ACIでのパケットドロップ障害の説明

内容

はじめに

本書では、各障害タイプと、その障害が発生したときの手順について説明します。シスコアプリケーションセントリックインフラストラクチャ(ACI)ファブリックの通常の動作中に、管理者は特定のタイプのパケットドロップの障害を確認できます。

管理対象オブジェクト

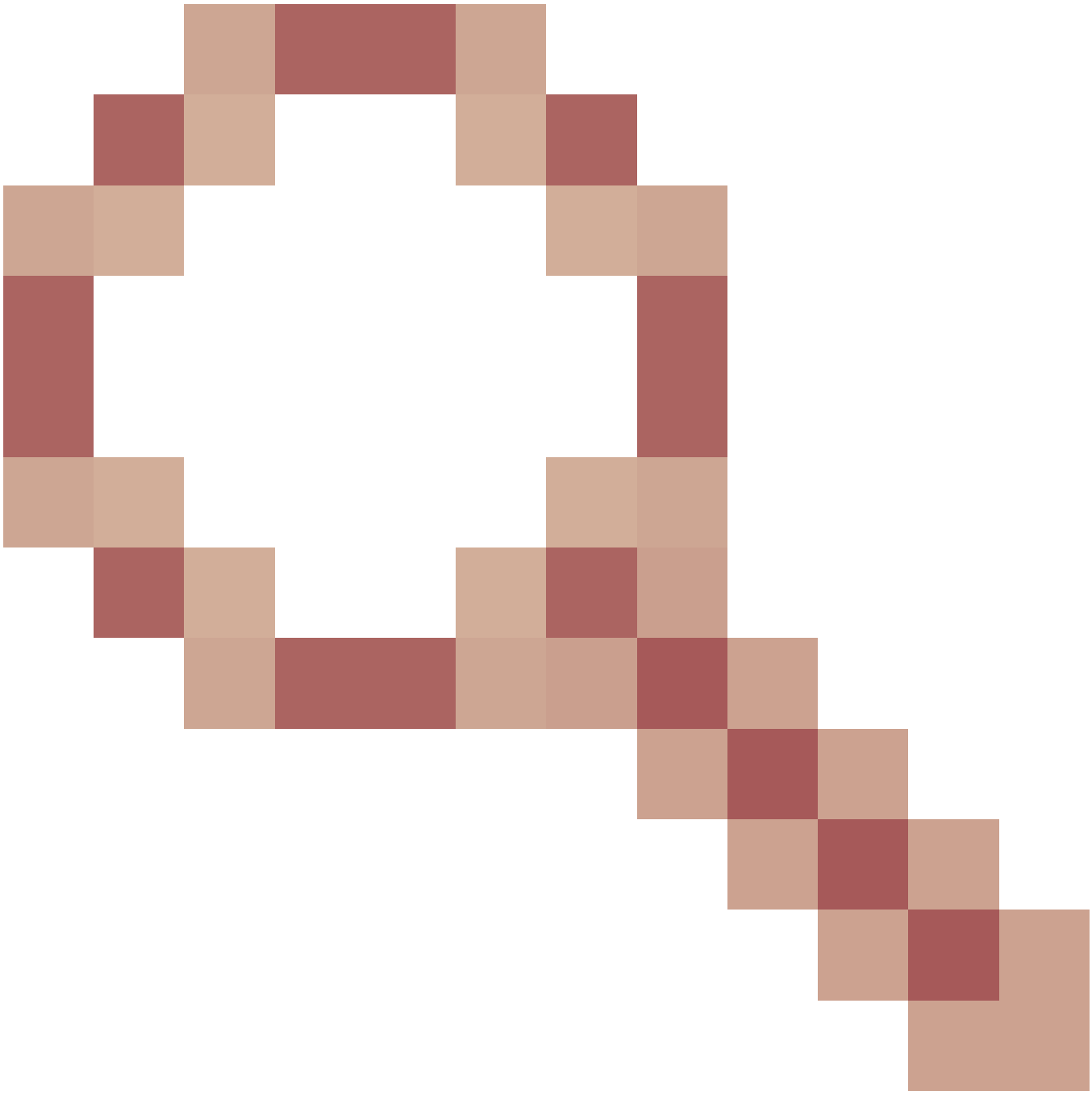
Cisco ACI では、すべてのエラーは管理対象オブジェクト（MO）で挙げられます。たとえば、障害「F11245 - ingress drop packets rate(l2IngrPktsAg15min:dropRate)」は、MO l2IngrPktsAg15minのパラメータ「dropRate」に関係しています。

このセクションでは、ドロップパケットの障害に関連する管理対象オブジェクト(MO)の例をいくつか紹介します。

	例	説明	サンプルパラメータ	サンプルMO対象 発生する障害

l2IngrPkts	l2IngrPkts5min l2IngrPkts15min l2IngrPkts1h 等。	これは VLAN ごとの各時間内の入力パケットの統計を表します.	dropRate floodRate multicastRate unicastRate	vlanCktEp(VLAN)
l2IngrPktsAg	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d 等。	これは、EPG、BD、VRFなどの入力パケットの統計情報を表します。たとえば、EPG統計は、EPGに属するVLAN統計の集約を表します。	dropRate floodRate multicastRate unicastRate	fvaepg(EPG) fvAp（アプリケーションプロファイル） fvBD(BD) l3extOut(L3OUT)
eqptIngrDropPkts	eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d 等。	これはインターフェイスごとの各時間内の入力ドロップ パケット統計を表します.	*1 forwardingRate *1 errorRate *1 bufferRate	l1PhysIf（物理ポート） pcAggrIf（ポートチャネル）

*1:SUP_REDIRECTパケットが転送ドロップとして記録されるため、複数のNexus 9000プラットフォームでのASICの制限により、eqptIngrDropPkts内のこれらのカウンタが誤って増加する可能性があります。詳細と修正済みバージョンについては、Cisco Bug ID CSCvo68407、およびCisco Bug ID CSCvn72699



も参照してください。

ハードウェア ドロップ カウンタのタイプ

ACI モードで動作する Nexus 9000 スイッチには、ASIC での入力インターフェイスのドロップの原因に関する主要なハードウェア カウンタが 3 つあります。

l2IngrPkts、l2IngrPktsAg の dropRate には、これらのカウンタが含まれます。eqptIngrDropPktsテーブルの3つのパラメータ(forwardingRate、errorRate、bufferRate)は、3つのインターフェイスカウンタを表します。

[転送（Forward）]

転送ドロップは、ASICのLookUp(LU)ブロックでドロップされるパケットです。LU ブロックでは、パケット転送の判断は、パケット ヘッダー情報に基づいて行われます。パケットをド

