

Explicar as falhas de queda de pacote na ACI

Contents

[Introdução](#)

[Objetos gerenciados](#)

[Tipos de Contador de Descarte de Hardware](#)

[Encaminhar](#)

[Erro](#)

[Buffer](#)

[Exibição de estatísticas de queda no CLI](#)

[Objetos gerenciados](#)

[Contadores de hardware](#)

[Folha](#)

[Coluna](#)

[Falhas](#)

[Taxa de pacotes descartados de entrada F112425 \(l2IngrPktsAg15min:dropRate\)](#)

[F100264 - Taxa de Pacotes de Perda de Buffer de Entrada \(eqptIngrDropPkts5min:bufferRate\)](#)

[F100696 - Encaminhamento de entrada de pacotes descartados \(eqptIngrDropPkts5min:forwardingRate\)](#)

[Limite de Estatísticas](#)

[Taxa de Pacotes Descartados de Encaminhamento em eqptIngrDropPkts](#)

[Taxa de Pacotes de Descarte de Entrada em l2IngrPktsAg](#)

Introdução

Este documento descreve cada tipo de falha e o procedimento quando você vê essa falha. Durante a operação normal de uma estrutura da Cisco Application Centric Infrastructure (ACI), o administrador pode ver Falhas de determinados tipos de Quedas de Pacotes.

Objetos gerenciados

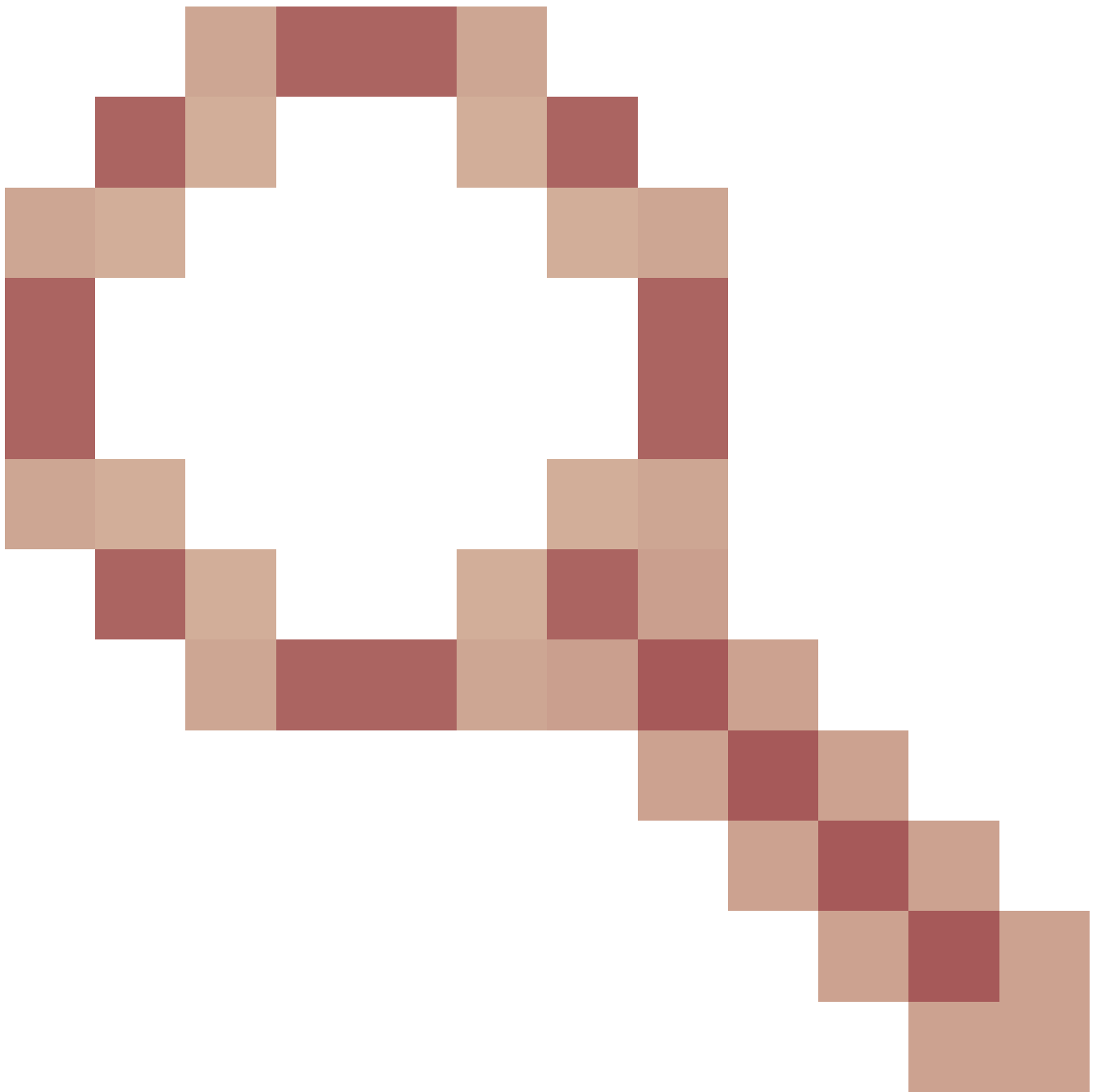
Na Cisco ACI, todas as falhas são apresentadas em Objetos gerenciados (MO). Por exemplo, uma falha F11245 - taxa de pacotes de queda de entrada (l2IngrPktsAg15min:dropRate) é relacionada ao parâmetro dropRate em MO l2IngrPktsAg15min.

Esta seção apresenta alguns dos exemplos de Objeto Gerenciado (MO) relacionados a falhas de descarte de pacotes.

