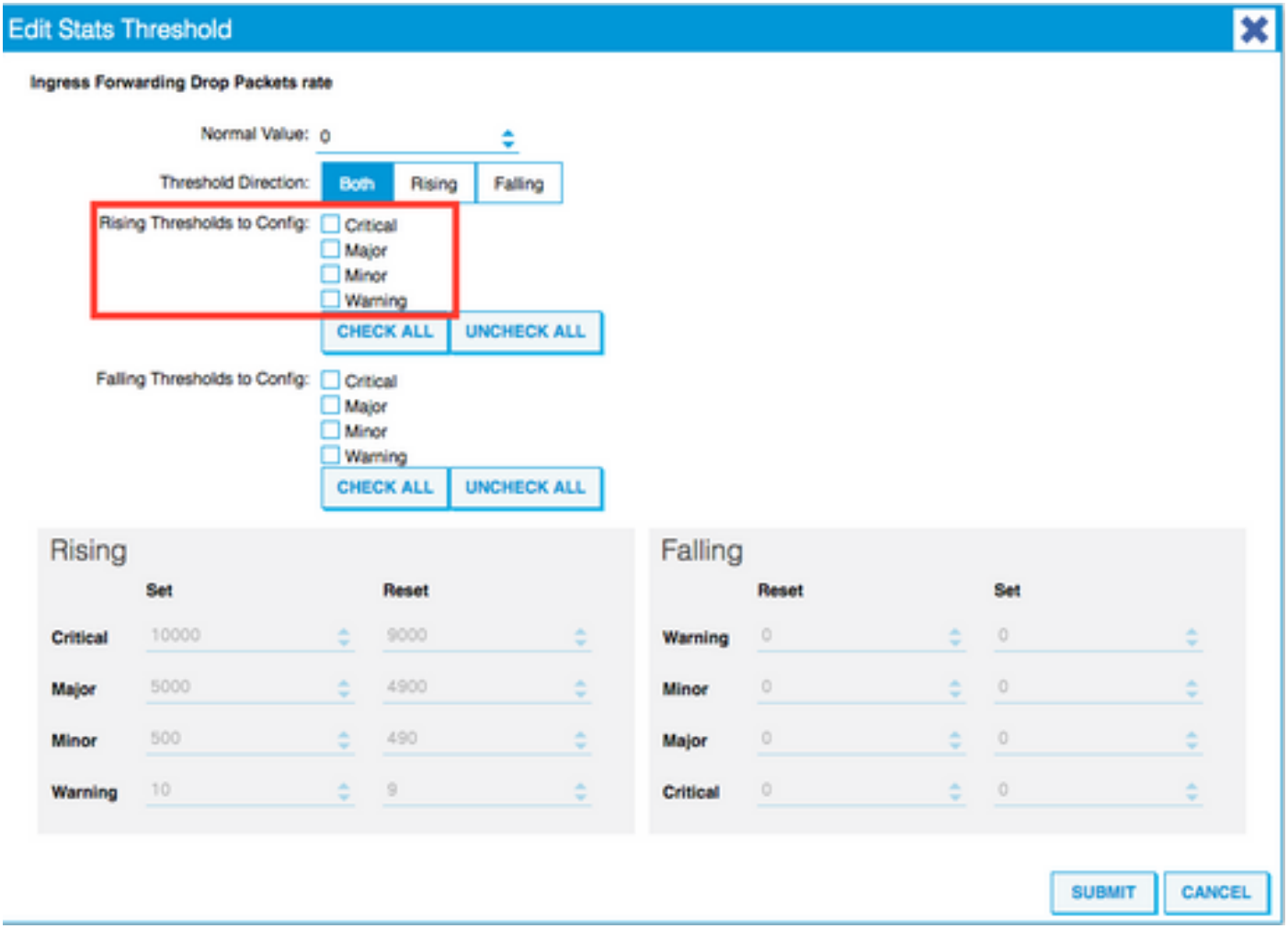
6.按一下「配置閾值」旁邊的+按鈕



7. 編輯轉發丟棄的閾值

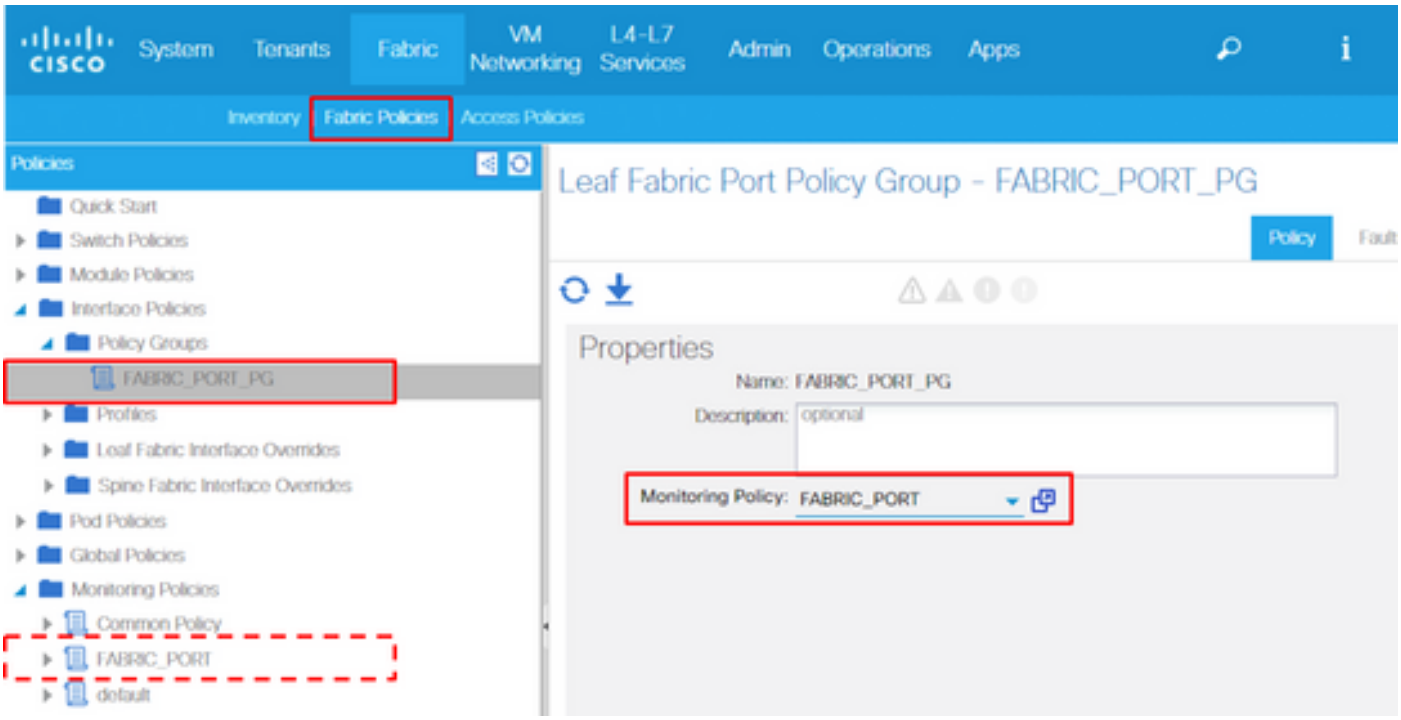


8. 建議停用遞增閾值，以配置嚴重、主要、次要和警告的轉發丟包率。



9. 將此新的監控策略應用於所需埠的介面策略組。請不要忘記在交換矩陣策略中相應配置介面配置檔案、交換機配置檔案等。

（使用預設策略時，可以跳過此步驟9）