ロップする判断の場合、転送ドロップがカウントされます。この問題が発生する原因はさまざまですが、主な原因について説明します。

SECURITY_GROUP_DENY

通信を許可す契約の欠如が原因のドロップ。

パケットがファブリックに入ると、スイッチは送信元と宛先 EPG を参照してこの通信を可能にする契約があるかどうかを確認します。送信元と宛先が異なるEPGにあり、その間でこのパケットタイプを許可する契約がない場合、スイッチはパケットをドロップし、SECURITY_GROUP_DENYのラベルを付けます。この場合転送ドロップ カウンタが増えます。

VLAN_XLATE_MISS

不適切な VLAN によるドロップ。

パケットがファブリックに入ると、スイッチはパケットを参照して、このポートの設定でこのパケットの受け入れが可能か判断します。 たとえば、10 の 802.1Q タグ付きファブリックにフレームが入るとします。スイッチのポートにVLAN 10が設定されている場合、スイッチは内容を検査し、宛先MACに基づいて転送の決定を行います。ただし、VLAN 10がポートにない場合は、ドロップされ、VLAN_XLATE_MISSとしてラベル付けされます。この場合転送ドロップ カウンタが増えます。

XLATEまたは「変換」となる理由は、ACIではリーフスイッチがカプセル化された802.1Qのフレームを受け入れ、VXLANおよびファブリック内でその他の正規化に使用する新しいVLANに変換するためです。導入されていないVLANを含むフレームが着信すると、変換は失敗します。

ACL_DROP

sup-tcam によるドロップ。

ACI のスイッチの sup-tcam には、通常の L2/L3 転送の判断に加えて適用する特殊なルールが含まれます。sup-tcam ルールは組み込み型でユーザ設定はできません。sup-tcam ルールの目的は主に一部の例外やコントロール プレーン トラフィックを処理することにあり、ユーザがチェックしたりモニタしたりするようには意図されていません。パケットがsup-tcamルールに抵触していて、パケットをドロップするルールである場合、ドロップされたパケットはACL_DROPとしてカウントされ、転送ドロップカウンタが増加します。これが発生する場合、通常はパケットが基本的なACI転送の原則に反する転送をされようとしていることを意味します。

ドロップの名前がACL_DROPであっても、このACLは、スタンドアロンNX-OSデバイスや他のルーティング/スイッチングデバイスで設定できる通常のアクセスコントロールリストとは異なります。

SUP_REDIRECT

これはドロップではありません。

リダイレクトされたsupパケット（CDP/LLDP/UDLD/BFDなど）は、パケットが正しく処理されてCPUに転送されていたとしても、転送ドロップとしてカウントできます。

これは、-EX、-FX、および – FX2プラットフォーム(N9K-C-YC93180EXやN9K-C93180YC-FXなど)で発生します。これらはドロップとしてカウントされませんが、-EX/-FX/-FX2プラットフォームのASICの制限によるものです。

エラー

スイッチが前面パネルインターフェイスの1つで無効なフレームを受信すると、エラーとしてドロップされます。 この例として、FCS や CRC エラーのフレームなどがあります。アップリンク/ダウンリンクのリーフポート、またはスパインポートを表示する場合は、show interfaceを使用してFCS/CRCエラーをチェックすることをお勧めします。 ただし、通常の動作時には、このカウンタにはシステムによってプルーニングされ、インターフェイスから送信される予定のないフレームも含まれるため、リーフまたはスパインポートのアップリンク/ダウンリンクポートでエラーパケットの増加が見られることが予想されます。

例：ルーティングされたパケットのTTL障害、同じインターフェイスでのブロードキャスト/フラッディングされたフレーム。

バッファ

スイッチがフレームを受信し、入出力のいずれかで使用できるバッファクレジットがない場合、フレームはバッファとともにドロップされます。 これは、ネットワークのどこかで輻輳が発生していることを示唆しています。障害を示すリンクがいっぱいであるか、宛先を含むリンクが輻輳している可能性があります。

CLI でのドロップ状態表示

管理対象オブジェクト

いずれかのAPICにセキュアシェル(SSH)で接続し、次のコマンドを実行します。

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

これにより、このクラスl2IngrPktsAg15minのすべてのオブジェクトインスタンスが提供されます。

特定のオブジェクトを照会するフィルタの例を示します。この例では、フィルタはtn-TENANT1/ap-APP1/epg-EPG1を含むdn属性のオブジェクトのみを表示します。

また、この例ではegrepを使用して、必要な属性だけを表示しています。

出力例1：テナントTENANT1、アプリケーションプロファイルAPP1、epg EPG1のEPGカウンタオブジェクト(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
```

または、オブジェクト dn がわかっている場合、-c の代わりにオプション -d を使用して特定のオブジェクトを取得することができます。

出力例2：テナントTENANT1、アプリケーションプロファイルAPP1、epg EPG2のEPGカウンタオブジェクト(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
```

ハードウェアカウンタ

エラーが表示される場合や、CLI を使用してスイッチポートのパケット ドロップを確認する場合は、一番の方法はハードウェアのプラットフォーム カウンタを表示することです。一部の例外を除き、ほとんどすべてのカウンタは show interface を使用して表示できます。 3 つの主要なドロップの原因はプラットフォーム カウンタを使用してのみ表示できます。 これらを表示するには、次の手順を実行します。

リーフ

リーフに SSH 接続し、次のコマンドを実行します。

```
ACI-LEAF#vsh_lc
module-1# show platform internal counters port <X>
                                        * X はポート番号を表します
```

イーサネット 1/31 の出力例：

```
<#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 -----
```

スパイン

ボックス型スパイン(N9K-C9336PQ)の場合は、リーフとまったく同じです。

モジュラスパイン（N9K-C9504など）の場合、プラットフォームカウンタを表示するには、最初に特定のラインカードを接続する必要があります。 スパインにSSH接続して、次のコマンドを実行します。

ACI-SPINE#vsh

ACI-SPINE# attach module <X>

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

* X は、表示したいラインカードのモジュール番号を表します

Y はポート番号を表します

イーサネット 2/1 の出力例：

```
<#root>

ACI-SPINE#

vsh

Cisco iNX-OS Debug Shell
This shell can only be used for internal commands and exists
for legacy reasons. User can 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 -----
```

障害

F112425：入力ドロップパケットレート(l2IngrPktsAg15min:dropRate)

[Description]：

このエラーの一般的な理由の1つは、転送ドロップの理由でレイヤ2パケットがドロップされることです。さまざまな原因がありますが、最も一般的な原因は次のとおりです。

一部のプラットフォーム(Cisco Bug ID CSCvo68407を参照)では、CPUにリダイレクトする必要があるL2パケット（CDP/LLDP/UDLD/BFDなど）が転送ドロップとしてログされ、CPUにコピーされるという制限があります。これは、これらのモデルで使用される

ASICの制限によるものです。

解決策：

記載されている廃棄は単に表面的なものであるため、ベストプラクティスの推奨は、「統計情報のしきい値」のセクションに示すように障害のしきい値を大きくすることです。方法については「統計情報のしきい値」の手順を参照してください。

F100264：入力バッファ廃棄パケットレート(eqptIngrDropPkts5min:bufferRate)

