丢包故障的说明在ACI的

目录

简介

当您看到此故障时，本文描述每个故障类型和步骤。在Cisco应用中心基础设施(ACI)结构的正常Operaton期间，管理员可能为丢包特定类型发现故障。

贡献用约瑟夫Ristaino，多久也Kishida， Cisco TAC工程师。

托管对象

在思科ACI中，所有故障被上升在托管对象(MO)下。例如，故障“*F11245 -入口丢弃数据包rate(l2IngrPktsAg15min:dropRate)*”在MO *l2IngrPktsAg15min*看待参数*dropRate*。

此部分引入一些示例**托管对象(MO)涉及丢弃数据包故障**。

	示例	说明	示例参数
l2IngrPkts	l2IngrPkts5min l2IngrPkts15min l2IngrPkts1h 等等。	在每个期限，这代表入口信息包统计数据每个VLAN	dropRat floodRa multicas unicastF
l2IngrPktsAg	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d 等等。	这等等代表入口信息包统计数据每个EPG、BD，VRF。 例如。) EPG stats代表的VLAN stats聚合属于EPG	dropRat floodRa multicas unicastF
eqptIngrDropPkts	eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d 等等。	在每个期限，这代表入口丢弃数据包统计信息每个接口	*1 forward *1 error *1 buffe

*1 ：在eqptIngrDropPkts的这些计数器从1.3(2)版本不再使用由于a - EX在向前丢弃的平台限制与SUP_REDIRECT。

请注释此实施可能在将来再更改。

硬件丢弃计数器类型

在连结运行在ACI模式的9000交换机，那里是入口接口丢弃原因的3个主要硬件计数器在ASIC。

在l2IngrPkts的一dropRate， l2IngrPktsAg包括那些计数器。三个参数(forwardingRate、errorRate， bufferRate)在eqptIngrDropPkts的上表代表每三个接口计数器。

前言

向前丢包，是在查找块的数据包(LU)被丢弃ASIC。在LU块中，信息包转发决定做基于信息包报头题头信息。如果决策是丢弃数据包，请转发丢弃计数。这可能发生的有各种各样的原因，但是请谈论主要部分：

SECURITY_GROUP_DENY

一丢弃由于缺少合同允许通信。

当数据包输入结构时，交换机查看源和目的EPG发现是否有允许此通信的合同。 如果源和目的用不同的EPG，并且没有允许在他们之间的此数据包类型的合同，交换机将丢弃数据包并且标记它作为SECURITY_GROUP_DENY。这增加向前丢弃计数器。

VLAN_XLATE_MISS

一丢弃由于不相应的VLAN。

当数据包输入结构时，交换机查看数据包确定在端口的配置是否允许此数据包。 例如，帧进入与802.1Q标记的结构10。 如果交换机有在端口的VLAN10，将检查内容并且做出根据目的地MAC的转发决策。 然而，如果VLAN10不在端口，它将丢弃它并且标记它作为VLAN_XLATE_MISS。 这将增加向前丢弃计数器。

“XLATE的”原因或“翻译”是，因为在ACI，分支交换机将采取有802.1Q encap的一帧并且翻译它对将使用VXLAN和其他标准化在结构里面的新的VLAN。 如果帧进来与没部署的VLAN， “转换”将发生故障。

ACL_DROP

一丢弃由于SUP TCAM。

在ACI交换机的SUP TCAM包含特殊规则应用在正常L2/L3转发决策顶部。在SUP TCAM的规则是可配置而不是内置的用户。SUP TCAM规则目标主要将处理一些没打算的例外或的一些控制层面流量和由用户检查或监控。当数据包点击SUP TCAM规则时，并且规则是丢弃数据包，丢弃的数据包计数，因为ACL_DROP和将增加向前丢弃计数器。当发生的这，它通常含义时数据包将转发基本ACI转发负责人。

