Erläuterung von Paketverlust-Fehlern in der ACI

Inhalt

Einführung

In diesem Dokument werden die einzelnen Fehlertypen und die Vorgehensweise beschrieben, wenn Sie diesen Fehler sehen. Beim normalen Betrieb einer Cisco Application Centric Infrastructure (ACI)-Fabric sieht der Administrator möglicherweise Fehler für bestimmte Arten von Paketverlusten.

Verwaltete Objekte

In der Cisco ACI werden alle Fehler unter Managed Objects (MO) ausgelöst. Beispielsweise bezieht sich der Fehler "*F11245 - Ingress Drop Packets Rate(l2IngrPktsAg15min:dropRate)*" auf den Parameter *dropRate* in MO *l2IngrPktsAg15min*.

In diesem Abschnitt werden einige Beispiele für **Managed Object (MO) in Bezug auf Paketfehler im Drop-Paket** vorgestellt.

	Beispiel	Beschreibung	Beispielparameter	Beispiel-MO gegen die Störungen hervorrufen
l2IngrPkte	l2IngrPkts5min l2IngrPkte15min l2IngrPkts1h usw.	Dies stellt Statistiken zu eingehenden Paketen pro VLAN während jedes Zeitraums dar.	DropRate Überschwemmungsrate Multicast-Rate Unicast-Rate	vlanCktEp (VLAN)
l2IngrPktsAG	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d usw.	Dies stellt Statistiken über Eingangspakete pro EPG, BD, VRF usw. dar. Beispiel:) EPG-Statistiken stellen die Aggregation von VLAN-Statistiken dar, die zur EPG gehören.	DropRate Überschwemmungsrate Multicast-Rate Unicast-Rate	fvAEPg (EPG) fvAP (Anwendungsprofil) FvBD (BD) l3extOut (L3OUT)
eqptIngrDropPkte	eqptIngrDropPkte15Min. eqptIngrDropPkts1h eqptIngrDropPkts1d usw.	Dies stellt Statistiken zu eingehenden Drop-Paketen pro Schnittstelle während jedes Zeitraums dar.	*1 Weiterleitungsrate *1 Fehlerrate *1 Pufferrate	l1PhysIf (physischer Port) pcAggrIf (Port-Channel)

*1: Diese Zähler in eqptIngrDropPkts können aufgrund einer ASIC-Einschränkung in mehreren Nexus 9000-Plattformen falsch angehoben werden, da SUP_REDIRECT-Pakete als Weiterleitungs-Drops protokolliert werden. Siehe auch CSCvo68407 und CSCvn72699 für weitere Details und feste Versionen.

Hardware-Drop-Zählertypen

Auf Nexus 9000-Switches, die im ACI-Modus ausgeführt werden, gibt es drei Hauptrechenzentren für die Eingangs-Schnittstelle, die im ASIC abgelegt werden.

Eine DropRate in l2IngrPkts, l2IngrPktsAg beinhaltet diese Zähler. Die drei Schnittstellenindikatoren repräsentieren drei Parameter (ForwardingRate, errorRate, bufferRate) in der obigen Tabelle für eqptIngrDropPkts.

Weiterleiten

Weiterleitungsverwerfen sind Pakete, die im LookUp-Block (LU) des ASIC verworfen werden.

Im LU-Block wird eine Paketweiterleitungsentscheidung basierend auf den Informationen des Paket-Headers getroffen. Wenn entschieden wird, das Paket zu verwerfen, wird Forward Drop gezählt. Es gibt verschiedene Gründe, warum dies passieren kann, aber lassen Sie uns über die wichtigsten Gründe sprechen:

SECURITY_GROUP_DENY

Ein Tropfen wegen fehlender Verträge, um die Kommunikation zu ermöglichen.

Wenn ein Paket in die Fabric eingeht, prüft der Switch die Quell- und Ziel-EPG, um festzustellen, ob ein Vertrag besteht, der diese Kommunikation zulässt. Wenn sich Quelle und Ziel in unterschiedlichen EPGs befinden und kein Vertrag besteht, der diesen Pakettyp zwischen ihnen zulässt, verwirft der Switch das Paket und benennt es als SECURITY_GROUP_DENY. Dadurch wird der Zähler für Weiterleitungs-Drop erhöht.

VLAN_XLATE_MISS

Ein Drop aufgrund eines ungeeigneten VLANs.

Wenn ein Paket in die Fabric eingeht, prüft der Switch das Paket, um festzustellen, ob die Konfiguration auf dem Port dieses Paket zulässt. Ein Frame gelangt beispielsweise mit einem 802.1Q-Tag von 10 in das Fabric. Wenn der Switch VLAN 10 auf dem Port hat, prüft er den Inhalt und trifft eine Weiterleitungsentscheidung auf der Grundlage der Ziel-MAC. Wenn sich VLAN 10 jedoch nicht auf dem Port befindet, wird es verworfen und als VLAN_XLATE_MISS bezeichnet. Dadurch wird der Zähler für Weiterleitungs-Drop erhöht.

Der Grund für "XLATE" oder "Translate" ist, dass der Leaf-Switch in der ACI einen Frame mit einer 802.1Q-Encap annimmt und in ein neues VLAN übersetzt, das für VXLAN und andere Normalisierungen innerhalb der Fabric verwendet wird. Wenn der Frame mit einem nicht bereitgestellten VLAN eingeht, schlägt die "Übersetzung" fehl.

ACL_DROP

Ein Tropfen aufgrund von sup-tcam.

sup-tcam in ACI-Switches enthält spezielle Regeln, die zusätzlich zur normalen L2/L3-Weiterleitungsentscheidung angewendet werden. Regeln in sup-tcam sind integriert und können nicht vom Benutzer konfiguriert werden. Die Sup-Tcam-Regeln sollen hauptsächlich Ausnahmen oder bestimmte Datenverkehrsmengen auf Kontrollebene behandeln und nicht von Benutzern überprüft oder überwacht werden. Wenn das Paket die sup-tcam-Regeln einhält und die Regel darin besteht, das Paket zu verwerfen, wird das verworfene Paket als ACL_DROP gezählt und erhöht den Weiterleitungs-Drop-Zähler. Dies bedeutet in der Regel, dass das Paket an grundlegende ACI-Weiterleitungs-Prinzipien weitergeleitet wird.

Beachten Sie, dass diese "ACL", obwohl der Drop-Name "ACL_DROP" ist, nicht mit der normalen Zugriffskontrollliste übereinstimmt, die auf eigenständigen NX-OS-Geräten oder anderen Routing-/Switching-Geräten konfiguriert werden kann.

SUP_REDIRECT

Das ist kein Tropfen.