[Description]：

このエラーは、バッファの理由でパケットがポートでドロップされたときに増加する可能性があります。 前述したように、これは通常、入力方向または出力方向のインターフェイスで輻輳が発生した場合に発生します。

解決策：

このエラーは、輻輳による環境で実際にドロップされたパケットを表します。 ドロップされたパケットは、ACIファブリックで実行されているアプリケーションの問題を引き起こす可能性があります。ネットワーク管理者は、パケットフローを分離し、輻輳が予想外のトラフィックフロー、非効率なロードバランシングなど、またはこれらのポートの予想される使用率によるものかどうかを判断できます。

F100696 – 入力転送ドロップパケット(eqptIngrDropPkts5min:forwardingRate)

注:F11245に関する前述のようなASICの制限により、これらの障害が発生する場合もあります。詳細については、Cisco Bug ID CSCvo68407（登録ユーザ専用）を参照してください。

このエラーの発生シナリオはいくつかあります。最も一般的なものは以下です。

説明 1) スパイン ドロップ

このエラーがスパインインターフェイスで発生する場合、不明なエンドポイントへのトラフィックが原因である可能性があります。 ARPまたはIPパケットがプロキシルックアップのスパインに転送され、エンドポイントがファブリックで不明の場合、特別な収集パケットが生成され、適切なBD（内部）マルチキャストグループアドレスのすべてのリーフに送信されます。これにより、ブリッジドメイン(BD)内の各リーフからARP要求がトリガーされ、エンドポイントが検出されます。 制約があるため、リーフで受信された収集パケットもファブリックに再度反映され、リーフに接続されたスパインリンクでの転送ドロップをトリガーします。このシナリオでの転送ドロップは、Generation 1スパインハードウェアでのみ増加します。

解決策 1）

この問題は、ACIファブリックに不必要な量の未知のユニキャストトラフィックを送信しているデバイスに起因することが判明しているため、どのデバイスがこれを引き起こしているのか調べ、それを防止できるかどうか検討する必要があります。通常はモニタリングの目的でサブネットの IP アドレスをスキャンまたはプローブするデバイスによって引き起こされています。 どの IP がこのトラフィックを送信しているのかを調べるには、エラーを示すスパイン インターフェイスに接続されたリーフに SSH 接続します。

次に、以下のコマンドを実行して収集パケットをトリガーしている送信元 IP アドレス（SIP）を確認します。

<#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.
```

次の出力例では、収集パケットが192.168.21.150によってトリガーされるため、これを軽減できるかどうかを確認することが推奨されています。

説明 2）リーフ ドロップ

このエラーがリーフインターフェイスで発生する場合、最も可能性の高い原因は前述のSECURITY_GROUP_DENYのドロップです。

解決策 2）

ACIリーフは、違反が原因で拒否されたパケットのログを保持します。このログは、

CPUリソースを保護するためにそれらをすべてキャプチャするわけではありませんが、それでも大量のログを提供します。

必要なログを取得するには、エラーが発生したインターフェイスがport-channelの一部である場合、このコマンドを使用してport-channelをgrepする必要があります。そうでない場合は、物理インターフェイスをgreppedにすることができます。

契約のドロップ量に応じてこのログはすぐにロールオーバーできます。

<#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
```

この場合、192.168.21.150はICMPメッセージ（IPプロトコル番号1）を192.168.20.3に送信しようとしています。ただし、ICMPを許可する2つのEPG間に契約がないため、パケットはドロップされます。ICMP が許可されるべきである場合、2 つの EPG 間に契約を追加できます。

統計情報のしきい値

このセクションでは、ドロップカウンタに対する障害を引き起こす可能性のある統計情報オブジェクトのしきい値を変更する方法について説明します。

各オブジェクト（l2IngrPkts、eqptIngrDropPktsなど）の統計情報のしきい値は、さまざまなオブジェクトに対するモニタリングポリシーを通じて設定します。

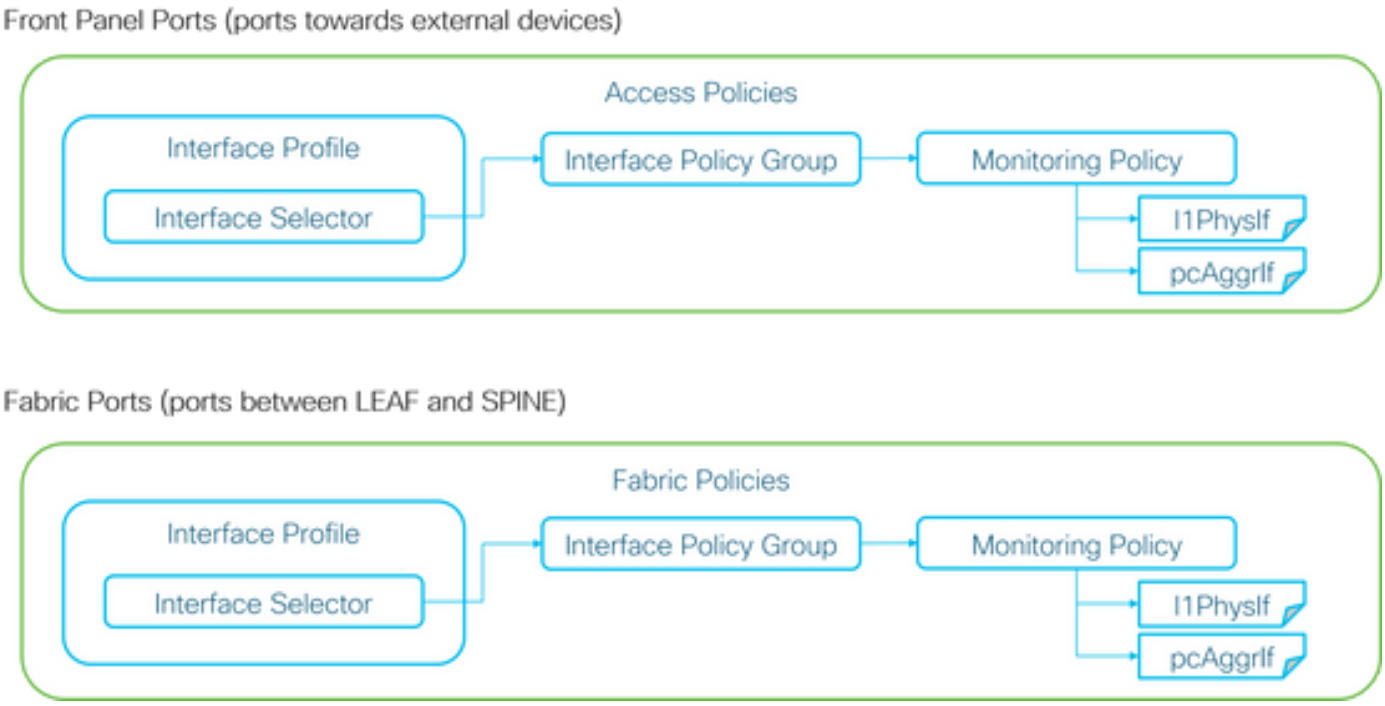
最初の表で説明したように、eqptIngrDropPktsは、たとえばl1PhysIfオブジェクトの下でモニタリングポリシーを使用してモニタされます。

eqptIngrDropPktsでの転送ドロップパケットレート

これには2つの部分があります。

+アクセスポリシー（外部デバイス向けポート、フロントパネルポート）

+ファブリックポリシー（リーフポートとスパインポートの間のポート。ファブリックポートとも呼ばれます）



各ポートオブジェクト(l1PhysIf、pcAggrIf)には、上の図に示すように、インターフェイスポリシーグループを介して独自のモニタリングポリシーを割り当てることができます。