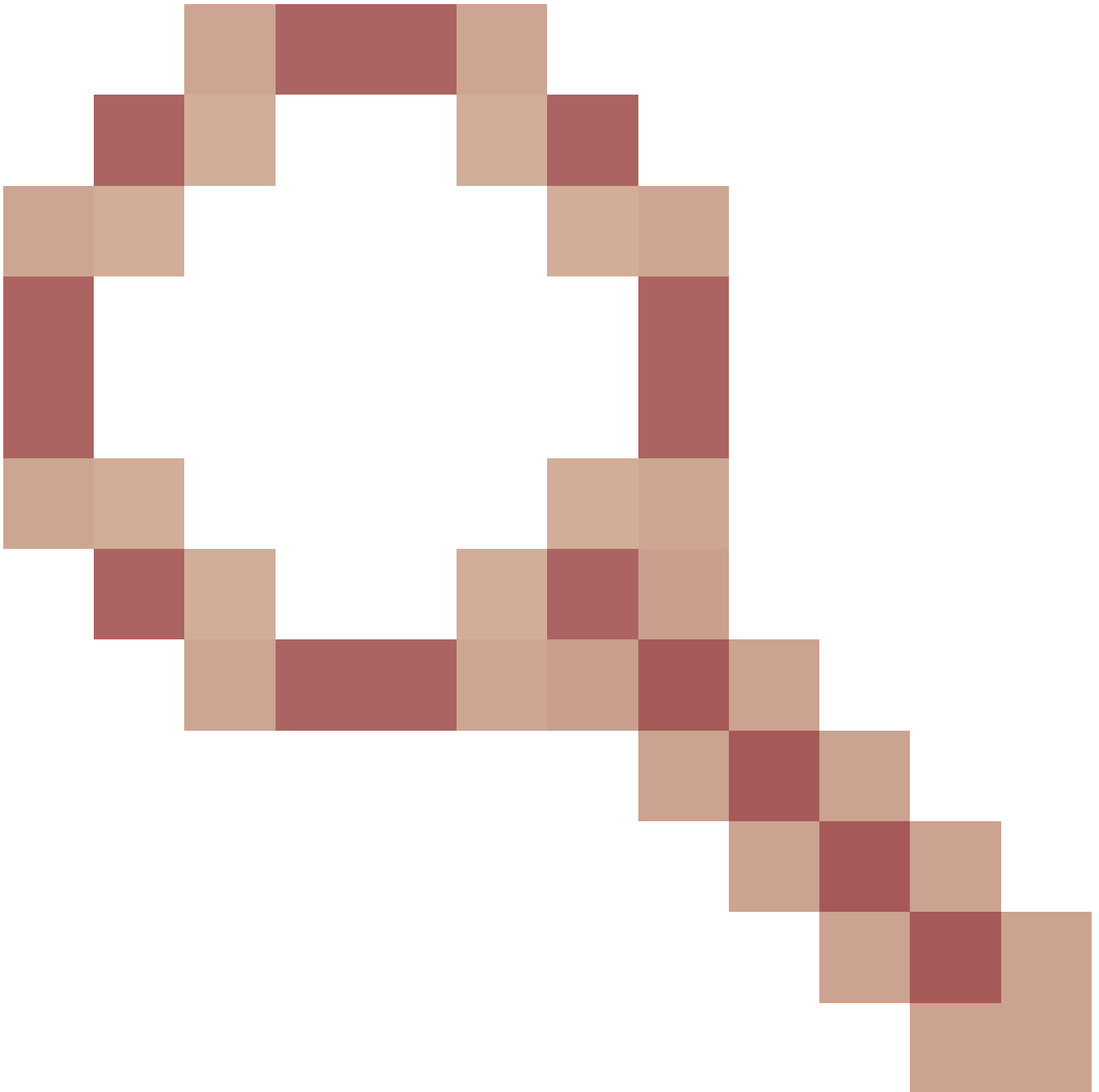
| | Exemplo | Descrição | Parâmetros de exemplo | Exemplo de MO contra |
|--|---------|-----------|-----------------------|----------------------|
| | | | | |

| | | | | |
|------------------|---|---|---|--|
| | | | | quais falhas são geradas |
| l2IngrPkts | l2IngrPkts5min l2IngrPkts15min l2IngrPkts1h etc. | Isso representa as estatísticas de pacotes de entrada por VLAN durante cada período. | taxa de queda floodRate multicastRate unicastRate | vlanCktEp (VLAN) |
| l2IngrPktsAg | l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d etc. | Isso representa estatísticas de pacotes de entrada por EPG, BD, VRF e assim por diante. Por exemplo, EPG stats representa a agregação de estatísticas de VLAN que pertencem ao EPG. | taxa de queda floodRate multicastRate unicastRate | fvAEPg (EPG) fvAp (Perfil do aplicativo) fvBD (BD) l3extSaída (L3OUT) |
| eqptIngrDropPkts | eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d etc. | Isso representa estatísticas de pacotes de queda de entrada por interface durante cada período. | Taxa de encaminhamento *1 Taxa de erro *1 *1 bufferTaxa | l1PhysIf (porta física) pcAggrIf (canal de porta) |

*1: esses contadores em eqptIngrDropPkts podem ser erroneamente elevados devido a uma limitação de ASIC em várias plataformas Nexus 9000, pois os pacotes SUP_REDIRECT estão sendo registrados como descartes de encaminhamento. Consulte também o bug da Cisco ID [CSCvo68407](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvo68407)



e o bug da Cisco ID [CSCvn72699](#)



para obter mais detalhes e versões corrigidas.

Tipos de Contador de Descarte de Hardware

Nos switches Nexus 9000 executados no modo ACI, há 3 contadores de hardware principais para razão de queda de interface de entrada no ASIC.

Uma `dropRate` em `I2IngrPkts`, `I2IngrPktsAg` inclui esses contadores. Três parâmetros (`forwardingRate`, `errorRate`, `bufferRate`) na tabela para `eqptIngrDropPkts` representam cada um dos três contadores de interface.

Encaminhar

Descartes de encaminhamento são pacotes que são descartados no bloco de consulta (LU) do ASIC. No bloco LU, uma decisão de encaminhamento de pacote é tomada com base nas

informações do cabeçalho do pacote. Se a decisão for descartar o pacote, Descartar encaminhamento será contado. Há uma variedade de razões para isso acontecer, mas falemos sobre as principais:

SECURITY_GROUP_DENY

Uma queda devido à falta de contratos para permitir a comunicação.

Quando um pacote entra na estrutura, o switch examina o EPG de origem e de destino para ver se há um contrato que permita essa comunicação. Se a origem e o destino estiverem em EPGs diferentes e não houver nenhum contrato que permita esse tipo de pacote entre eles, o switch descartará o pacote e o rotulará como SECURITY_GROUP_DENY. Isso incrementa o contador Descartar Encaminhamento.