Ein Sup-umgeleitetes Paket (z. B. CDP/LLDP/UDLD/BFD usw.) kann als Forward Drop gezählt werden, selbst wenn das Paket korrekt verarbeitet und an die CPU weitergeleitet wurde.

Dies kann nur bei der -EX-Plattform wie N9K-C93180YC-EX auftreten. Diese sollten nicht als "Drop" gezählt werden, allerdings aufgrund der ASIC-Einschränkung in der -EX-Plattform.

Fehler

Wenn der Switch einen ungültigen Frame an einer der Schnittstellen an der Vorderseite empfängt, wird er als Fehler verworfen. Beispiele hierfür sind Frames mit FCS- oder CRC-Fehlern.
Im Normalbetrieb wird jedoch erwartet, dass Fehlerpakete auf Uplink-Ports von Leafs oder Spine-Ports inkrementiert werden. Bei Uplink-Leaf-Ports oder Spine-Ports ist es am besten, FCS/CRC-Fehler mithilfe von "show interface" zu überprüfen.

Puffer

Wenn der Switch einen Frame empfängt und keine Puffer-Credits für ein- oder ausgehenden Datenverkehr verfügbar sind, wird der Frame mit "Buffer" verworfen. Dies deutet in der Regel auf eine Überlastung im Netzwerk hin. Die Verbindung, die den Fehler anzeigt, kann voll sein, oder die Verbindung, die das Ziel enthält, kann überlastet sein.

Anzeigen von Drop Stats in der CLI

Verwaltete Objekte

Secure Shell (SSH) auf einen der APIC zugreifen und die folgenden Befehle ausführen.

apic1# **moquery -c l2IngrPktsAg15min**

Dadurch werden alle Objektinstanzen für diese Klasse l2IngrPktsAg15min bereitgestellt.

Hier ein Beispiel mit einem Filter, um ein bestimmtes Objekt abzufragen. In diesem Beispiel zeigt der Filter nur ein Objekt mit den Attributen **dn** an, das "tn-TENANT1/ap-APP1/epg-EPG1" enthält.

In diesem Beispiel wird mit einem Verweis auf den Verweis nur die erforderlichen Attribute angezeigt.

Beispielausgabe 1: EPG-Zählerobjekt (l2IngrPktsAg15min) des Tenant TENANT1, Anwendungsprofil 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
```

Oder wir könnten eine andere Option **-d** anstelle von **-c** verwenden, um ein bestimmtes Objekt zu erhalten, wenn Sie das Objekt dn kennen.

Beispielausgabe 2: EPG-Zählerobjekt (l2IngrPktsAg15min) des Tenant TENANT1, Anwendungsprofil 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
```

Hardwarezähler

Wenn Sie Fehler sehen oder Paketverluste auf Switch-Ports mithilfe der CLI überprüfen möchten, sollten Sie dies am besten durch Anzeigen der Plattformzähler in der Hardware tun. Die meisten, aber nicht alle Zähler werden mithilfe der **Show-Schnittstelle** angezeigt. Die drei Hauptgründe für einen Ausfall können nur mit den Plattformzählern angezeigt werden. So zeigen Sie diese an:

Leaf

SSH zum Leaf und führen Sie diese Befehle aus.

ACI-LEAF# **vsh_lc**
module-1# **show platform internal counter port <X>**
*** wobei X für die Portnummer steht**

Beispielausgabe für Ethernet 1/31:

```
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 -----
```

Spine

Bei einem Boxtyp-Spine (N9K-C9336PQ) ist er genau identisch mit Leaf.

Bei modularen Spines (N9K-C9504 usw.) müssen Sie zunächst die jeweilige Linecard anschließen, bevor Sie die Plattformzähler anzeigen können. SSH am Spine und Ausführung dieser Befehle

ACI-SPINE# **vsh**

ACI-SPINE# **Attach-Modul <X>**

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

* wobei X die Modulnummer für die Linecard darstellt, die Sie anzeigen möchten.

Y steht für die Portnummer

Beispielausgabe für Ethernet 2/1:

```
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 -----
```

Fehler

F112425 - Rate der eingehenden Pakete (l2IngrPktsAg15min:dropRate)

Beschreibung:

Einer der beliebten Gründe für diesen Fehler ist, dass Layer-2-Pakete mit dem Grund "Forward Drop" verworfen werden. Es gibt verschiedene Gründe, aber die häufigste ist:

Auf einigen Plattformen (siehe CSCvo68407)), es gibt eine Einschränkung, bei der L2-Pakete, die an die CPU umgeleitet werden müssen (z. B. CDP/LLDP/UDLD/BFD usw.), als "Forward Drop" protokolliert und in die CPU kopiert werden. Dies ist auf eine Einschränkung der in diesen Modellen verwendeten ASIC zurückzuführen.

Auflösung:

Die oben beschriebenen Tropfen sind rein kosmetisch, daher Die Best Practice-Empfehlung besteht darin, den Grenzwert für den Fehler zu erhöhen, wie im Abschnitt **"Statistische Schwellenwerte"** dargestellt. Beachten Sie dazu die Anweisungen im Grenzwert für Statistiken.

F100264 - Paketrate des Eingangspuffers (eqptIngrDropPkts5min:bufferRate)

Beschreibung:

Dieser Fehler kann sich erhöhen, wenn Pakete auf einem Port mit dem Grund "Puffer" verworfen werden. Wie oben erwähnt, geschieht dies in der Regel, wenn eine Schnittstelle in Eingangs- oder Ausgangsrichtung überlastet ist.

Auflösung:

Dieser Fehler stellt die aufgrund einer Überlastung tatsächlich verworfenen Pakete in der Umgebung dar. Die verworfenen Pakete können Probleme mit Anwendungen verursachen, die in der ACI-Fabric ausgeführt werden. Netzwerkadministratoren sollten den Paketfluss isolieren und ermitteln, ob die Überlastung auf unerwartete Datenverkehrsflüsse, ineffizienten Lastenausgleich usw. zurückzuführen ist. oder erwartete Nutzung an diesen Ports.

F100696 - Drop-Pakete für die eingehende Weiterleitung (eqptIngrDropPkts5min:ForwardingRate)

Hinweis: Eine ASIC-Einschränkung wie oben für F11245 erwähnt kann dazu führen, dass diese Fehler ebenfalls ausgelöst werden. Siehe CSCvo68407 für weitere Informationen.

Dieser Fehler wird durch einige Szenarien verursacht. Die häufigste ist:

Beschreibung 1) Spine Drops

Wenn dieser Fehler auf einer Spine-Schnittstelle angezeigt wird, kann er auf Datenverkehr zu einem unbekannten Endpunkt zurückzuführen sein.