デフォルトでは、APIC GUIのFabric > Access PoliciesとFabric > Fabric Policiesの両方にデフォルトのモニタリングポリシーがあります。これらのデフォルトのモニタリングポリシーは、すべてのポートにそれぞれ割り当てられます。アクセスポリシーのデフォルトのモニタリングポリシーは前面パネルポート用で、ファブリックポリシーのデフォルトのモニタリングポリシーはファブリックポート用です。

ポートごとにしきい値を変更する必要がない限り、各セクションのデフォルトのモニタリングポリシーを直接変更して、すべての前面パネルポートまたはファブリックポート（あるいはその両方）に変更を適用できます。

この例では、ファブリックポート（ファブリックポリシー）上のeqptIngrDropPktsでの転送ドロップのしきい値を変更します。フロントパネルポートのFabric > Access Policiesでも同じ操作を行います。

1. Fabric > Fabric Policies > Monitoring Policiesの順に移動します。

2. 右クリックして、Create Monitoring Policyを選択します。

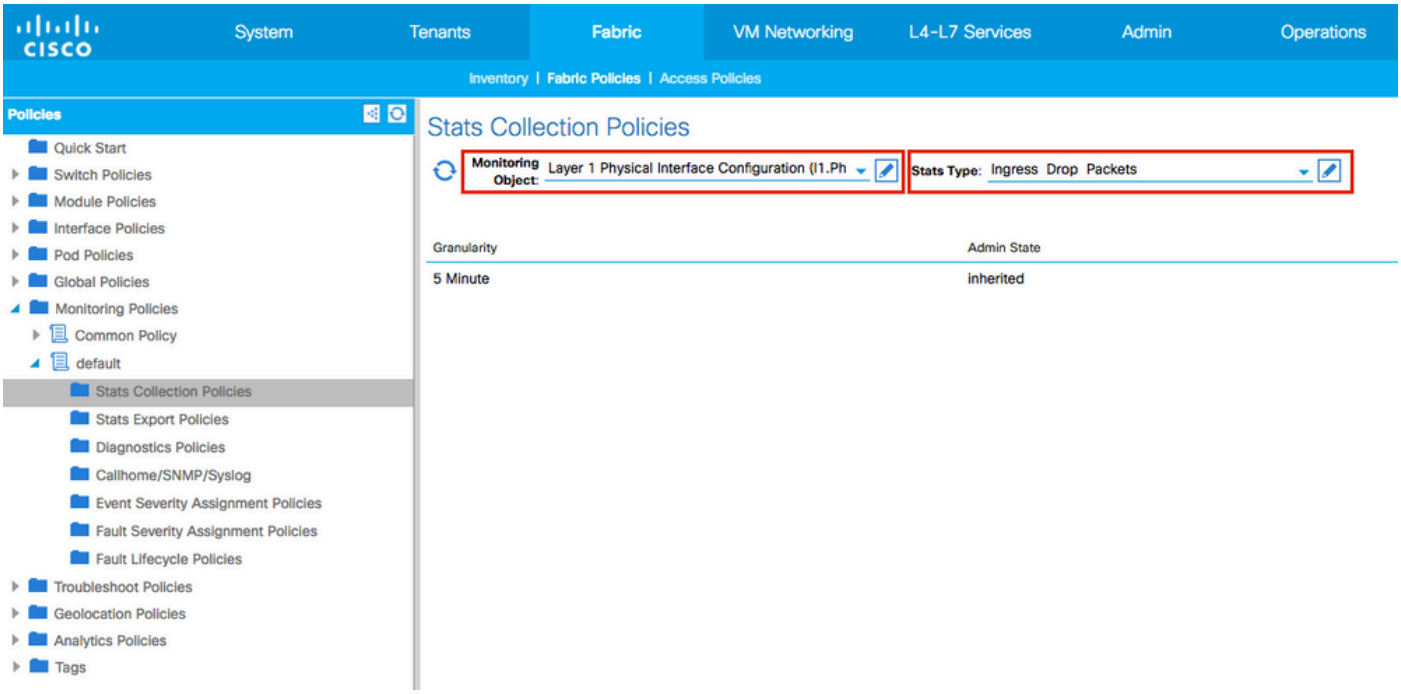
(しきい値の変更をすべてのファブリックポートに適用できる場合は、新しいファブリックポートを作成する代わりに、defaultに移動します)。

3. 新しい監視ポリシーまたはデフォルトを展開し、統計収集ポリシーに移動します。

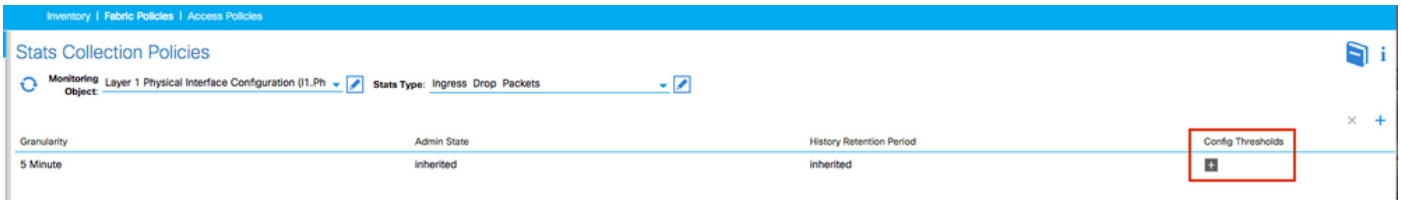
4. 右側のペインでモニタリングオブジェクトの鉛筆アイコンをクリックし、Layer 1 Physical Interface Configuration (l1.PhysIf)を選択します。