VLAN_XLATE_MISS

Uma queda devido a uma VLAN inadequada.

Quando um pacote entra na estrutura, o switch examina o pacote para determinar se a configuração na porta permite esse pacote. Por exemplo, um quadro entra na estrutura com uma marca 802.1Q de 10. Se o switch tiver a VLAN 10 na porta, ele inspecionará o conteúdo e tomará uma decisão de encaminhamento com base no MAC de destino. No entanto, se a VLAN 10 não estiver na porta, ela será descartada e rotulada como VLAN_XLATE_MISS. Isso incrementa o contador Descartar Encaminhamento.

O motivo para XLATE ou Translate é que, na ACI, o switch leaf pega um quadro com um encapsulamento 802.1Q e o converte em uma nova VLAN que é usada para VXLAN e outra normalização dentro da estrutura. Se o quadro vier com uma VLAN não implantada, a conversão falhará.

ACL_DROP

Uma queda por causa de sup-tcam.

o sup-tcam em switches ACI contém regras especiais a serem aplicadas sobre a decisão normal de encaminhamento de L2/L3. As regras em sup-tcam são incorporadas e não podem ser configuradas pelo usuário. O objetivo das regras de sup-tcam é lidar principalmente com algumas exceções ou com parte do tráfego do plano de controle e não se destina a ser verificado ou monitorado pelos usuários. Quando o pacote está atingindo as regras de sup-tcam e a regra é descartar o pacote, o pacote descartado é contado como ACL_DROP e incrementa o contador de Descarte de Encaminhamento. Quando isso ocorre, geralmente significa que o pacote está prestes a ser encaminhado em relação aos princípios básicos de encaminhamento da ACI.

Mesmo que o nome do descarte seja ACL_DROP, essa ACL não é a mesma que a lista de controle de acesso normal que pode ser configurada em dispositivos NX-OS autônomos ou em qualquer outro dispositivo de roteamento/switching.

SUP_REDIRECT

Isso não é uma gota.

Um pacote redirecionado sup (por exemplo, CDP/LLDP/UDLD/BFD e assim por diante) pode ser contado como Descarte de Encaminhamento mesmo que o pacote seja processado corretamente e encaminhado para a CPU.

Isso ocorre nas plataformas -EX, -FX e -FX2, como N9K-C93180YC-EX ou N9K-C93180YC-FX. Estes não podem ser contados como queda, no entanto, é por causa da limitação ASIC em plataformas -EX/-FX/-FX2.

Erro

Quando o switch recebe um quadro inválido em uma das interfaces do painel frontal, ele é descartado como um erro. Exemplos disso incluem quadros com erros de FCS ou CRC. Ao observar as portas leaf Uplink/Downlink ou portas spine, é melhor verificar se há erros de FCS/CRC usando show interface. No entanto, em operações normais, espera-se que os pacotes de erro sejam incrementados nas portas Uplink/Downlinks de leafs ou portas Spine, pois esse contador também inclui quadros que são removidos pelo sistema e não espera-se que sejam enviados para fora da interface.

Exemplo: falhas de TTL para pacotes roteados, quadros de broadcast/inundados da mesma interface.

Buffer

Quando o switch recebe um quadro e não há créditos de buffer disponíveis para entrada ou saída, o quadro é descartado com o Buffer. Isso geralmente sugere um congestionamento em algum lugar da rede. O link que está mostrando a falha pode estar cheio ou o link que contém o destino pode estar congestionado.

Exibição de estatísticas de queda no CLI

Objetos gerenciados

Secure Shell (SSH) para um dos APIC e execute esses comandos.

```
apic1#moquery -c I2IngrPktsAg15min
```

Fornecer todas as instâncias de objeto desta classe I2IngrPktsAg15min.

Aqui está um exemplo com um filtro para consultar um objeto específico. Neste exemplo, o filtro deve mostrar apenas um objeto com atributos dn que inclui tn-TENANT1/ap-APP1/epg-EPG1.

Além disso, este exemplo usa egrep para mostrar apenas atributos obrigatórios.

Saída de exemplo 1: objeto de contador EPG (l2IngrPktsAg15min) do locatário TENANT1, perfil de aplicativo APP1, epg EPG1.

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

| | | | |
|--------------|---|---|---|
| dn | : | uni/tn-TENANT1/ap-APP1/epg-EPG1/CD12IngrPktsAg15min | |
| dropPer | : | 30 | <--- number of drop packet in the current periodic interval |
| dropRate | : | 0.050000 | <--- drop packet rate = dropPer(30) / periodic interval |
| 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 |

Ou podemos usar outra opção -d em vez de -c para obter um objeto específico se você souber o dn do objeto.

Exemplo de saída 2: objeto de contador EPG (l2IngrPktsAg15min) do locatário TENANT1, perfil de aplicativo APP1, epg EPG2.

```
apic1# moquery -d uni/tn-TENANT1/ap-APP1/epg-EPG2/CD12IngrPktsAg15min | egrep 'dn|drop[P,R]|rep'
```

| | | | |
|--------------|---|---------------------------------------|--|
| dn | : | uni/tn-jw1/BD-jw1/CD12IngrPktsAg15min | |
| dropPer | : | 30 | |
| dropRate | : | 0.050000 | |
| repIntvEnd | : | 2017-03-03T15:54:58.021-08:00 | |
| repIntvStart | : | 2017-03-03T15:44:58.020-08:00 | |

Contadores de hardware

Se você vir falhas ou quiser verificar descartes de pacotes nas portas do switch usando o CLI, a melhor maneira de fazer isso é visualizando os contadores da plataforma no hardware. A maioria dos contadores, mas não todos, é mostrada usando show interface. Os 3 motivos principais de queda só podem ser visualizados usando os contadores da plataforma. Para visualizá-los, execute estas etapas:

Folha

Use SSH para a folha e execute esses comandos.

```
ACI-LEAF#vsh_lc  
module-1# show platform internal counters port <X>
```

* onde X representa o número da porta

Exemplo de saída para Ethernet 1/31:

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

Coluna

Para um tipo de caixa spine (N9K-C9336PQ), é exatamente o mesmo que Leaf.