注意，即使丢弃名称是ACL_DROP，此“ACL”不是同在独立NX-OS设备或所有其他路由/swtching的设备可以配置的正常一样访问控制表。

SUP_REDIRECT

这不是丢弃。

一口重定向的数据包(即等等CDP/LLDP/UDLD/BFD)可能算作是向前数据包正确地处理并且转发对CPU的丢弃均等想法。

这可能发生只- EX平台例如N9K-C93180YC-EX。这些不应该算作是“由于ASIC限制-EX平台的丢弃”然而。

错误

当交换机接收一无效帧时，丢弃作为错误。 此的示例包括有FCS或CRC错误的帧。

缓冲区

当交换机接收帧，并且没有缓冲区信用值可用为入口或出口，帧用“缓冲区”将丢弃。 这典型地暗示拥塞某处在网络。 显示故障可能全双工的链路或者，包含目的地的链路可能拥塞。

查看在CLI的丢弃统计

托管对象

安全壳SSH到一个APIC和运行根据命令。

apic1# **moquery - c l2IngrPktsAg15min**

这为此类l2IngrPktsAg15min将提供所有对象例程。

这是一示例以查询一个特定对象的过滤器。在本例中，过滤器是显示与属性**dn的仅**一个对象哪些包括"tn-TENANT1/ap-APP1/epg-EPG1"。

并且此示例使用egrep显示仅需要的属性。

示例输出1 ：EPG计数器对象(l2IngrPktsAg15min)承租人TENANT1，应用配置文件APP1，epg EPG1。

```
apic1# 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
```

或者我们可能使用另一个选项**- d**而不是**-**获得一个特定对象的**c**是否认识对象dn。

示例输出2 ：EPG计数器对象(l2IngrPktsAg15min)承租人TENANT1，应用配置文件APP1，epg EPG2。

```
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
```

硬件计数器

使用CLI，如果看到故障或者要检查在连接孔的丢包，要执行此的最佳方法是通过查看平台计数器在硬件方面。使用**show interface ,** 多数，但是不是所有的计数器显示。 使用平台计数器，3个主要丢弃原因可能只查看。 为了查看这些，执行这些步骤：

分支

运行SSH对分支和这些命令。

ACI-LEAF# **vsh_lc**
module-1#**显示平台内部计数器端口<x>**
* X代表端口号的地方

etherent 1/31的示例输出：

```
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 -----
```