（デフォルトのポリシーを使用する場合は、ステップ4をスキップできます）。

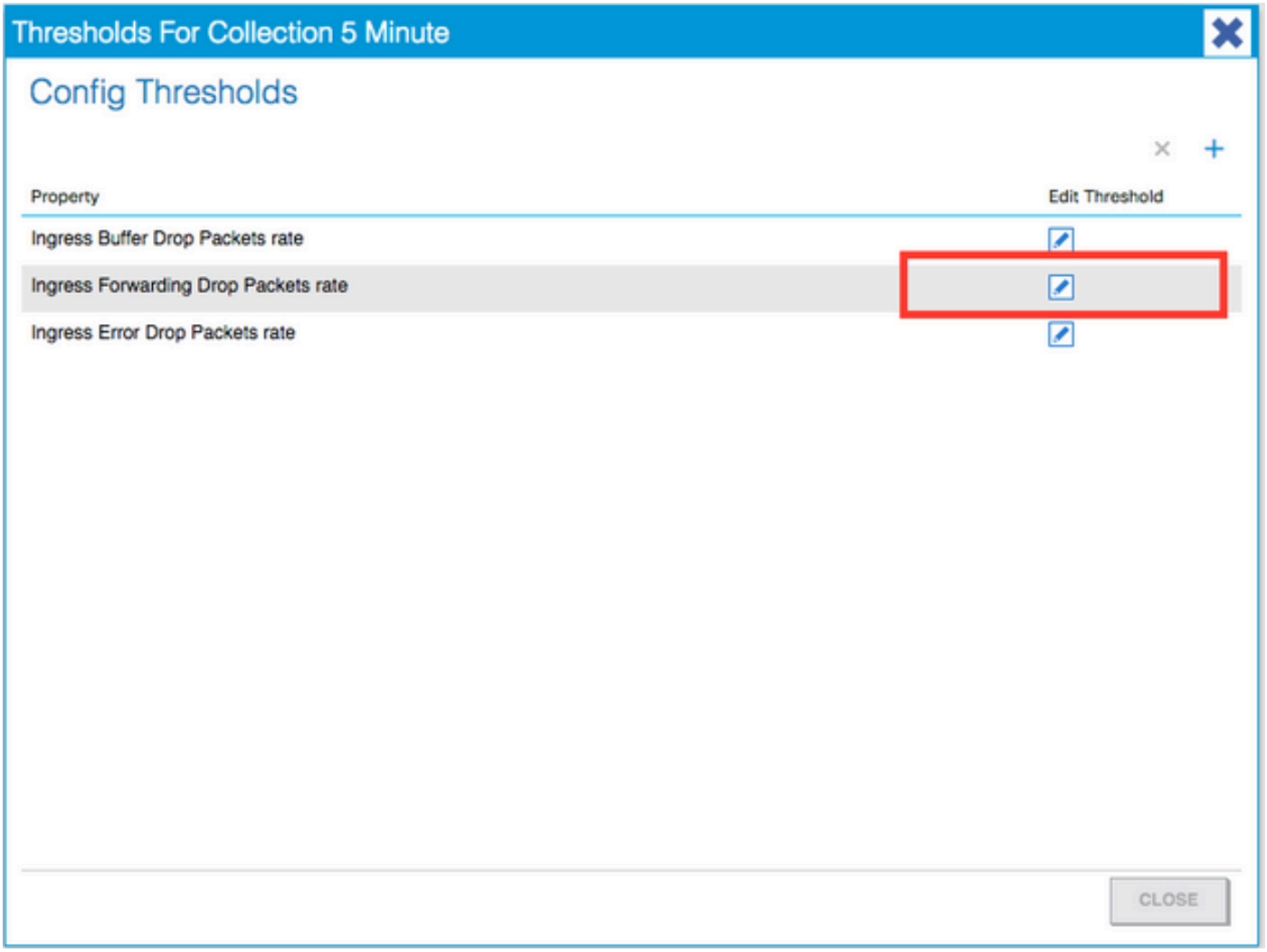
5. 右側のペインのMonitoring Objectドロップダウンから、Layer 1 Physical Interface Configuration (l1.PhysIf)とStats Typeを選択し、Ingress Drop Packetsを選択します