Para colunas modulares (N9K-C9504 e assim por diante), você deve primeiro anexar a placa de linha específica antes de poder visualizar os contadores da plataforma. Use SSH para o spine e execute estes comandos:

```
ACI-SPINE#vsh
```

```
ACI-SPINE#attach module <X>
```

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

* onde X representa o número do módulo da placa de linha que você gostaria de visualizar

Y representa o número da porta

Exemplo de saída para ethernet 2/1:

<#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 -----

Falhas

F112425 - Taxa de pacotes descartados de entrada
(I2IngrPktsAg15min:dropRate)

Descrição:

Uma das razões mais comuns para essa falha é que os pacotes da Camada 2 são descartados com a razão de Descarte de Encaminhamento. Há uma variedade de razões, mas a mais comum é:

Em algumas plataformas (consulte o bug da Cisco ID [CSCvo68407](#)), há uma limitação em que os pacotes L2 que precisam ser redirecionados para a CPU (por exemplo, CDP/LLDP/UDLD/BFD e assim por diante), são registrados como uma queda de encaminhamento e são copiados para a CPU. Isso se deve a uma limitação do ASIC usado nesses modelos.

Resolução:

As quedas descritas são puramente cosméticas, portanto, a melhor prática recomendada é aumentar o limite para a falha, como mostrado na seção Limite de estatísticas. Para fazer isso, consulte as instruções no Stats Threshold.

F100264 - Taxa de Pacotes de Perda de Buffer de Entrada (eqptIngrDropPkts5min:bufferRate)


Descrição:

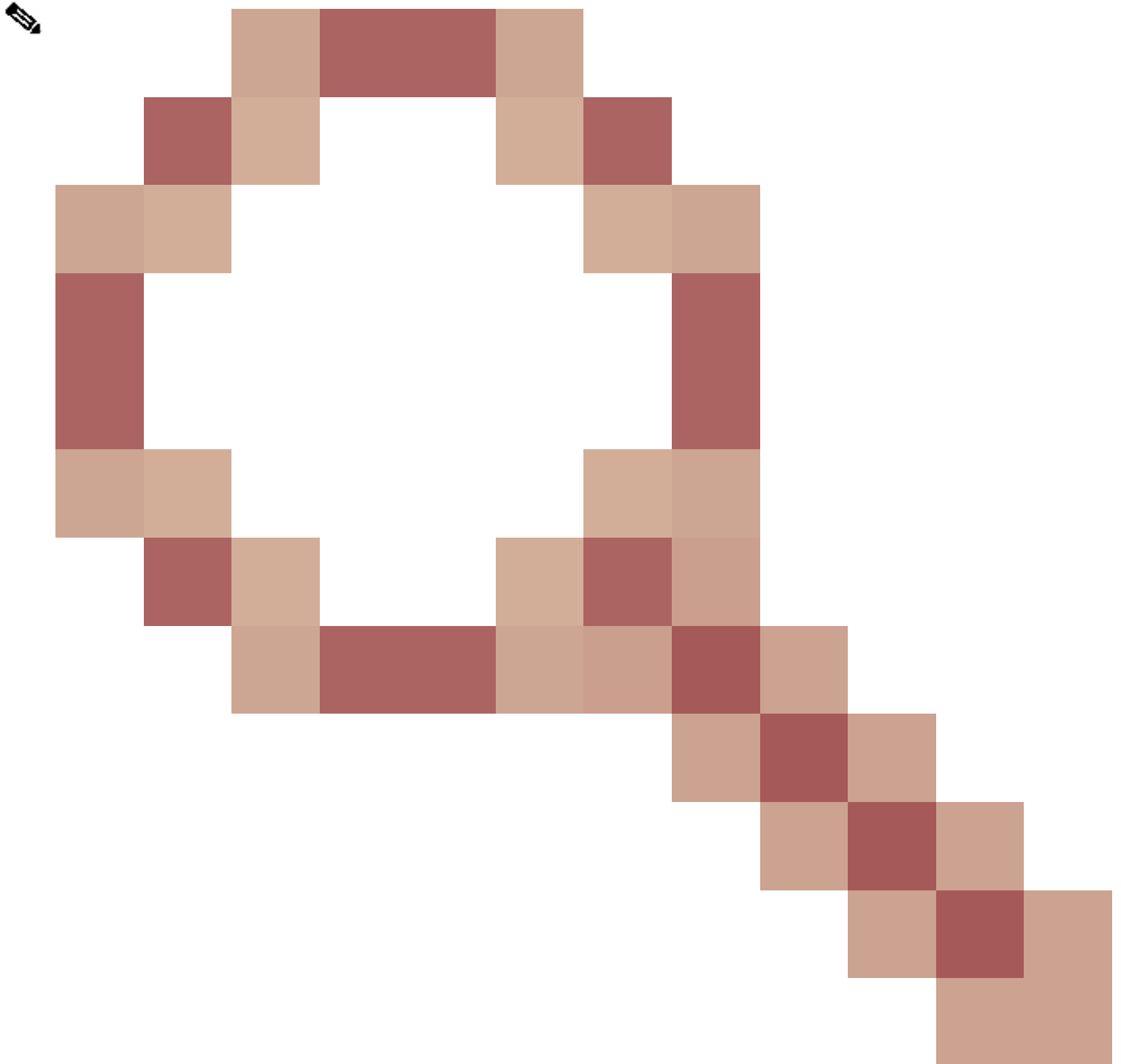
Essa falha pode ser incrementada quando os pacotes estão sendo descartados em uma porta com o motivo Buffer. Como mencionado anteriormente, isso geralmente acontece quando há congestionamento em uma interface na direção de entrada ou de saída.

Resolução:

Essa falha representa pacotes descartados no ambiente devido ao congestionamento. Os pacotes descartados podem estar causando problemas com os aplicativos em execução na estrutura da ACI. Os administradores de rede podem isolar o fluxo de pacotes e determinar se o congestionamento é devido a fluxos de tráfego inesperados, balanceamento de carga ineficiente e assim por diante ou utilização esperada nessas portas.

F100696 - Encaminhamento de entrada de pacotes descartados (eqptIngrDropPkts5min:forwardingRate)

 Observação: uma limitação ASIC como a mencionada anteriormente para F11245 pode fazer com que essas falhas também sejam levantadas. Consulte o bug da Cisco ID [CSCvo68407](#)



para obter mais detalhes.