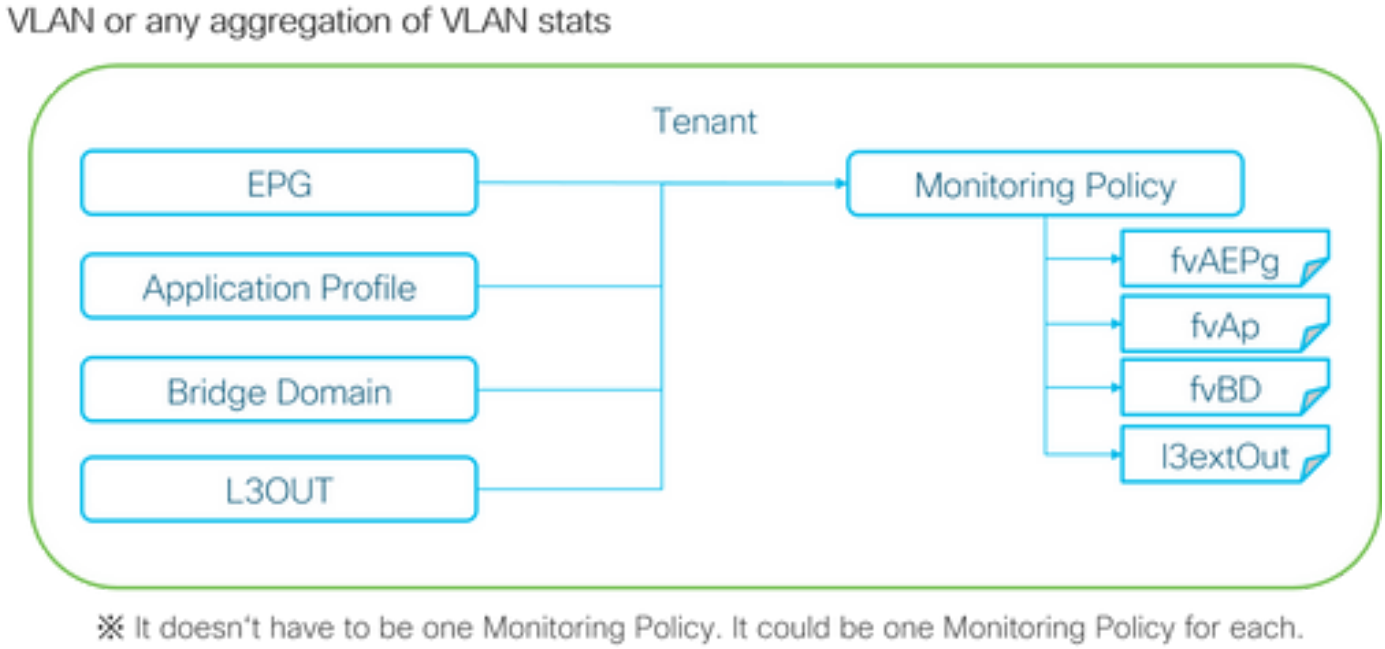


10. 如果這是針對前面板連線埠（存取原則），請對彙總介面(pc.AggrIf)執行與第1層實體介面組態(l1.PhysIf)相同的工作，如此一來，新的監控原則即可套用至連線埠通道以及實體連線埠。

（使用預設策略時，可以跳過此步驟10）

l2IngrPktsAg中的入口丟棄資料包速率

這個有好幾個部分。



如上圖所示，l2IngrPktsAg在許多對象下受到監控。上圖只顯示部分範例，但不會顯示l2IngrPktsAg的所有物件。但是，統計資訊的閾值是透過監控策略以及l1PhysIf或pcAggrIf下的eqptIngrDropPkts配置的。

每個對象(EPG(fvAEPg)、網橋域(fvBD)等)都可以為其分配自己的監控策略，如上圖所示。

預設情況下，除非另外進行配置，否則租戶下的所有這些對象都將使用Tenant > Common > Monitoring Policies > default下的default Monitoring Policy。