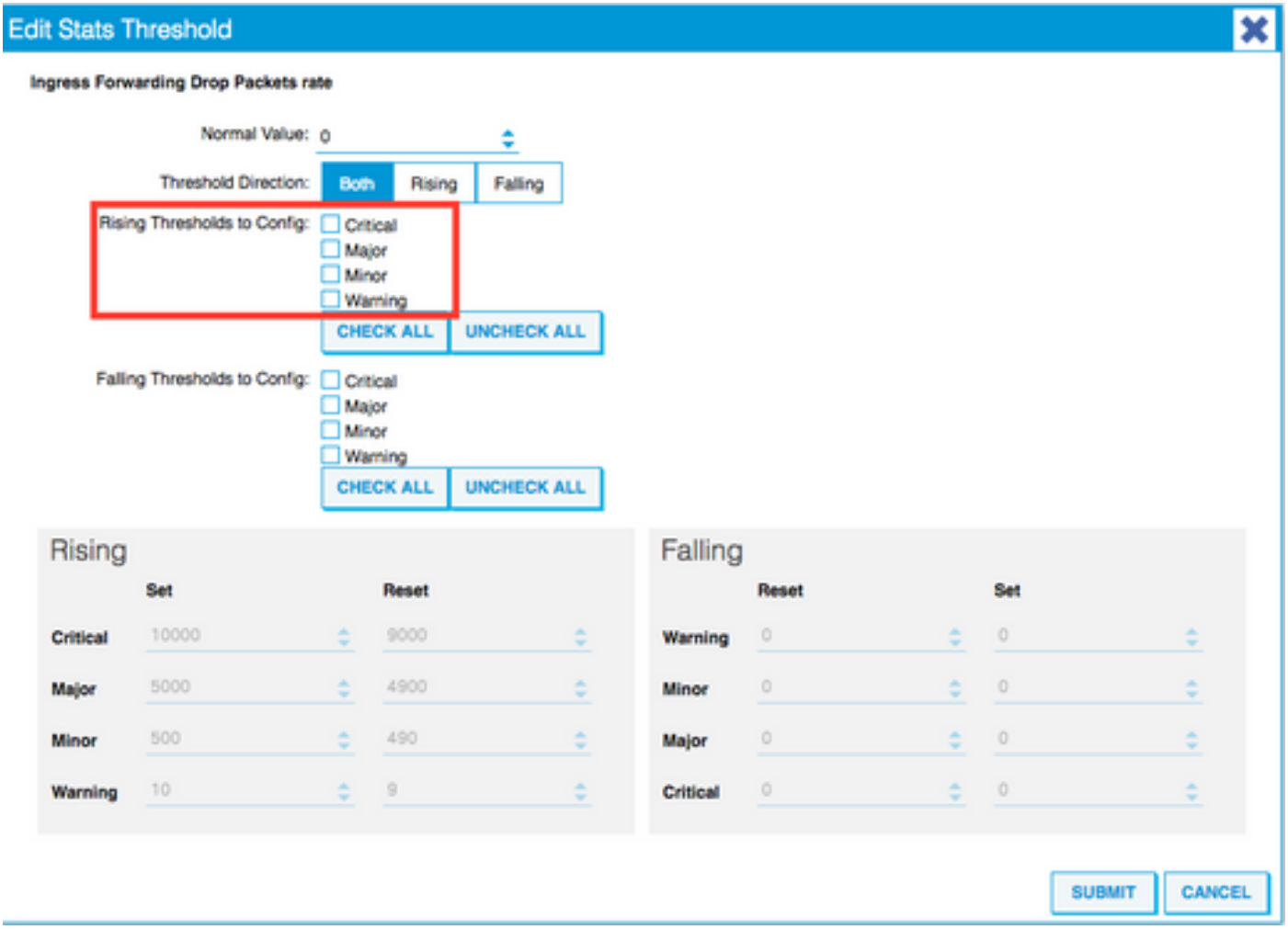
6. Config Thresholdsの横にある+をクリックします。



7. 転送ドロップのしきい値を編集します。

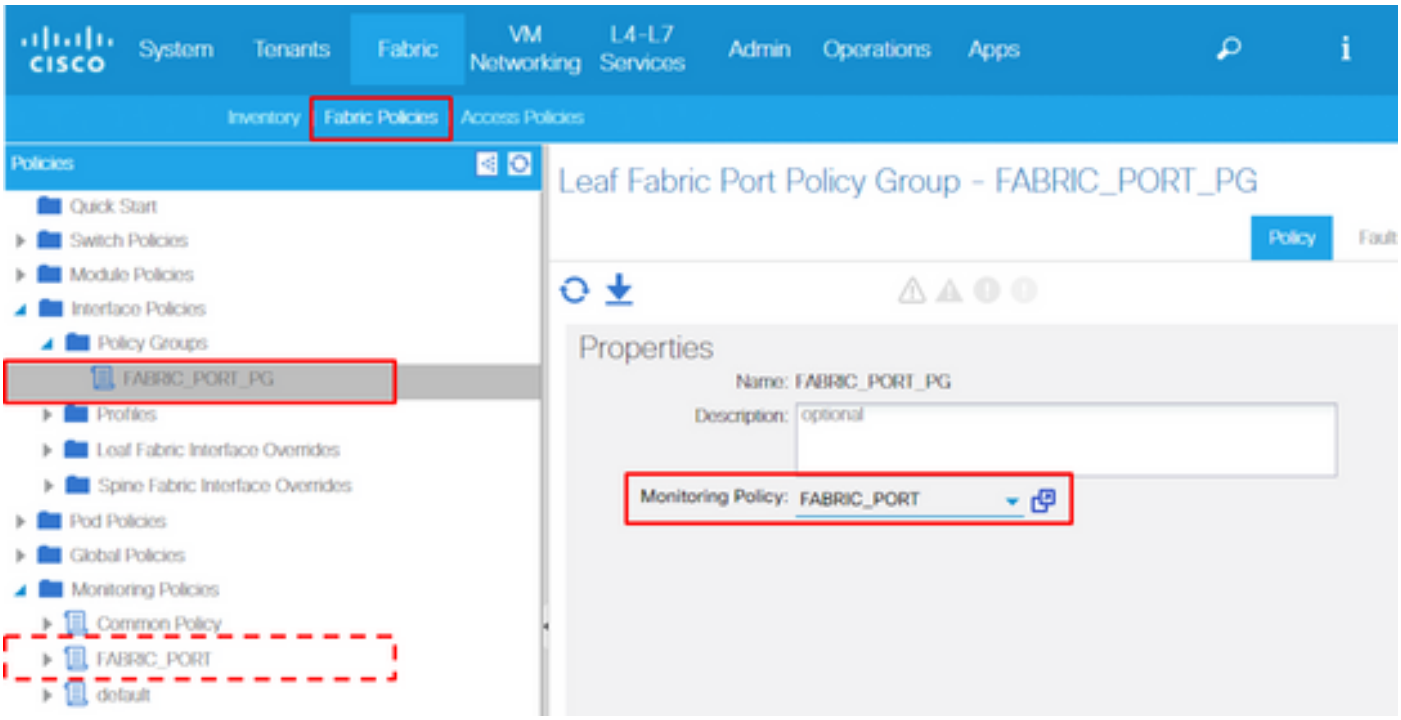


8. 転送ドロップレートのメジャー、マイナー、警告の設定の上昇しきい値を無効にすることが推奨されます。



9. 必要なポートのインターフェイスポリシーグループにこの新しいモニタリングポリシーを適用します。それに応じて、インターフェイスプロファイル、スイッチプロファイルなどをファブリックポリシーに設定することを忘れないでください。

（デフォルトのポリシーを使用する場合は、ステップ9をスキップできます）。

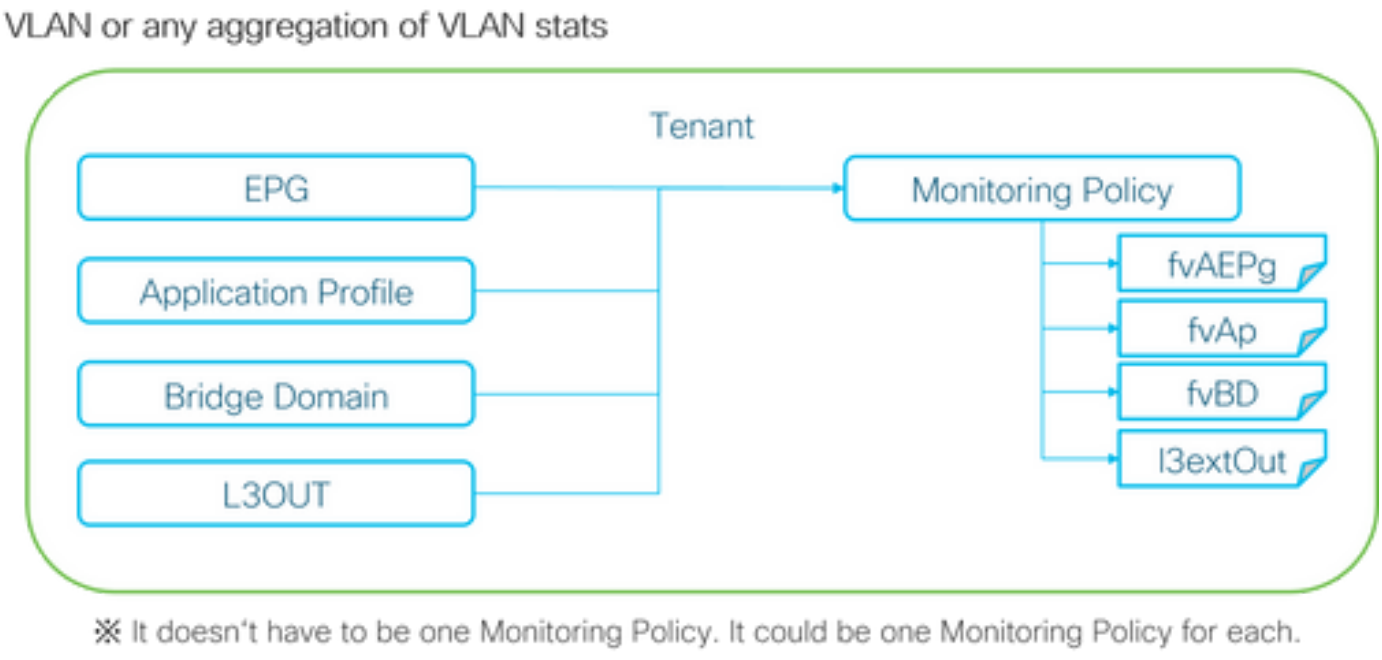


10. 前面パネルポート（アクセスポリシー）の場合、レイヤ1物理インターフェイス設定(l1.PhysIf)とは異なり、Aggregated Interface(pc.AggrIf)についても同じことを実行します。これにより、物理ポートだけでなくポートチャネルにも新しいモニタリングポリシーを適用できます。