Essa falha é causada por alguns cenários. O mais comum é:

Descrição 1) Gotas da Coluna

Se essa falha for vista em uma interface Spine, pode ser devido ao tráfego em direção a um endpoint desconhecido. Quando um pacote ARP ou IP é encaminhado para a coluna para uma consulta de proxy e o ponto final é desconhecido na estrutura, um pacote glean especial é gerado e enviado a todos os leafs no endereço de grupo multicast BD (interno) apropriado. Isso dispara uma solicitação ARP de cada folha no domínio de ponte (BD) para descobrir o ponto final. Devido a uma limitação, o pacote de limpeza recebido pela folha também é refletido de volta na estrutura novamente e aciona uma queda de encaminhamento no link da coluna conectada à folha. A queda direta nesse cenário é incrementada apenas no hardware spine da geração 1.

Resolução 1)

Como se sabe que o problema é causado por um dispositivo que envia uma quantidade desnecessária de tráfego unicast desconhecido para a estrutura da ACI, é necessário descobrir qual dispositivo está causando isso e ver se isso pode ser evitado. Isso geralmente é causado por dispositivos que verificam ou sondam endereços IP em sub-redes para fins de monitoramento. Para descobrir qual IP está enviando esse tráfego, use o SSH na folha conectada à interface spine mostrando a falha.

A partir daí, você pode executar este comando para ver o endereço IP de origem (sip) que está acionando o pacote glean:

```
<#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.
```

Neste exemplo de saída, o pacote glean é disparado por 192.168.21.150 e é recomendável ver se isso pode ser mitigado.

Descrição 2) Leaf Drops

Se essa falha for vista em uma interface de folha, a causa mais provável é devido a quedas SECURITY_GROUP_DENY mencionadas.

Resolução 2)

A folha da ACI mantém um registro dos pacotes negados devido a violações. Esse registro não captura todos eles para proteger os recursos da CPU, no entanto, ele ainda fornece uma grande quantidade de registros.

Para obter os registros necessários, se a interface em que a falha é gerada fizer parte de um canal de porta, é necessário usar esse comando e grep para o canal de porta. Caso contrário, a interface física pode ser ignorada.

Esse registro pode ser rapidamente transferido, dependendo da quantidade de quedas de contrato.