Wenn ein ARP oder ein IP-Paket zur Proxy-Suche an den Spine weitergeleitet wird und der Endpunkt in der Fabric unbekannt ist, wird ein spezielles Glean-Paket generiert und an alle Leafs der entsprechenden BD-Multicast-Gruppenadresse (intern) gesendet. Dadurch wird von jedem Leaf in der Bridge-Domäne (BD) eine ARP-Anforderung ausgelöst, um den Endpunkt zu ermitteln. Aufgrund einer Einschränkungwird das vom Leaf empfangene Glean-Paket ebenfalls wieder in die Fabric übernommen und löst einen Weiterleitungs-Drop auf der Spine-Verbindung aus, die mit dem Leaf verbunden ist. Der Weiterleitungs-Drop in diesem Szenario wird nur auf Spine-Hardware der Generation 1 erhöht.

Resolution 1)

Da bekannt ist, dass das Problem dadurch verursacht wird, dass ein Gerät eine unnötige Menge von Unicast-Datenverkehr an die ACI-Fabric sendet, muss ermittelt werden, welches Gerät diese Ursache verursacht, und überprüft werden, ob diese verhindert werden kann. Dies wird in der Regel durch Geräte verursacht, die IP-Adressen in Subnetzen zu Überwachungszwecken scannen oder abfragen. Um zu ermitteln, welche IP-Adresse diesen Datenverkehr sendet, wird SSH auf das Leaf gesetzt, das mit der Spine-Schnittstelle verbunden ist und den Fehler anzeigt.

Von dort können Sie diesen Befehl ausführen, um die Quell-IP-Adresse (SIP) anzuzeigen, die das Gateway auslöst:

```
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
```

In der Ausgabe dieses Beispiels wird das glean-Paket durch 192.168.21.150 ausgelöst. Es wird empfohlen zu prüfen, ob dies verringert werden kann.

Beschreibung 2) Leaf Drops

Wenn dieser Fehler auf einer Leaf-Schnittstelle auftritt, ist der wahrscheinlichste Fall auf die erwähnten SECURITY_GROUP_DENY-Drops zurückzuführen.

Resolution 2)

Das ACI-Leaf speichert ein Protokoll von Paketen, die aufgrund von Vertragsverletzungen abgelehnt wurden. Dieses Protokoll erfasst nicht alle Pakete, um CPU-Ressourcen zu schützen, bietet Ihnen jedoch weiterhin eine große Anzahl von Protokollen.

Wenn die Schnittstelle, an der der Fehler ausgelöst wird, Teil eines Port-Channels ist, müssen Sie diesen Befehl und grep für den Port-Channel verwenden, um die erforderlichen Protokolle abzurufen. Andernfalls kann die physische Schnittstelle übersichtlich dargestellt werden.

Dieses Protokoll kann je nach Anzahl der verworfenen Verträge schnell übernommen werden.

```
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
```

In diesem Fall versucht 192.168.21.150, ICMP-Meldungen (IP Protocol Number 1) an 192.168.20.3 zu senden. Es gibt jedoch keinen Vertrag zwischen den beiden EPGs, der ICMP zulässt, sodass das Paket verworfen wird. Wenn ICMP zugelassen werden soll, kann zwischen den beiden EPGs ein Vertrag hinzugefügt werden.

Statistikgrenzwert

In diesem Abschnitt wird beschrieben, wie Sie einen Schwellenwert für Statistikobjekte ändern, die möglicherweise einen Fehler beim Drop-Zähler auslösen können.

Ein Grenzwert für die Statistiken der einzelnen Objekte (z. B. l2IngrPkts, eqptIngrDropPkts) wird durch Überwachungsrichtlinie für verschiedene Objekte konfiguriert.

Wie in der Tabelle am Anfang erwähnt, wird eqptIngrDropPkts unter z. B. l1PhysIf-Objekten mithilfe von Überwachungsrichtlinie überwacht.

Weiterleitungs-Drop-Paketrate in eqptIngrDropPkts

Dafür gibt es zwei Teile.

+ Zugriffsrichtlinien (Ports für externe Geräte). auch als Frontblendenkabel bezeichnet)

+ Fabric-Richtlinien (Ports zwischen LEAF und SPINE). auch Fabric-Ports genannt)

Front Panel Ports (ports towards external devices)

Fabric Ports (ports between LEAF and SPINE)

Jedem Port-Objekt (l1PhysIf, pcAggrIf) kann wie im obigen Bild gezeigt eine eigene **Überwachungsrichtlinie** über die **Schnittstellenrichtliniengruppe** zugewiesen werden.

Standardmäßig gibt es in der APIC-GUI unter **Fabric > Access Policies** und **Fabric > Fabric Policies** eine **Standard-Überwachungsrichtlinie**. Diese Standard-Überwachungsrichtlinien werden jeweils allen Ports zugewiesen. Die Standard-Überwachungsrichtlinie unter "Access Policies" (Zugriffsrichtlinien) ist für Front-Panel-Ports und die Standard-Überwachungsrichtlinie unter Fabric-Richtlinien für Fabric-Ports.

Sofern keine Änderung der Schwellenwerte pro Port erforderlich ist, kann die Standard-Überwachungsrichtlinie in jedem Abschnitt direkt geändert werden, um die Änderung für alle Ports an der Vorderseite und/oder Fabric-Ports anzuwenden.

Im folgenden Beispiel werden die Schwellenwerte für Forward Drop in eqptIngrDropPkts an Fabric-Ports (**Fabric-Richtlinien**) geändert. Führen Sie das Gleiche unter **Fabric > Zugriffsrichtlinien** für die Ports an der Vorderseite durch.

1. Navigieren Sie zu **Fabric > Fabric Policies>Monitoring Policies.**

2. Klicken Sie mit der rechten Maustaste, und wählen Sie "Überwachungsrichtlinie erstellen" aus.

(Wenn die Schwellenwertänderung auf alle Fabric-Ports angewendet werden kann, navigieren Sie zur **Standardeinstellung,** anstatt eine neue zu erstellen.)