（デフォルトのポリシーを使用する場合は、ステップ10をスキップできます）。

l2IngrPktsAgでの入力ドロップパケットレート

これには複数の部分があります。



上の図に示すように、l2IngrPktsAgは多くのオブジェクトの下でモニタされます。上の図は一

部の例のみを示していますが、l2IngrPktsAgのすべてのオブジェクトを示しているわけではありません。ただし、統計情報のしきい値は、l1PhysIfまたはpcAggrIfでモニタリングポリシーおよびeqptIngrDropPktsによって設定されます。

上の図に示すように、各オブジェクト(EPG(fvAEPg)、ブリッジドメイン(fvBD)など)に独自のモニタリングポリシーを割り当てることができます。

デフォルトでは、特に設定しない限り、テナントの下にあるすべてのオブジェクトは、Tenant > common > Monitoring Policies > defaultの下のデフォルトのモニタリングポリシーを使用します。

各コンポーネントごとにしきい値を変更する必要がない限り、テナント共通のデフォルトのモニタリングポリシーを直接変更して、関連するすべてのコンポーネントに変更を適用できます。

この例では、ブリッジドメインのl2IngrPktsAg15minの入力ドロップパケットレートのしきい値を変更します。

1.テナント>（テナント名）> [モニタリングポリシー]に移動します。

（デフォルトのモニタリングポリシーを使用する場合、または新しいモニタリングポリシーをテナント全体に適用する必要がある場合は、テナントを共通にする必要があります）

2. 右クリックして、Create Monitoring Policyを選択します。

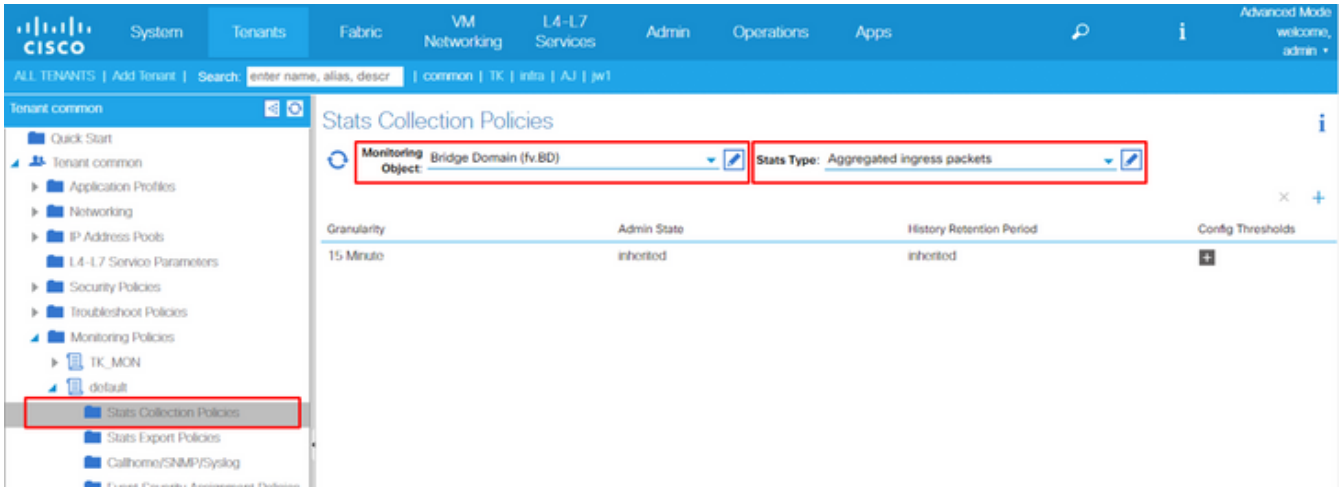
(しきい値の変更をすべてのコンポーネントに適用できる場合は、新しい変更を作成する代わりに、defaultに移動します)。

3. 新しい監視ポリシーまたはデフォルトを展開し、統計収集ポリシーに移動します。

4. 右側のペインでMonitoring Objectの鉛筆アイコンをクリックし、Bridge Domain (fv.BD)を選択します。

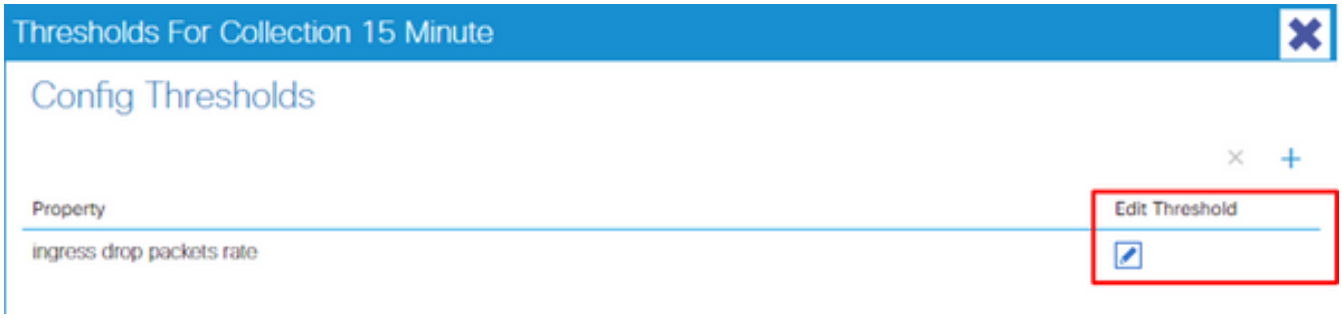
（デフォルトのポリシーを使用する場合は、ステップ4をスキップできます）。

5. 右ペインのMonitoring Objectドロップダウンから、Bridge Domain (fv.BD)とStats Typeを選択し、Aggregated ingress packetsを選択します。