<#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
```

Nesse caso, 192.168.21.150 está tentando enviar mensagens ICMP (número de protocolo IP 1) para 192.168.20.3. No entanto, não há contrato entre os 2 EPGs que permitem o ICMP, portanto, o pacote é descartado. Se o ICMP deve ser permitido, um contrato pode ser adicionado entre os dois EPGs.

Limite de Estatísticas

Esta seção descreve como alterar um limite para objetos de estatísticas que poderiam potencialmente levantar uma falha contra o contador de queda.

Um limite para estatísticas de cada objeto (por exemplo, l2IngrPkts, eqptIngrDropPkts) é configurado por meio da Política de Monitoramento em relação a vários objetos.

Como mencionado na tabela no início, eqptIngrDropPkts é monitorado em, por exemplo, objetos l1PhysIf por meio da Política de monitoramento.

Taxa de Pacotes Descartados de Encaminhamento em eqptIngrDropPkts

Há duas partes para isso.

- + Políticas de acesso (portas para dispositivos externos, também conhecidas como portas do painel frontal)

- + Políticas de malha (portas entre LEAF e SPINE, também conhecidas como portas de malha)

Front Panel Ports (ports towards external devices)



Fabric Ports (ports between LEAF and SPINE)



Cada objeto de porta (I1Physlf, pcAggrlf) pode receber sua própria Política de monitoramento através do Grupo de Política de Interface, como mostrado na figura acima.

Por padrão, há uma política de monitoramento padrão em Fabric > Access Policies e Fabric > Fabric Policies na GUI do APIC. Essas Políticas de monitoramento padrão são atribuídas a todas as portas, respectivamente. A política de monitoramento padrão em Políticas de acesso é para portas do painel frontal e a política de monitoramento padrão em Políticas de malha é para portas de malha.

A menos que seja necessário alterar limites por portas, a política de monitoramento padrão em cada seção pode ser modificada diretamente para aplicar a alteração a todas as portas do painel frontal e/ou portas de estrutura.

Este exemplo é para alterar limites para Queda de encaminhamento em eqptIngrDropPkts em portas de malha (Políticas de malha). Faça o mesmo em Fabric > Access Policies (Estrutura > Políticas de acesso) para portas do painel frontal.

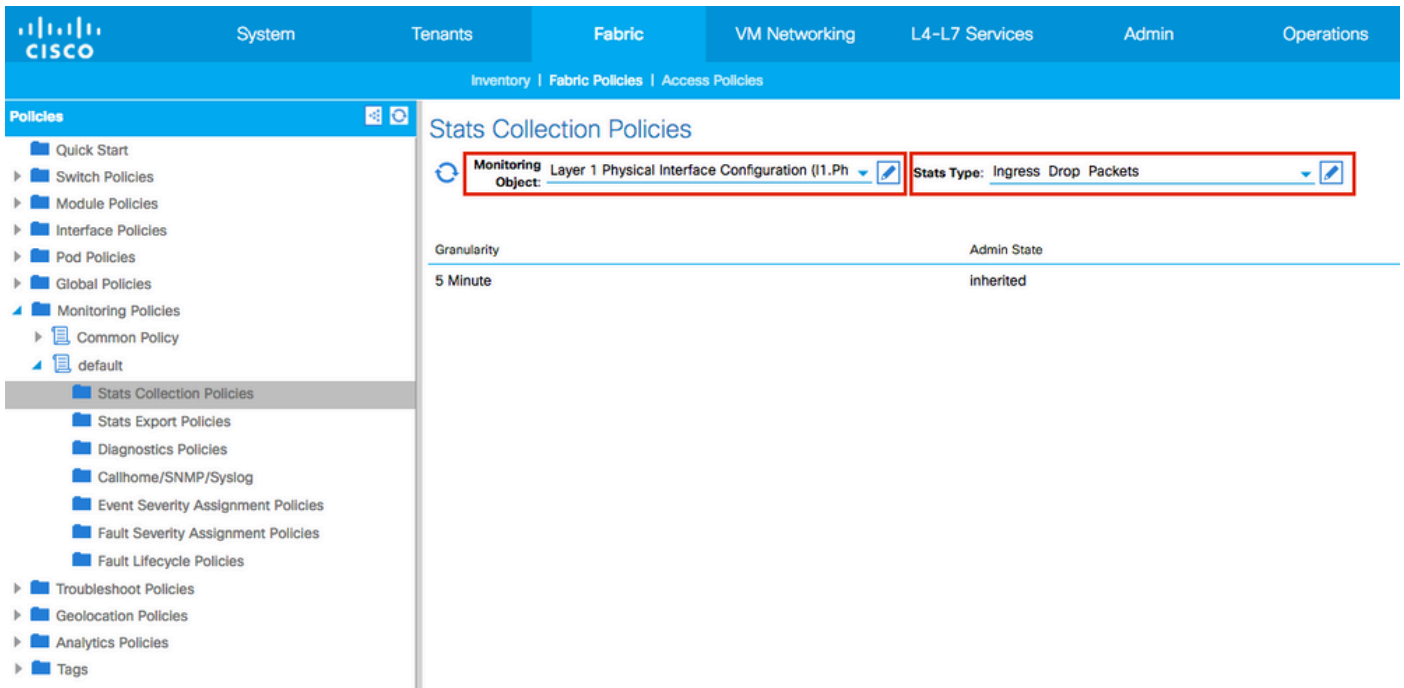
1. Navegue até Fabric > Fabric Policies > Monitoring Policies.
2. Clique com o botão direito do mouse e selecione Criar Política de Monitoramento.

(Se a alteração de limite puder ser aplicada a todas as portas de malha, navegue para o padrão em vez de criar uma nova.)

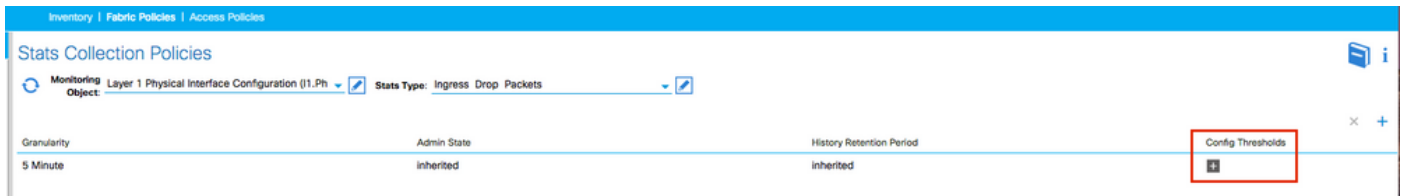
3. Expanda a nova Política de Monitoramento ou padrão e navegue até Políticas de Coleta de Estatísticas.
4. Clique no ícone do lápis para o Objeto de Monitoramento no painel direito, selecione Configuração de Interface Física da Camada 1 (I1.Physlf).