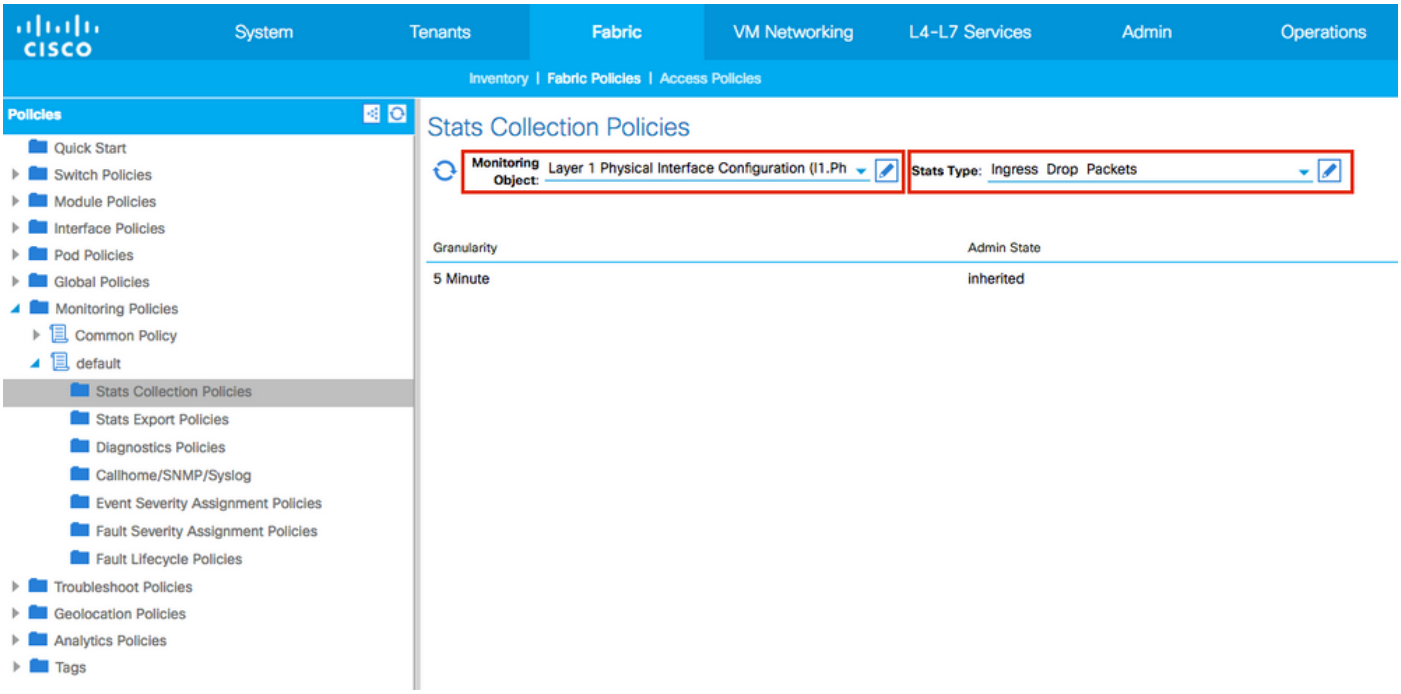
3. Erweitern Sie die neue Überwachungsrichtlinie oder den neuen Standardwert, und navigieren Sie zu **Statistikauflistungsrichtlinien..**

4. Klicken Sie auf das Bleistiftsymbol für das **Überwachungsobjekt** im rechten Bereich, und wählen Sie **Physical Interface Configuration (L1.PhysIf)** für **Layer 1 aus**.

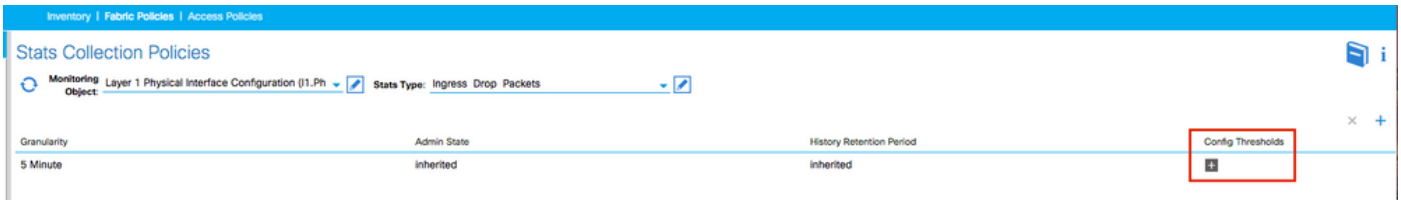
(Dieser Schritt 4 kann übersprungen werden, wenn die Standardrichtlinie verwendet wird.)

5. Wählen Sie im rechten Bereich des Dropdown-Menüs **Monitoring Object**

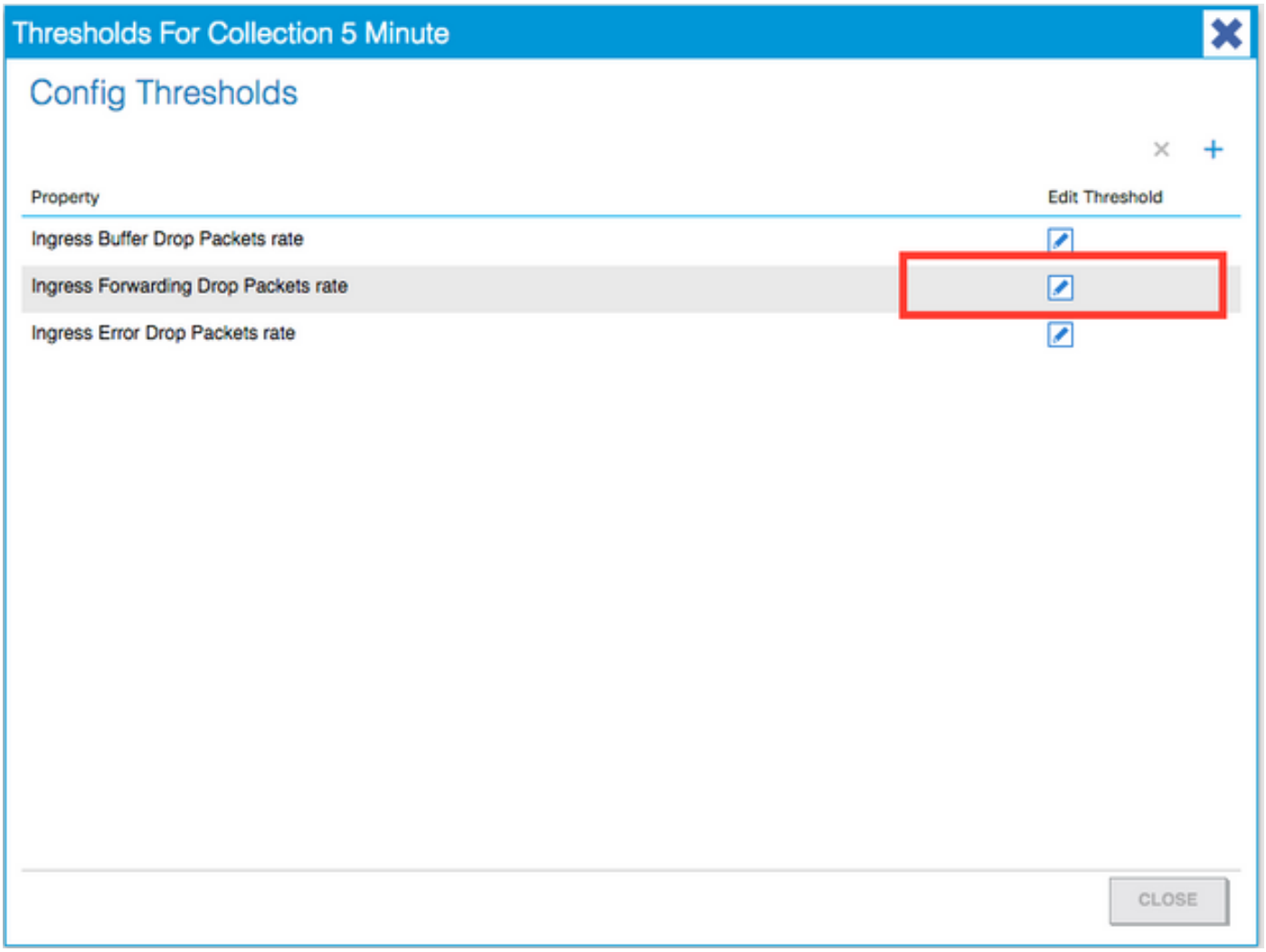
(Überwachungsobjekt) die Option **Layer 1 Physical Interface Configuration (l1.PhysIf)** und **Stats Type (Statustyp) aus**, und wählen Sie **Ingress Drop Packets (Eingangs-Drop-Pakete) aus.**