除非需要更改每個元件的閾值，否則可以直接修改租戶common下的預設監控策略，以將更改應用於所有相關元件。

以下示例更改網橋域中l2IngrPktsAg15min的入口丟棄資料包速率的閾值。

1. 導航到租戶>（租戶名稱）>監控策略。

（如果使用預設監控策略，或者需要跨租戶應用新的監控策略，則租戶必須是通用的）

2. 按一下滑鼠右鍵並選取「建立監督原則」。

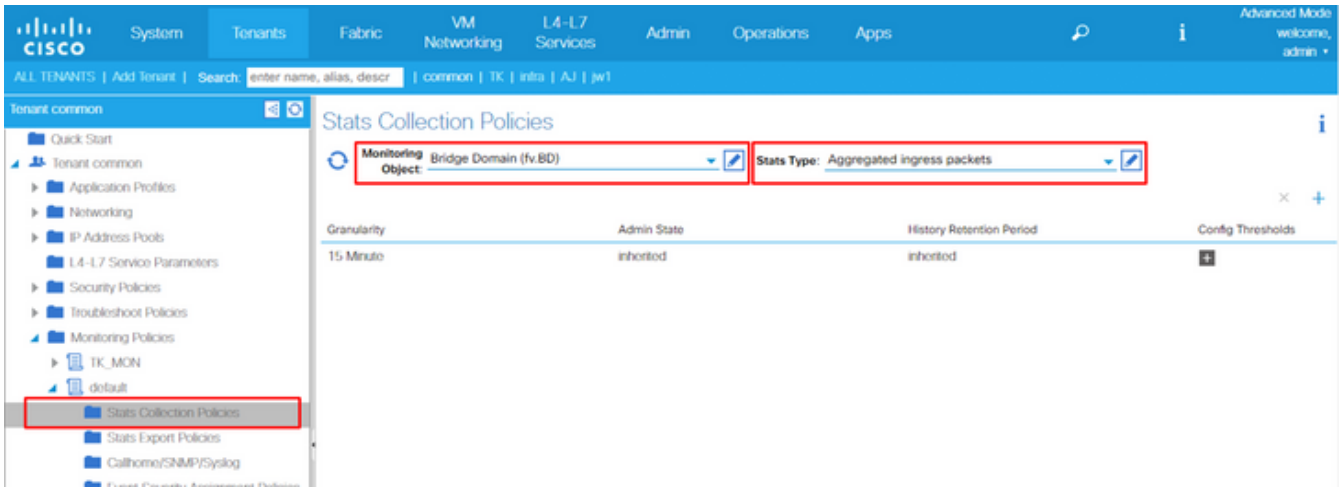
(如果閾值更改可應用於所有元件，請導航到default，而不是建立新元件)