(A Etapa 4 pode ser ignorada quando a política padrão for usada.)

5. No menu suspenso Monitoring Object no painel direito, escolha Layer 1 Physical Interface Configuration (I1.PhysIf) e Stats Type, escolha Ingress Drop Packets






6. Clique no botão + Próximo a Config Thresholds.



7. Edite o Limite para Eliminação de Encaminhamento.

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 |  |

CLOSE

8. A recomendação é desativar o aumento dos limites para configurar para crítico, principal, secundário e aviso para taxa de queda de encaminhamento.

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

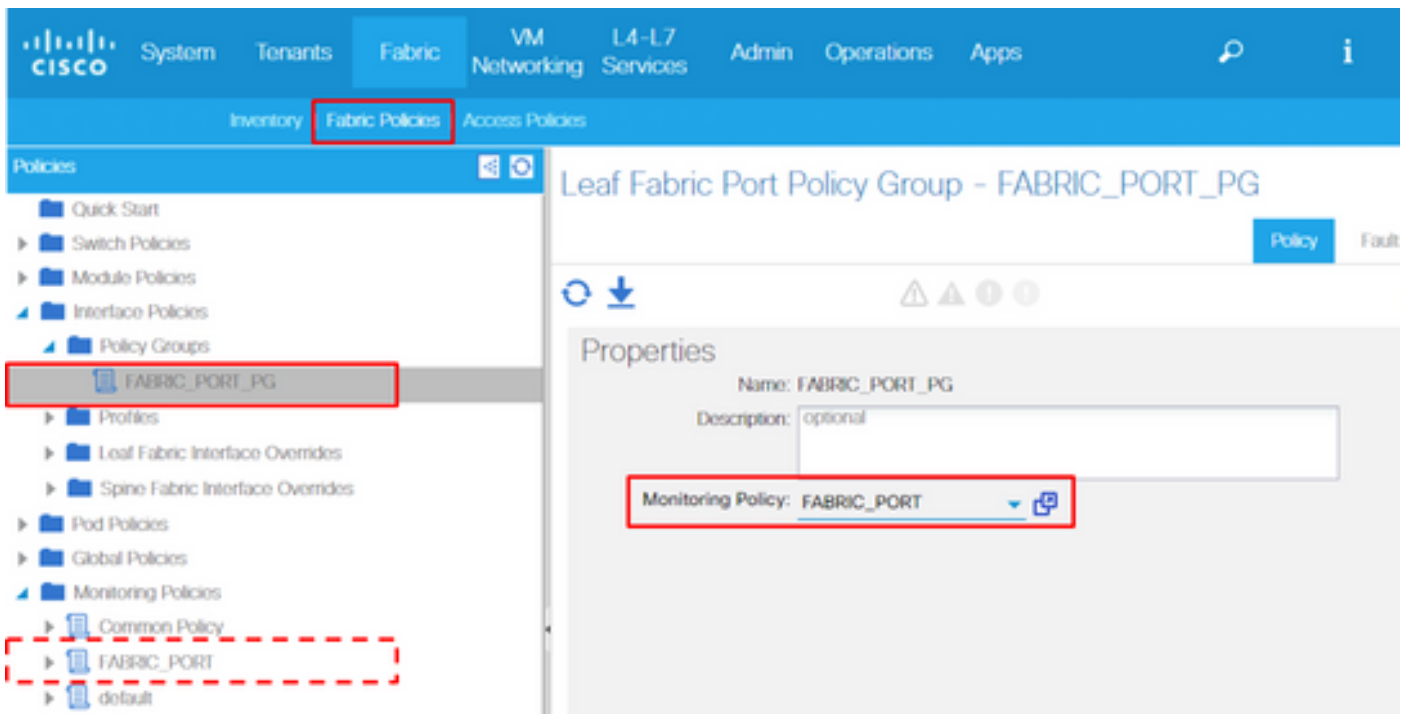
| | Set | Reset |
|-----------------|-------|-------|
| Critical | 10000 | 9000 |
| Major | 5000 | 4900 |
| Minor | 500 | 490 |
| Warning | 10 | 9 |

| | Reset | Set |
|-----------------|-------|-----|
| Warning | 0 | 0 |
| Minor | 0 | 0 |
| Major | 0 | 0 |
| Critical | 0 | 0 |

SUBMIT CANCEL

9. Aplique esta nova Política de Monitoramento ao Grupo de Política de Interface para as portas necessárias. Não se esqueça de configurar o Perfil de interface, o Perfil do switch e assim por diante nas Políticas de estrutura de acordo.

(A Etapa 9 pode ser ignorada quando a política padrão for usada.)



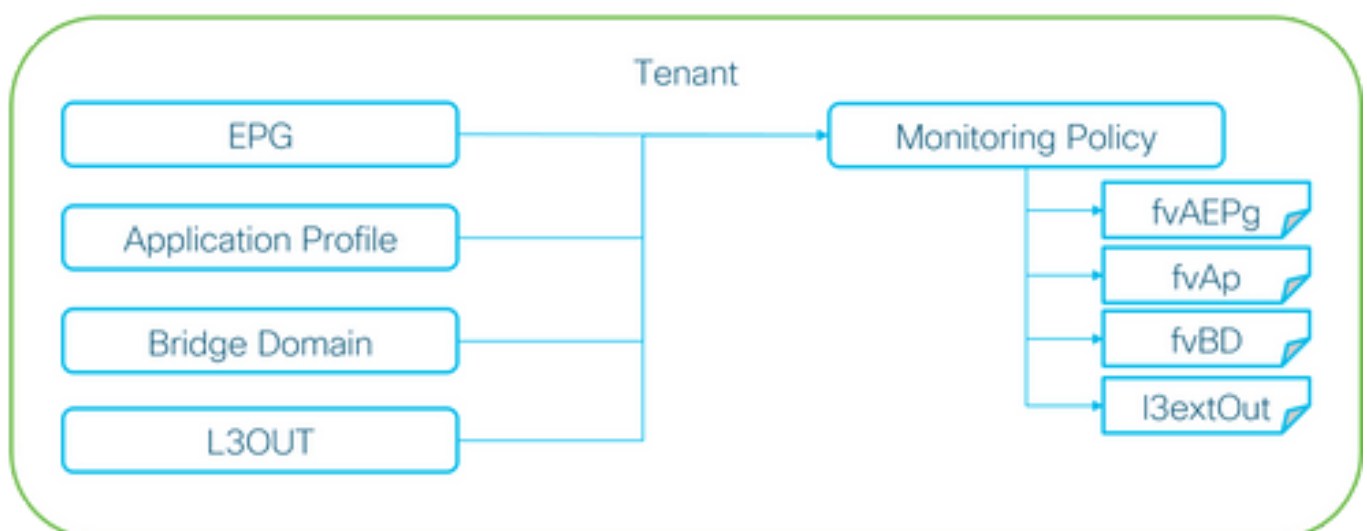
10. Se for para as portas do painel frontal (Políticas de acesso), execute o mesmo procedimento para a Interface agregada (pc.AggrIf) em oposição à Configuração de interface física da camada 1 (I1.PhysIf) para que esta nova Política de monitoramento possa ser aplicada ao canal de porta e também à porta física.

(A Etapa 10 pode ser ignorada quando a política padrão for usada.)

Taxa de Pacotes de Descarte de Entrada em I2IngrPktsAg

Há várias partes para isso.

VLAN or any aggregation of VLAN stats



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

Como mostra a figura acima, I2IngrPktsAg é monitorado em muitos objetos. A figura acima

mostra apenas alguns exemplos, mas não todos os objetos para I2IngrPktsAg. No entanto, o limite para estatísticas é configurado por meio da Diretiva de Monitoramento, bem como de eqptIngrDropPkts em I1PhysIf ou pcAggrIf.

Cada objeto (EPG(fvAEPg), domínio de ponte (fvBD), etc.) pode receber sua própria política de monitoramento, como mostrado na figura acima.

Por padrão, todos esses objetos em locatário usam a Política de monitoramento padrão em Locatário > comum > Políticas de monitoramento > padrão, a menos que seja configurado de outra forma.

A menos que seja necessário alterar os limites por cada componente, a Política de Monitoramento padrão em locatário comum pode ser modificada diretamente para aplicar a alteração para todos os componentes relacionados.