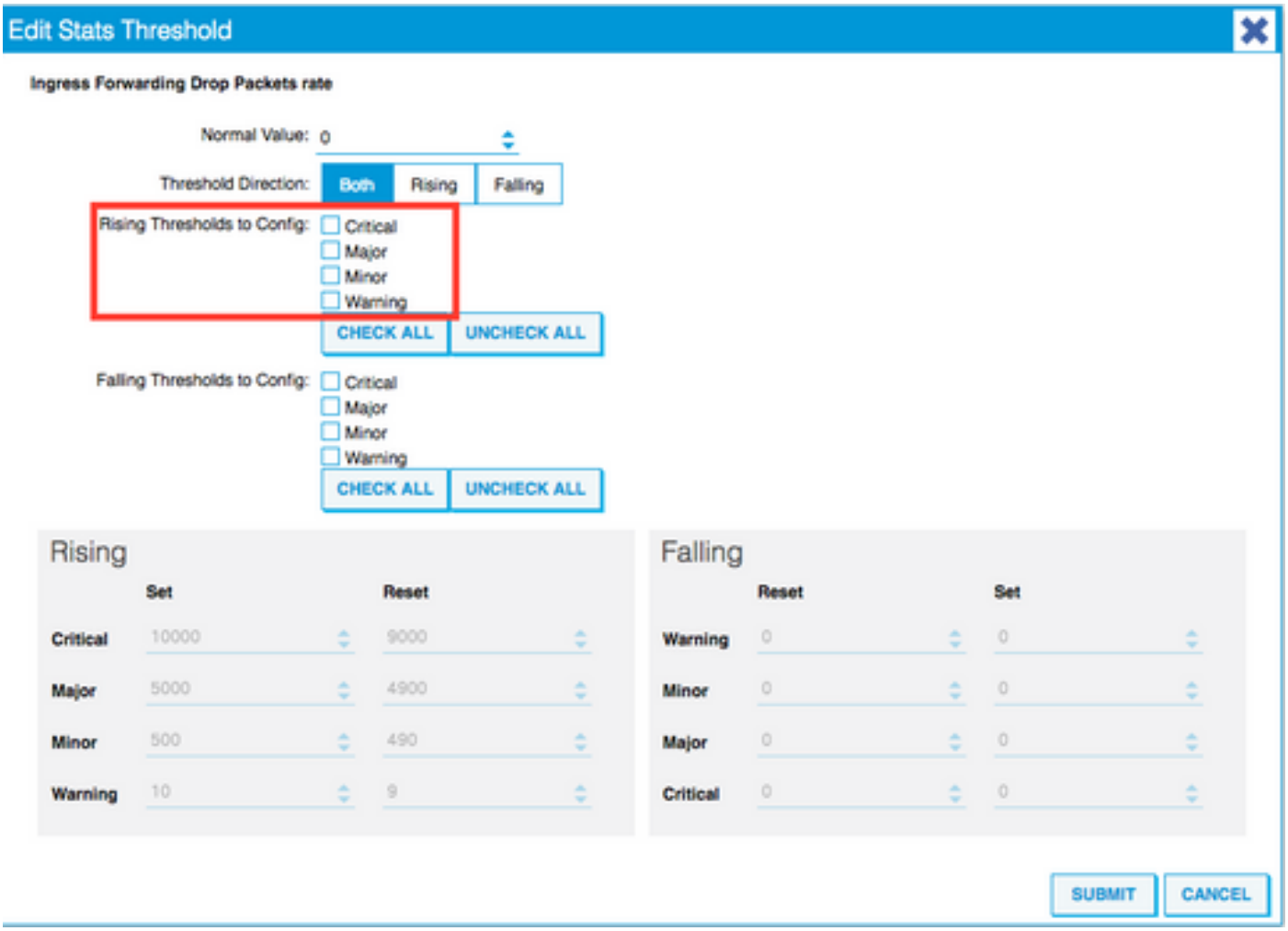


6. Config Thresholdsの横にある+をクリックします。

7. 転送ドロップのしきい値を編集します。

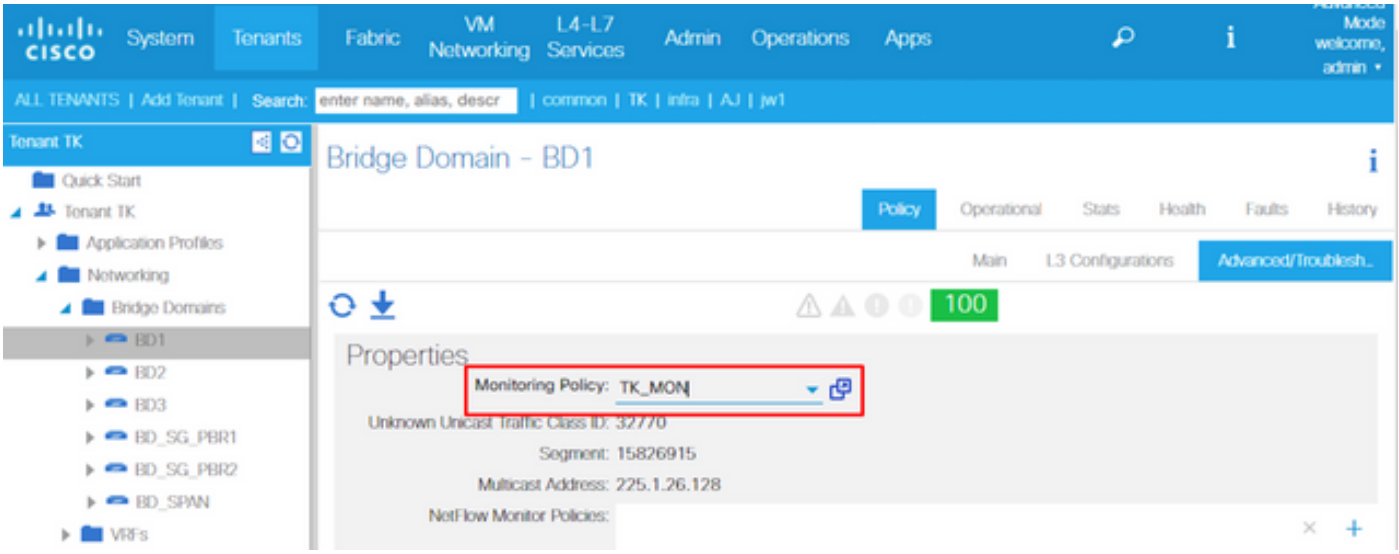


8. 転送ドロップレートのメジャー、マイナー、警告の設定の上昇しきい値を無効にすることが推奨されます。



9. しきい値の変更が必要なブリッジドメインに、この新しいモニタリングポリシーを適用します。

（デフォルトのポリシーを使用する場合は、ステップ9をスキップできます）。



注：
デフォルト以外のモニタリングポリシーには、デフォルトのモニタリングポリシーに存在する設定を含めることはできません。これらの設定をデフォルトのモニタリングポリシーと同じにする必要がある場合、ユーザはデフォルトのモニタリングポリシーの設定を確認し、デフォルト以外のモニタリングポリシーに同じポリシーを手動で設定する必要があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。