3. 展開新的「監控政策」或預設值，然後定位至統計資料收集政策。

4. 按一下右窗格上「監督物件」的鉛筆圖示，選取「橋接網域(fv.BD)」。

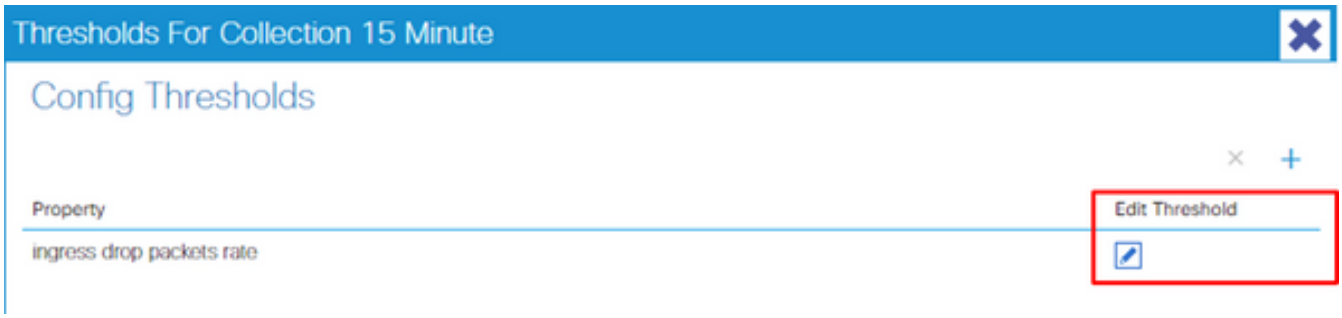
（使用預設策略時，可以跳過此步驟4）

5. 從右側窗格中的Monitoring Object下拉選單中選擇Bridge Domain (fv.BD)和Stats Type，然後選擇Aggregated ingress packets。