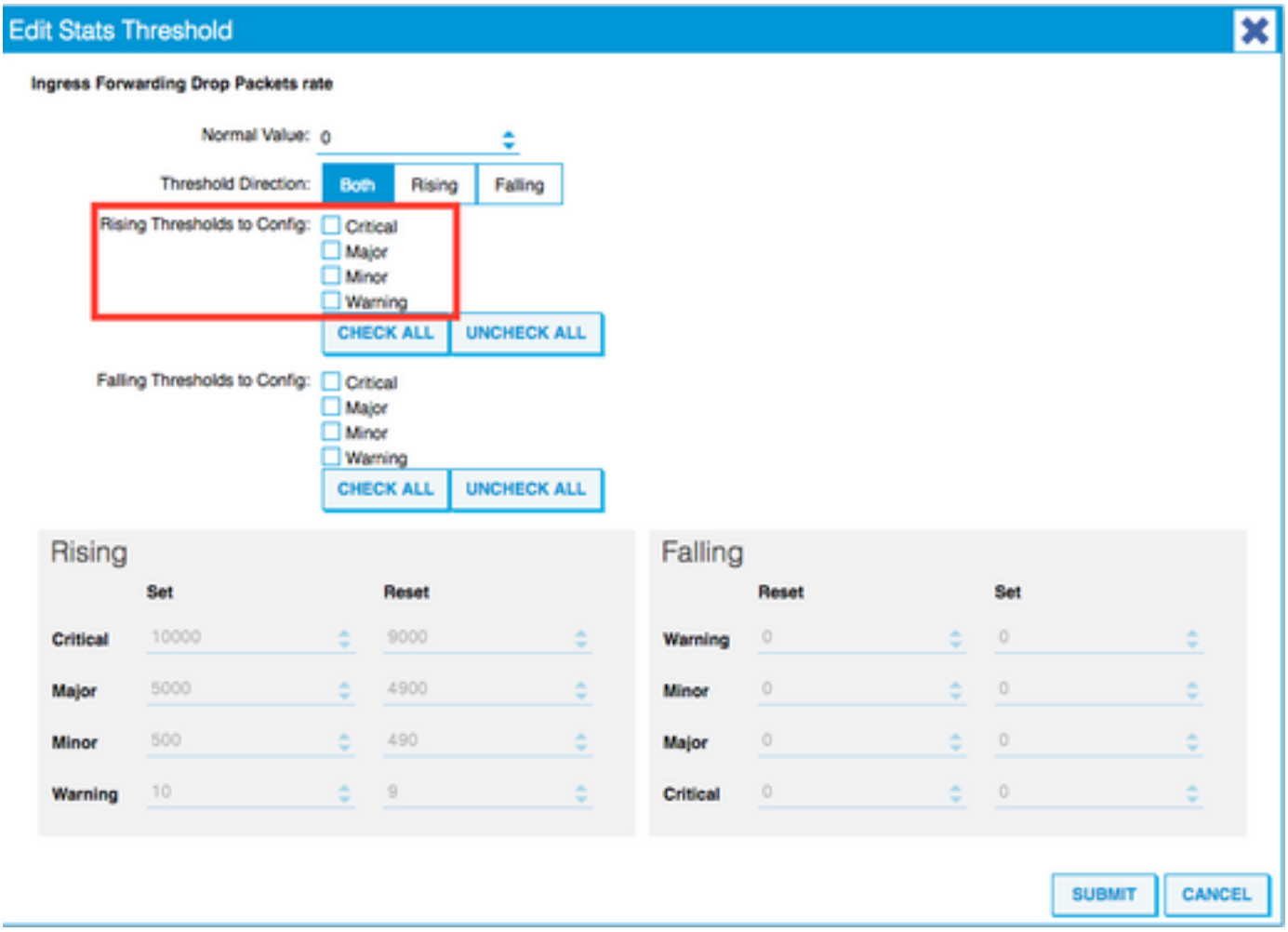
6. Klicken Sie auf das **+** neben Config Thresholds (Konfigurationsschwellenwerte).