Este exemplo é para alterar os limites da taxa de pacotes de queda de entrada em I2IngrPktsAg15min no domínio de ponte.

1. Navegue até Locatário > (nome do locatário) > Políticas de Monitoramento.

(o locatário precisa ser comum se a política de monitoramento padrão for usada ou a nova política de monitoramento precisar ser aplicada a todos os locatários)

2. Clique com o botão direito do mouse e selecione Criar Política de Monitoramento.

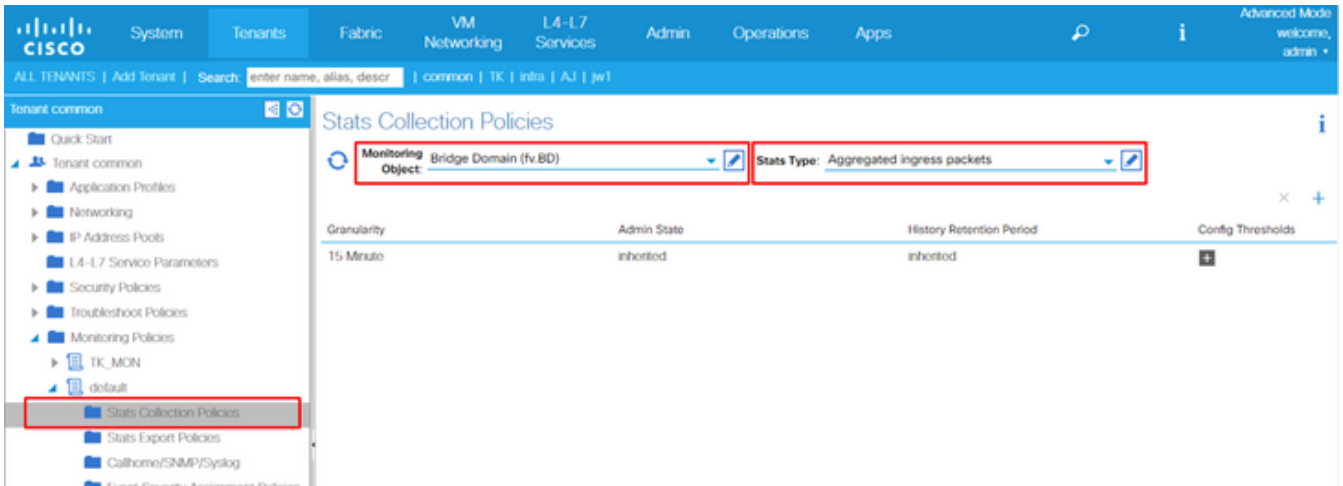
(Se a alteração de limite puder ser aplicada a todos os componentes, navegue para o padrão em vez de criar um novo.)

3. Expanda a nova Política de Monitoramento ou padrão e navegue até Políticas de Coleta de Estatísticas.

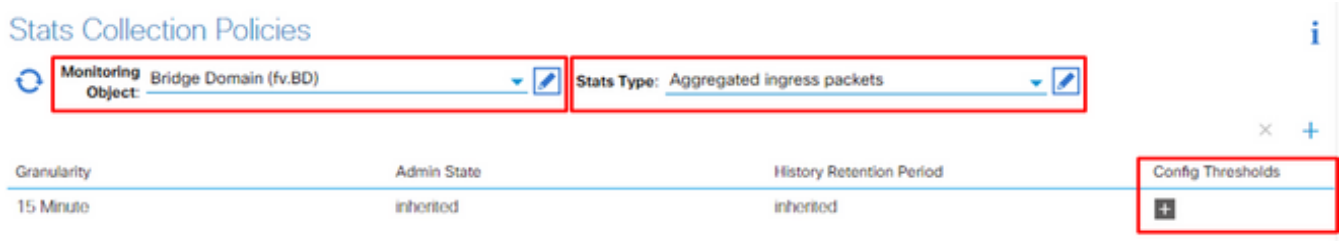
4. Clique no ícone do lápis para o Objeto de Monitoramento no painel direito, selecione Domínio do Bridge (fv.BD).

(A Etapa 4 pode ser ignorada quando a política padrão for usada.)

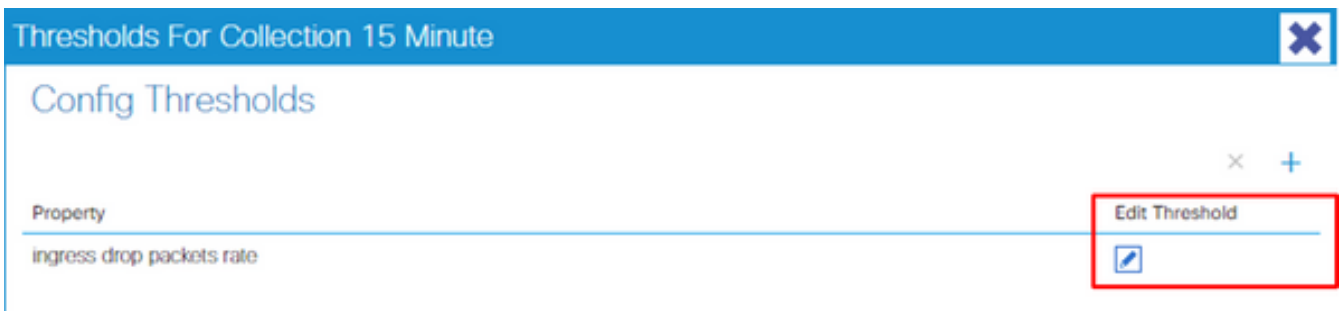
5. No menu suspenso Monitoring Object no painel direito, escolha Bridge Domain (fv.BD) e Stats Type, escolha Aggregated ingress packets.



6. Clique no botão + Próximo a Config Thresholds.



7. Edite o Limite para Eliminação de Encaminhamento.



8. A recomendação é desativar o aumento dos limites para configurar para crítico, principal, secundário e aviso para taxa de queda de encaminhamento.

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 | | | Falling | | |
|----------|-------|-------|----------|-------|-----|
| | Set | Reset | | Reset | Set |
| Critical | 10000 | 9000 | Warning | 0 | 0 |
| Major | 5000 | 4900 | Minor | 0 | 0 |
| Minor | 500 | 490 | Major | 0 | 0 |
| Warning | 10 | 9 | Critical | 0 | 0 |


SUBMIT CANCEL

9. Aplique esta nova Política de Monitoramento ao Domínio de Bridge, que requer alteração de limite.

(A Etapa 9 pode ser ignorada quando a política padrão for usada.)

The screenshot shows the Cisco SD-WAN GUI for a Tenant TK. The left sidebar shows the navigation tree with 'Bridge Domains' expanded to 'BD1'. The main panel shows the configuration for 'Bridge Domain - BD1'. The 'Policy' tab is selected, and the 'Monitoring Policy' is set to 'TK_MON', which is highlighted with a red box. Other properties shown include 'Unknown Unicast Traffic Class ID: 32770', 'Segment: 15826915', and 'Multicast Address: 225.1.26.128'. A green status indicator shows '100'.

NOTE:
A Política de Monitoramento não padrão não pode ter configurações presentes na Política de Monitoramento padrão. Se for necessário manter essas configurações iguais à Política

 de Monitoramento padrão, os usuários precisarão verificar a configuração da Política de Monitoramento padrão e configurar manualmente as mesmas políticas em uma Política de Monitoramento não padrão.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.