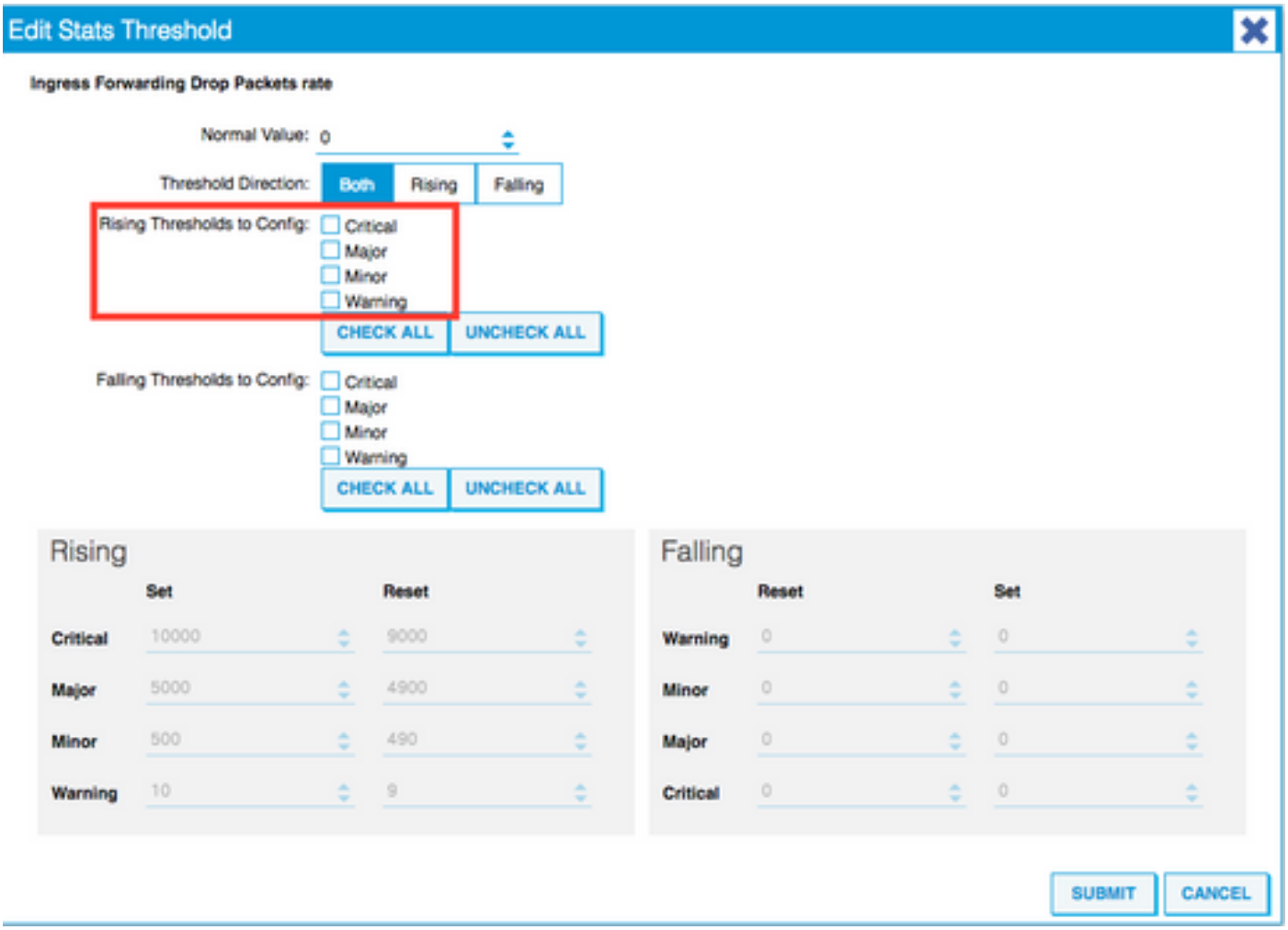


6.按一下「配置閾值」旁邊的+按鈕

7. 編輯轉發丟棄的閾值

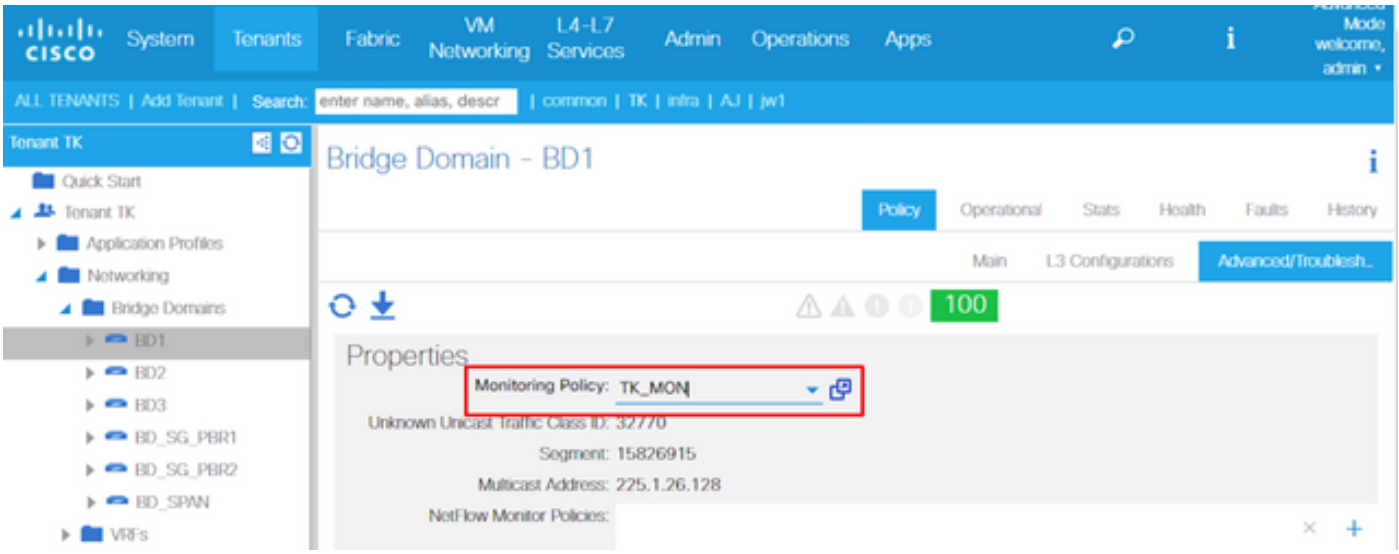


8. 建議停用遞增閾值，以配置嚴重、主要、次要和警告的轉發丟包率。



9. 將此新監控策略應用於需要更改閾值的網橋域。

（使用預設策略時，可以跳過此步驟9）



附註

非預設監控策略可能沒有預設監控策略上的配置。如果需要保持這些配置與預設監控策略相同，則使用者需要檢查預設監控策略配置，並在非預設監控策略上手動配置相同策略。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。