7. Schwellenwert für Weiterleitungsverlust bearbeiten

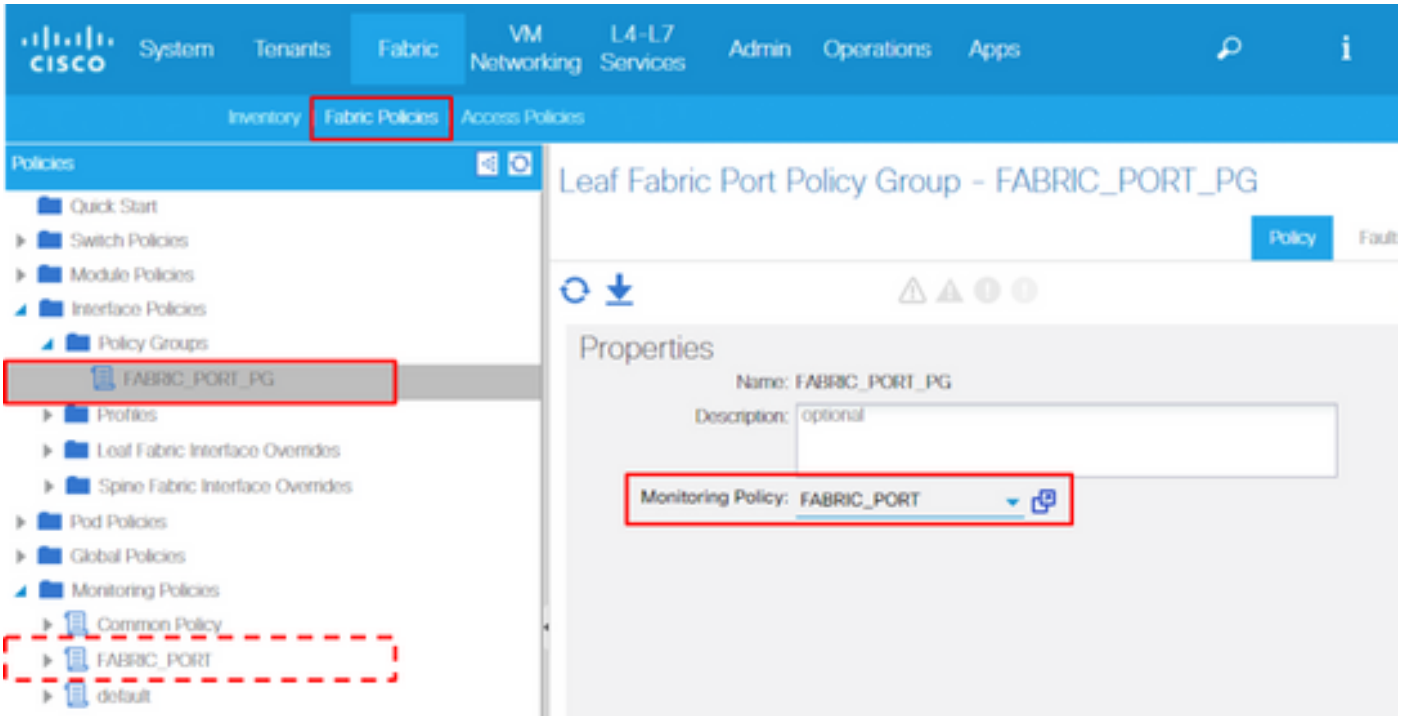


8. Es wird empfohlen, die steigenden Schwellenwerte für die Konfiguration für kritische, Haupt-, Nebenfach- und Warnungen bei der Weiterleitungsabbrecherquote zu deaktivieren.



9. Wenden Sie diese neue Überwachungsrichtlinie auf die Schnittstellenrichtliniengruppe für die erforderlichen Ports an. Bitte vergessen Sie nicht, das Schnittstellenprofil, das Switch-Profil usw. zu konfigurieren.. in Fabric-Richtlinien entsprechend.

(Dieser Schritt 9 kann übersprungen werden, wenn die Standardrichtlinie verwendet wird.)

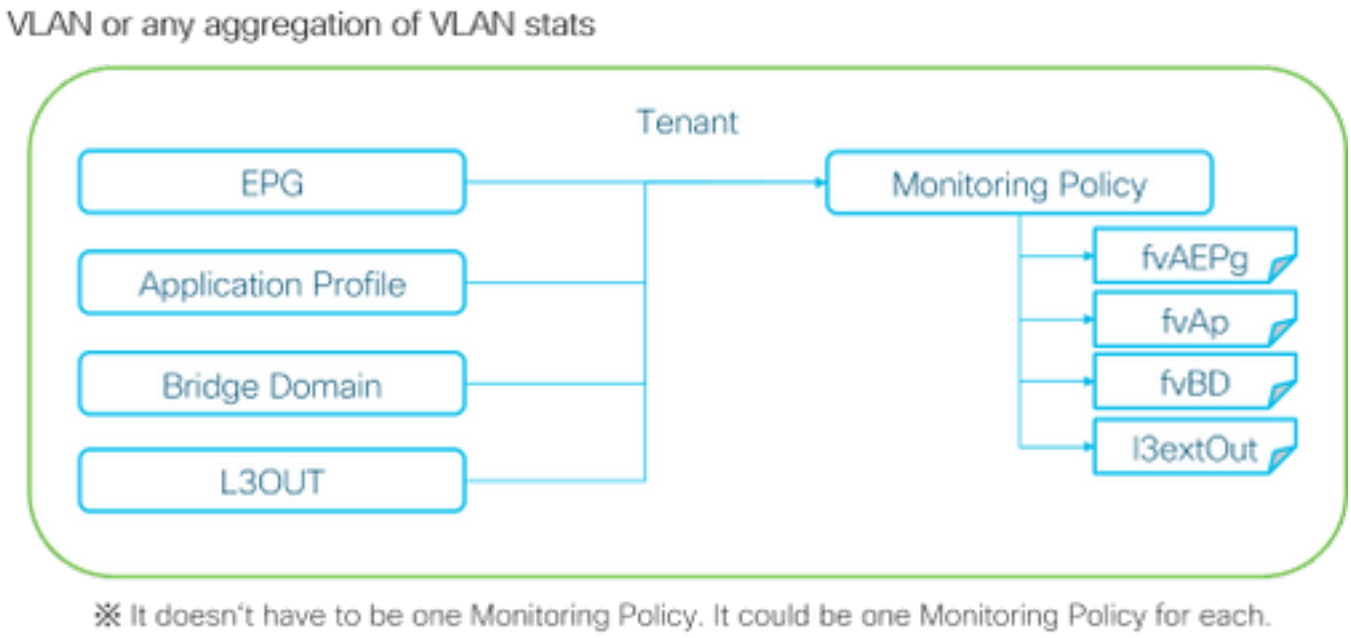


10. Wenn es sich um Front-Panel-Ports (Zugriffsrichtlinien) handelt, sollten Sie für **aggregierte Schnittstellen (pc.AggrIf)** dasselbe tun wie für die **physische Layer-1-Schnittstellenkonfiguration (l1.PhysIf)**, damit diese neue Überwachungsrichtlinie sowohl auf Port-Channel als auch auf physischen Port angewendet werden kann.

(Dieser Schritt 10 kann übersprungen werden, wenn die Standardrichtlinie verwendet wird.)

Paketrate bei eingehenden Datenverlusten in l2IngrPktsAG

Dafür gibt es mehrere Teile.



Wie das obige Bild zeigt, wird l2IngrPktsAg unter vielen Objekten überwacht. Im obigen Bild werden nur einige Beispiele, aber nicht alle Objekte für l2IngrPktsAg angezeigt. Der Schwellenwert für Statistiken wird jedoch durch Überwachungsrichtlinie sowie eqptIngrDropPkts unter l1PhysIf oder pcAggrIf konfiguriert.