脊椎

对于一块箱式脊椎(N9K-C9336PQ)，它正确地是同分支一样。

对于模块化脊椎(等等N9K-C9504)，您必须首先附加特定的线路卡，在您能查看平台计数器前。 运行SSH对脊椎和这些命令

ACI-SPINE# **vsh**

ACI-SPINE#**附上模块<x>**

module-2#**显示平台内部计数器端口<y>**。

* X代表您希望查看的线卡的地方模块号

Y代表端口号

以太网的2/1示例输出：

```
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

F11245 -入口丢弃信息包速率(l2IngrPktsAg15min:dropRate)

说明：

当Layer2数据包被撤销与“向前丢弃”原因时，此故障能增加。 因为有各种各样不同的原因，

最普通一个是：

在- EX平台例如N9K-C93180YC-EX，有L2数据包需要重新定向到CPU的限制(即CDP/LLDP/UDLD/BFD等等)，将被记录，因为“向前丢弃”以及复制对CPU。 这归结于用于连结9000的EX型号的限制关于ASIC。

因此，当大量控制层面协议在接口时启用，这些故障可能被上升。

解决方法：

因为没有服务影响，最佳实践推荐是增加故障的阈值如**统计阈值**部分所显示。 为了执行此，请参阅在统计阈值的说明。

F100264 -入口缓冲区丢弃信息包速率(eqptIngrDropPkts5min:bufferRate)

说明：

此故障能增加，当数据包在与原因“缓冲区”的端口丢弃如上所述时，这典型地发生，当有在接口的拥塞在入口或输出方向。

解决方法：

此故障表示在环境的实际丢弃的数据包由于拥塞。 丢弃的数据包可能导致与运行的应用程序的问题的ACI结构。 网络管理员应该隔离数据包流和确定拥塞是否归结于意外的通信流、效率低的负载均衡等等;或者在那些端口的预计利用率。

F100696 -入口转发丢弃数据包(eqptIngrDropPkts5min:forwardingRate)

注意：开始在版本1.3(2)，向前丢包从eqptIngrDropPkts5min对象删除，因此不应该为此问题看到此故障。

此故障是由一些个方案造成的。 最普通一个是：

说明1)脊椎丢包

当ARP或IP数据包转发对代理查找的脊椎，并且终端是未知在结构，一特殊汇集数据包将生成并且发送到在适当的BD的所有分支
组播组地址。 这将触发从每个分支的一个ARP请求在网桥域(BD)发现终端。 由于限制，分支接收的汇集数据包也反射
回到结构和触发在脊椎链路的一转发丢弃。 向前丢弃在生成1脊椎硬件只被增加。

解决方法1)

因为您知道问题是由发送未知单播流量的设备导致的到ACI结构，设备导致这的您需要推测和发现是否可以防止它。 这通常是由为在子网的IP地址为监控目的扫描或探查的设备造成的。 为了查找什么IP发送此流量，在连接对显示故障的脊椎接口的分支上的SSH。

从那里，您能运行此命令发现源IP地址(sip)触发汇集数据包：

```
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 = Rece
ived 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 = Rece
ived 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 = Rece
ived 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 = Rece
ived glean packet is an IP packet
```

从那里，您能调查192.168.21.150为什么发送此流量到结构和看到是否能从那里缓和它。

说明2)分支丢包

如果此故障在分支接口被看到，很可能casue归结于被提及的SECURITY_GROUP_DENY丢包。

解决方法2)

在分支上，您保持拒绝的数据包日志由于收缩侵害。仍然提供您大量的日志的此日志不捕获所有保护CPU资源然而。

要获得日志什么您想要，如果接口故障被上升是Port-Channel的一部分，您需要使用此命令和grep Port-Channel。 否则，您能使用物理接口：

此日志可以根据相当数量合同丢包迅速滚动。

```
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: 0x8c604
f0288fc, 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: 0x8c604
f0288fc, 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 500387 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, 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 499779 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, 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 499624 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
```