Jedes Objekt (EPG(fvAEPg), Bridge Domain(fvBD), etc..) kann eine eigene **Überwachungsrichtlinie** zugewiesen werden, wie in der Abbildung oben gezeigt.

Standardmäßig verwenden alle Objekte unter Tenant die **Standardüberwachungsrichtlinie** unter **Tenant > common > Monitoring Polices > default**, sofern nichts anderes konfiguriert wurde.

Sofern nicht für jede Komponente eine Änderung der Schwellenwerte erforderlich ist, kann die Standard-Überwachungsrichtlinie unter Tenant common direkt geändert werden, um die Änderung für alle zugehörigen Komponenten anzuwenden.

Im folgenden Beispiel werden die Schwellenwerte für die Durchsatzrate von Ingress Drop Packets in l2IngrPktsAg15min in der Bridge-Domäne geändert.

1. Navigieren Sie zu **Tenant > (Tenant-Name) > Monitoring Policies (Überwachungsrichtlinien).**

(Tenant muss gleich sein, wenn die Standard-Überwachungsrichtlinie verwendet wird oder die neue Überwachungsrichtlinie auf Tenants angewendet werden muss.)

2. Klicken Sie mit der rechten Maustaste, und wählen Sie "Überwachungsrichtlinie erstellen" aus.

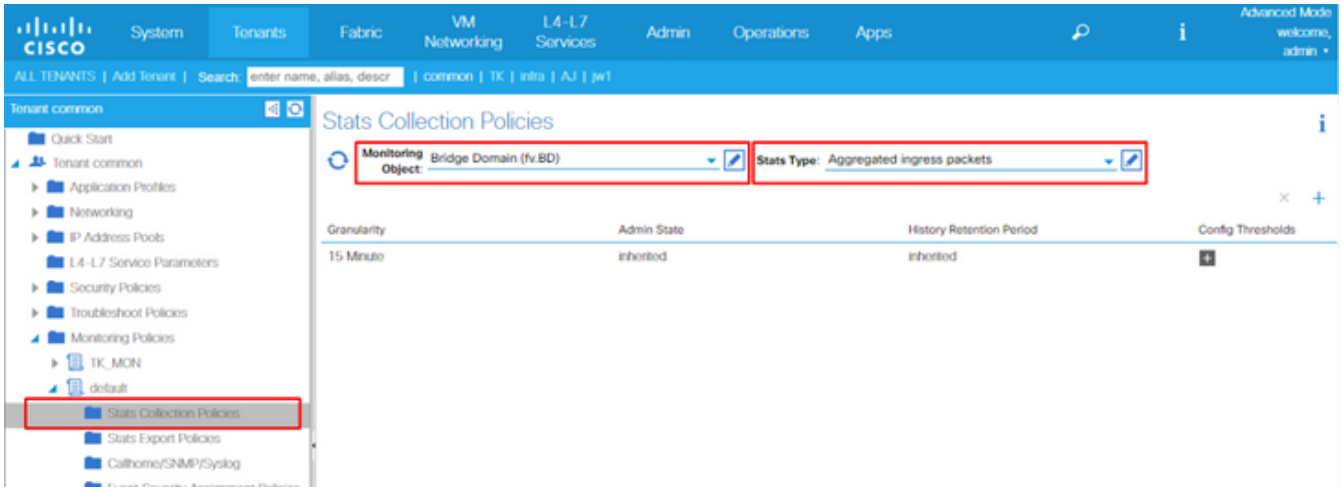
(Wenn die Schwellenwertänderung auf alle Komponenten angewendet werden kann, navigieren Sie zur **Standardeinstellung,** anstatt eine neue zu erstellen.)

3. Erweitern Sie die neue Überwachungsrichtlinie oder den neuen Standardwert, und navigieren Sie zu **Statistikauflistungsrichtlinien..**

4. Klicken Sie im rechten Bereich auf das Bleistiftsymbol für das **Überwachungsobjekt**, und wählen Sie **Bridge-Domäne (fv.BD).**

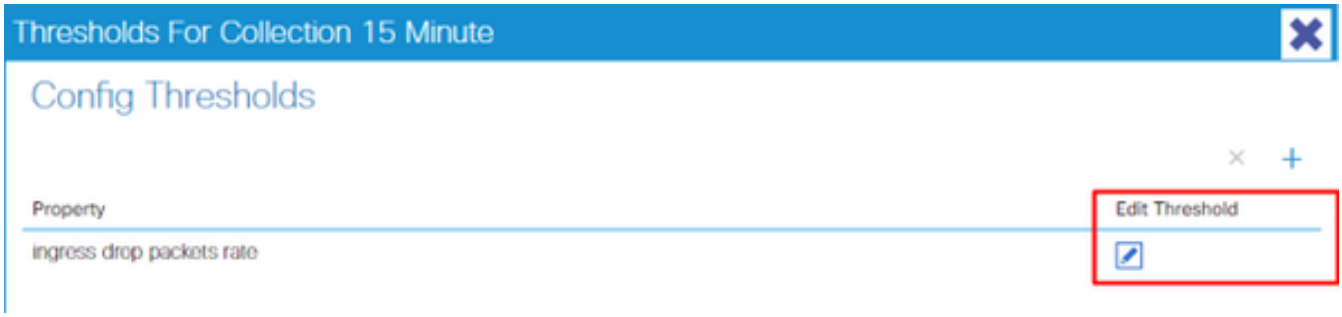
(Dieser Schritt 4 kann übersprungen werden, wenn die Standardrichtlinie verwendet wird.)

5. Wählen Sie im rechten Bereich des Dropdown-Menüs **Überwachungsobjekt** die Option **Bridge Domain (fv.BD)** und **Stats Type (Statustyp) aus**, und wählen Sie **Aggregated Ingress Packets (Aggregierte Eingangspakete) aus.**