```
Id: 59, SMac: 0x8c604
f0288fc, 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
```

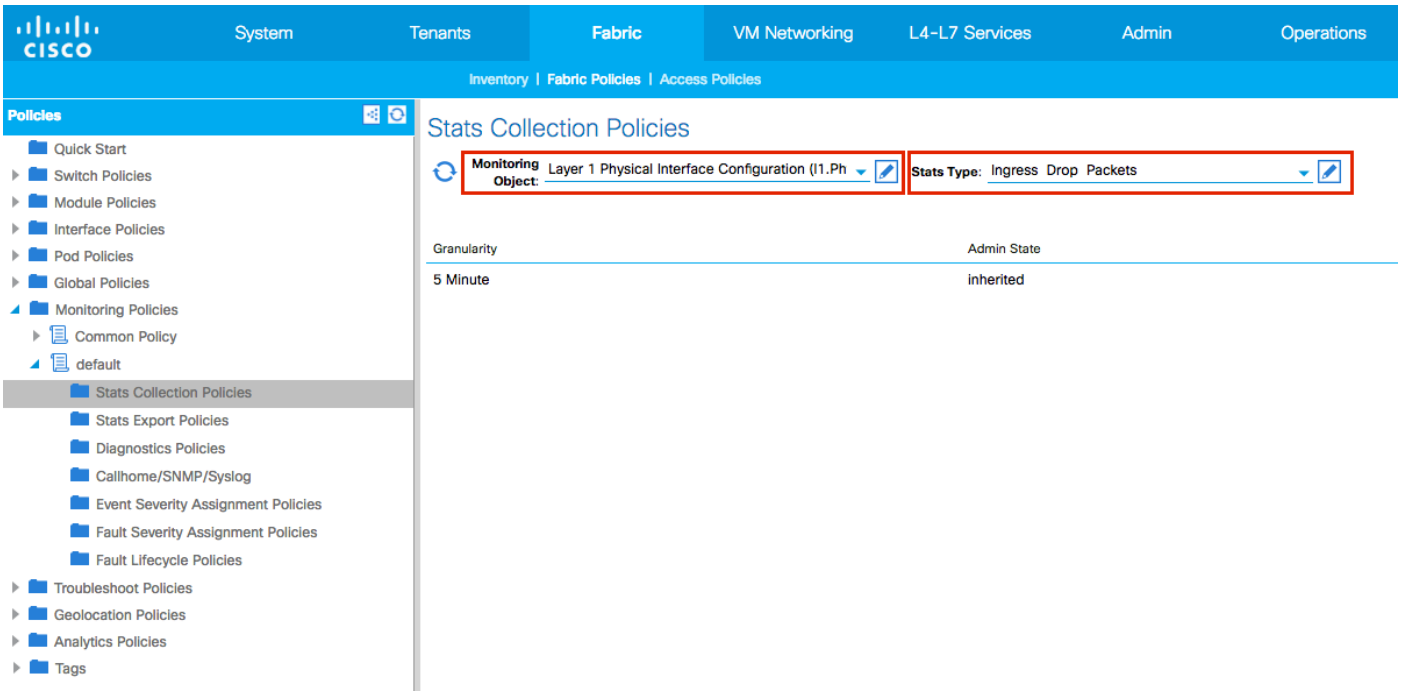
在这种情况下， 192.168.21.150尝试传送ICMP信息(对192.168.20.3的IP协议号1)。 然而，没有允许ICMP在2个EPG的之间的合同，因此数据包丢弃。 如果ICMP应该允许，合同可以被添加在两个EPG之间。

统计阈值

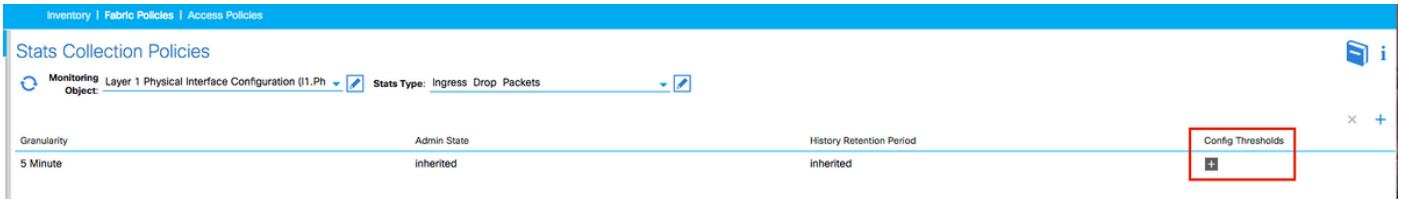
此部分描述如何更改的一阈值可能潜在培养故障agaist丢弃计数器的统计信息对象。

以下示例是更改向前*丢弃的*阈值在*eqptIngrDropPkts*。