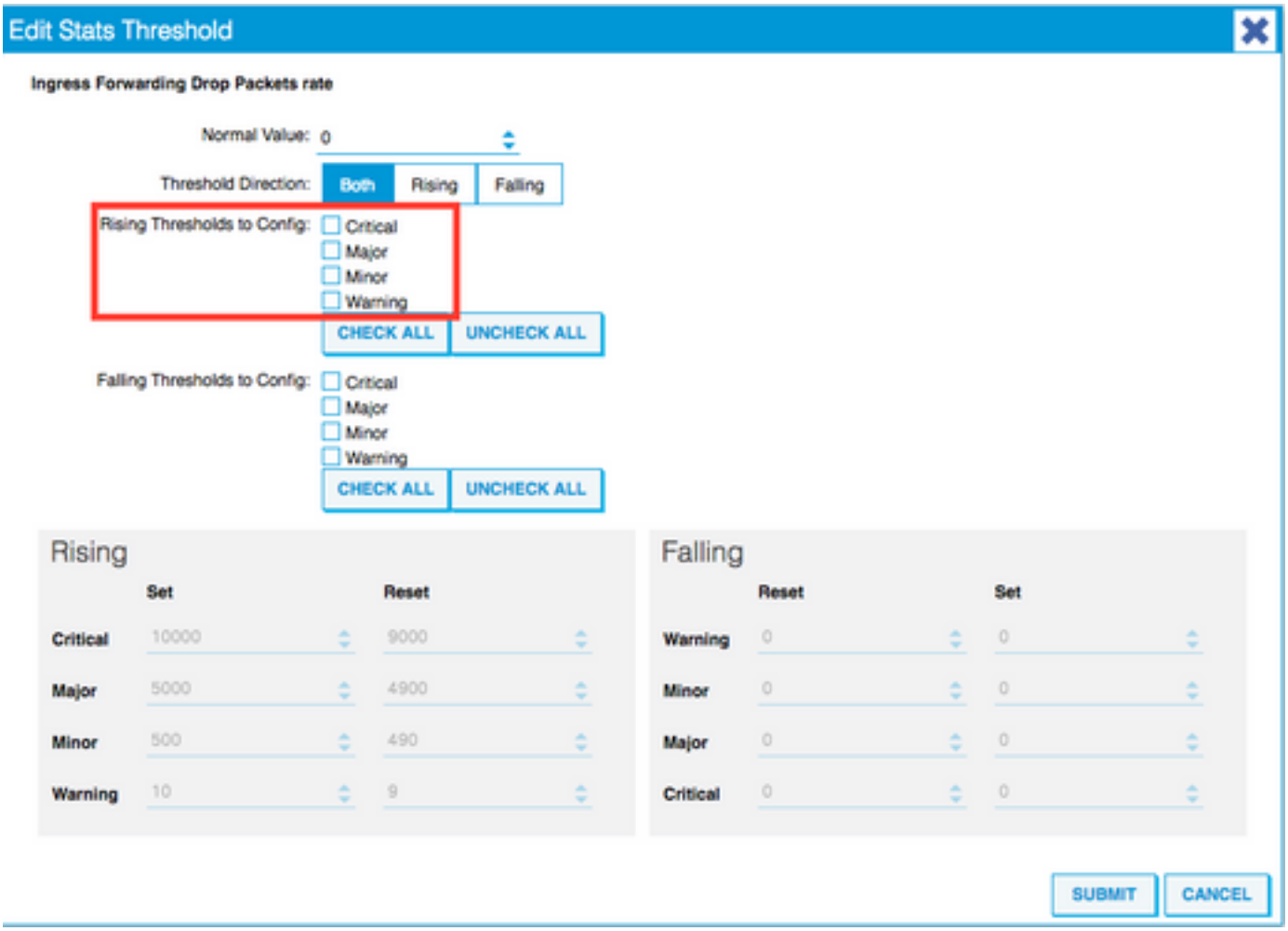


6. Klicken Sie auf das **+** neben Config Thresholds (Konfigurationsschwellenwerte).

7. Schwellenwert für Weiterleitungsverlust bearbeiten

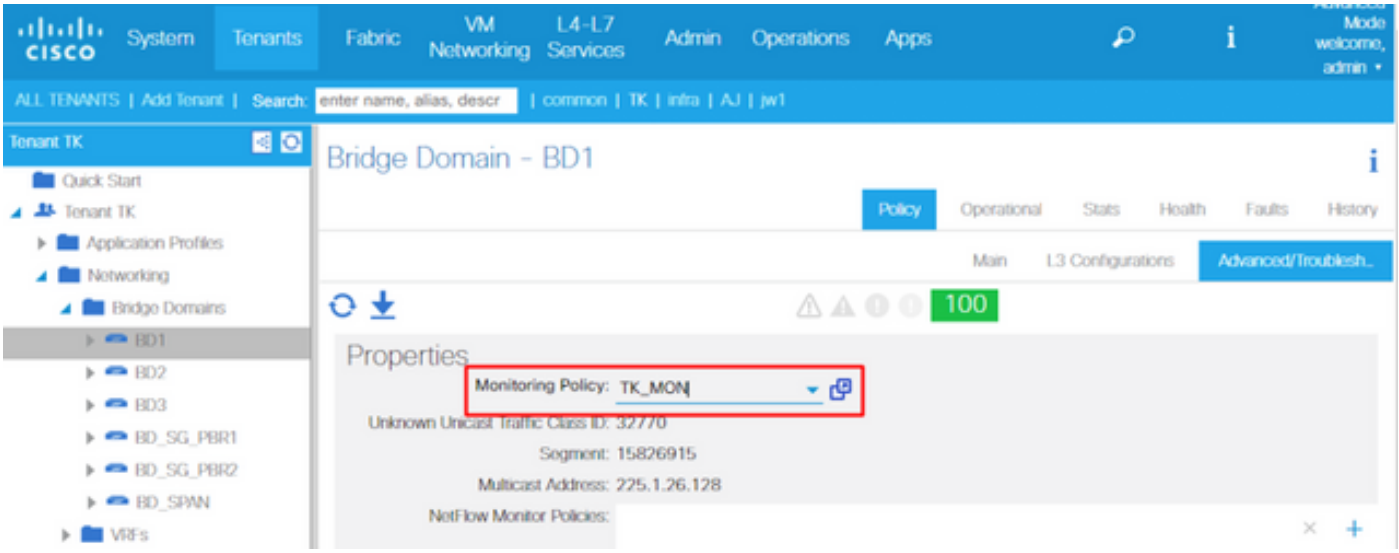


8. Es wird empfohlen, die steigenden Schwellenwerte für die Konfiguration für kritische, Haupt-, Nebenfach- und Warnungen bei der Weiterleitungsabbrecherquote zu deaktivieren.



9. Wenden Sie diese neue Überwachungsrichtlinie auf die Bridge-Domäne an, die eine Änderung des Schwellenwerts erfordert.

(Dieser Schritt 9 kann übersprungen werden, wenn die Standardrichtlinie verwendet wird.)



HINWEIS

Nicht standardmäßige Überwachungsrichtlinie kann keine Konfigurationen enthalten, die in der Standard-Überwachungsrichtlinie enthalten sind. Wenn diese Konfiguration mit der Standardüberwachungsrichtlinie übereinstimmen muss, müssen die Benutzer die Standardkonfiguration der Überwachungsrichtlinie überprüfen und die gleichen Richtlinien manuell für eine Überwachungsrichtlinie konfigurieren, die nicht der Standardrichtlinie entspricht.