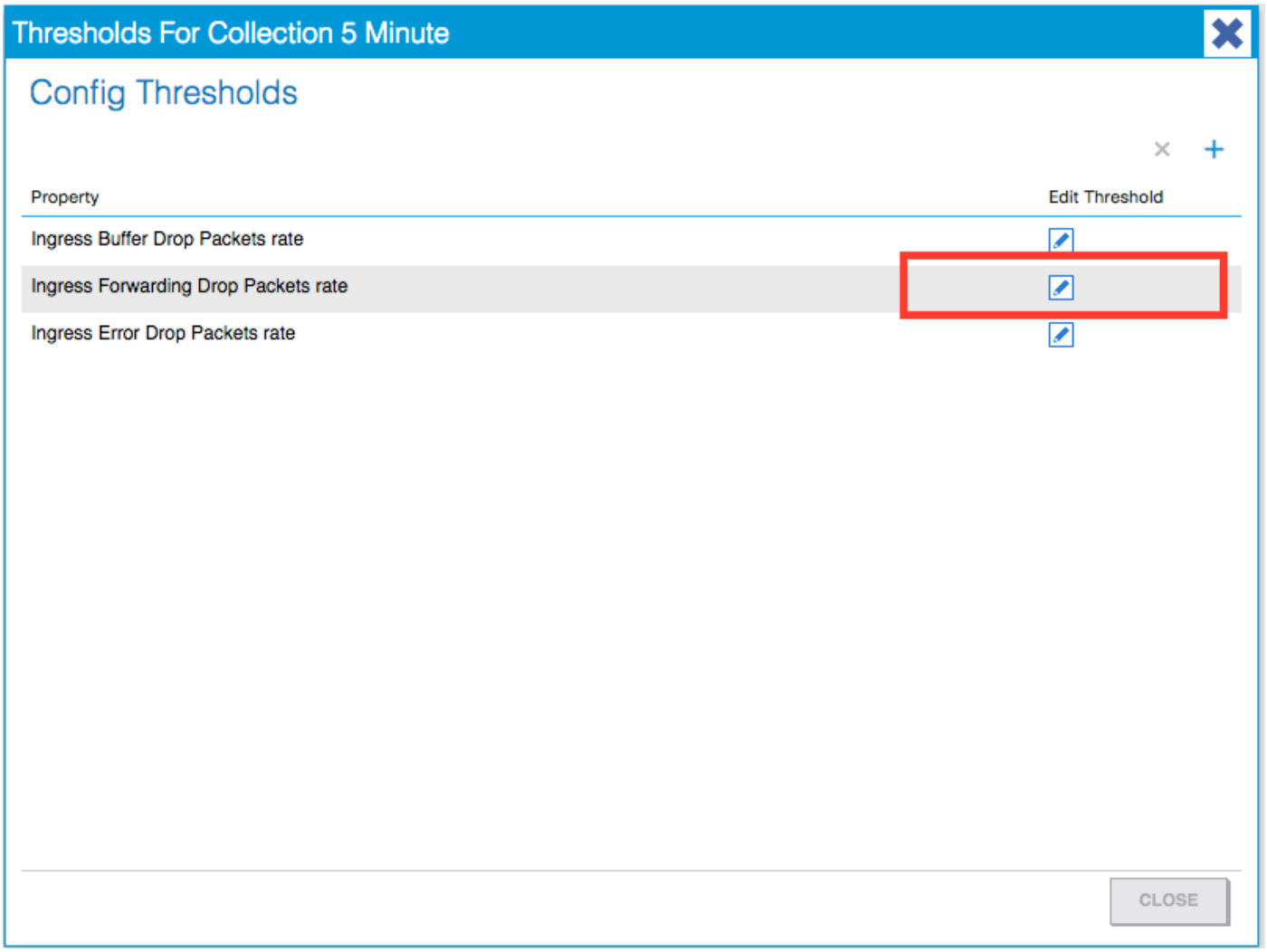
1. 导航对**>Monitoring策略>默认>Stats的结构>Fabric策略集策略。**
2. 从**监听对象请**丢弃下来，选择**第1层物理接口配置(l2.PhysIf)，**并且**统计类型**，选择**入口丢弃数据包**



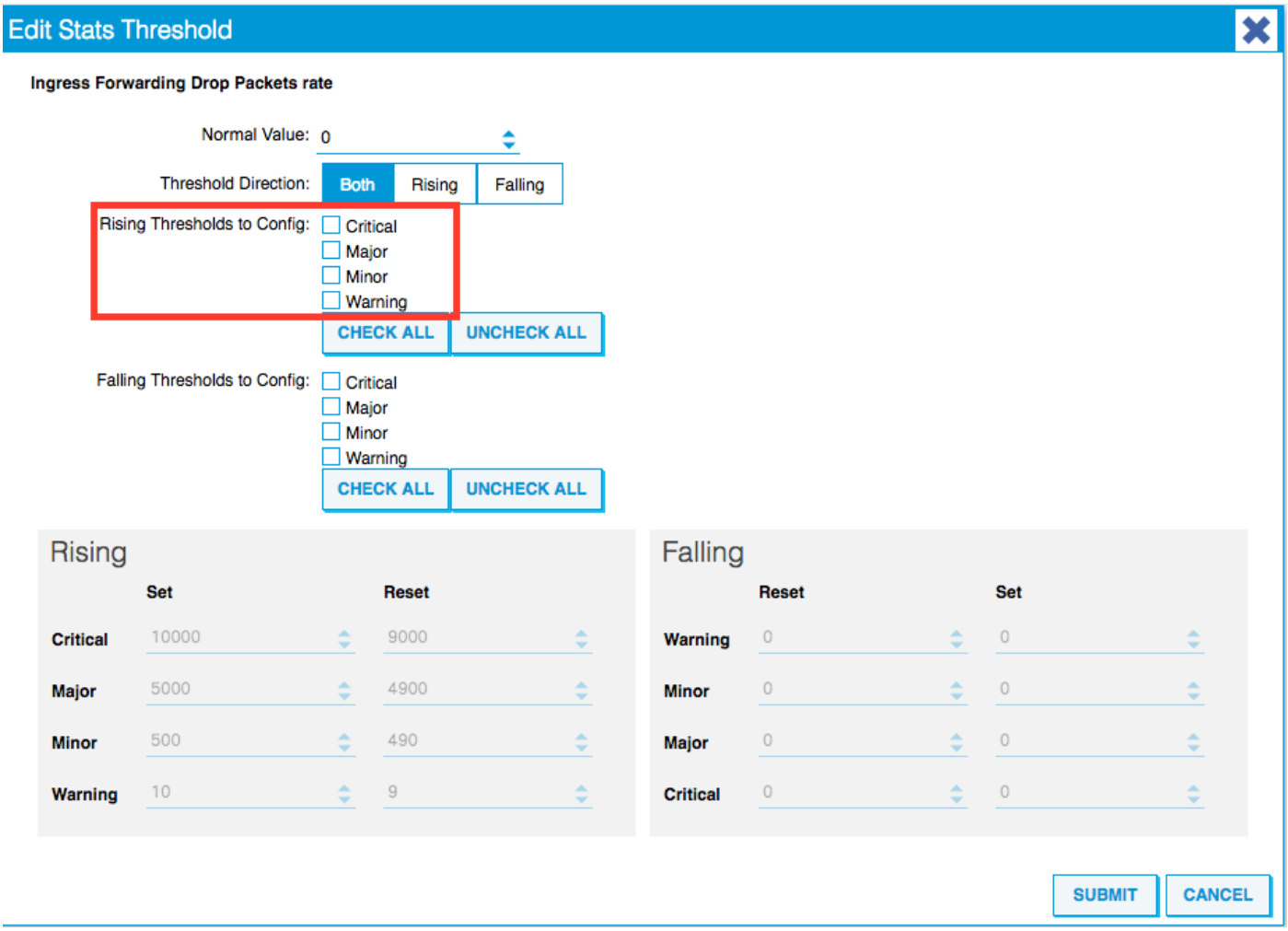
3. 在设置阈值旁边点击+



4.编辑缓冲丢弃的阈值



5. 建议是禁用上升阀为重要，专业，较小和警告配置转发的丢弃速率。


Edit Stats Threshold
Ingress Forwarding Drop Packets rate
Normal Value: 0
Threshold Direction: Both Rising Falling
Rising Thresholds to Config: Critical Major Minor Warning
CHECK ALL UNCHECK ALL
Falling Thresholds to Config: Critical Major Minor Warning
CHECK ALL UNCHECK ALL
Rising
Set Reset
Critical 10000 9000
Major 5000 4900
Minor 500 490
Warning 10 9
Falling
Reset Set
Warning 0 0
Minor 0 0
Major 0 0
Critical 0 0
SUBMIT CANCEL