

Explicaciones de los errores de paquetes descartados en ACI

Contenido

[Introducción](#)

[Objetos administrados](#)

[Tipos de contadores de caídas de hardware](#)

[Reenvío](#)

[Error](#)

[Buffer](#)

[Visualización de estadísticas de descarte en CLI](#)

[Objetos administrados](#)

[Contadores de hardware](#)

[Hoja](#)

[Columna](#)

[Fallos](#)

[F112425 - velocidad de paquetes descartados de entrada \(I2IngrPktsAg15min:dropRate\)](#)

[F100264 - velocidad de paquetes descartados del búfer de entrada \(eqptIngrDropPkts5min:bufferRate\)](#)

[F100696 - paquetes descartados de reenvío de entrada \(eqptIngrDropPkts5min:forwardingRate\)](#)

[Umbral de estadísticas](#)

[Velocidad de paquetes descartados de reenvío en eqptIngrDropPkts](#)

[Tasa de paquetes descartados de entrada en I2IngrPktsAg](#)

Introducción

Este documento describe cada tipo de falla y el procedimiento para detectar esta falla. Durante el funcionamiento normal de un fabric de Cisco Application Centric Infrastructure (ACI), es posible que el administrador detecte fallos en determinados tipos de caídas de paquetes.

Objetos administrados

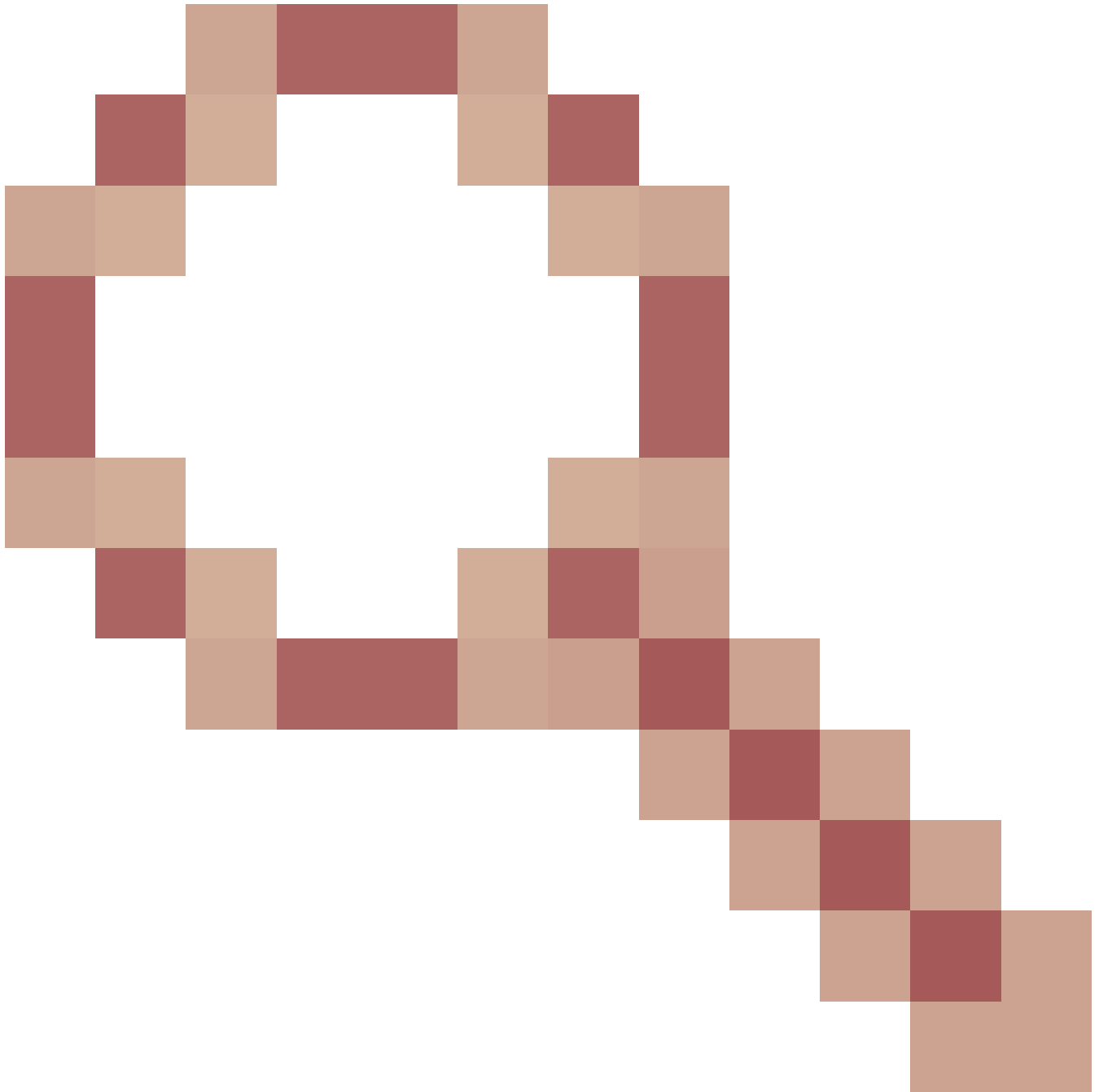
En Cisco ACI, todos los fallos se generan en objetos administrados (MO). Por ejemplo, un error " F11245 - tasa de paquetes descartados de ingreso (I2IngrPktsAg15min:dropRate) " se refiere al parámetro dropRate en MO I2IngrPktsAg15min.

Esta sección presenta algunos ejemplos de objetos administrados (MO) relacionados con fallos de paquetes descartados.

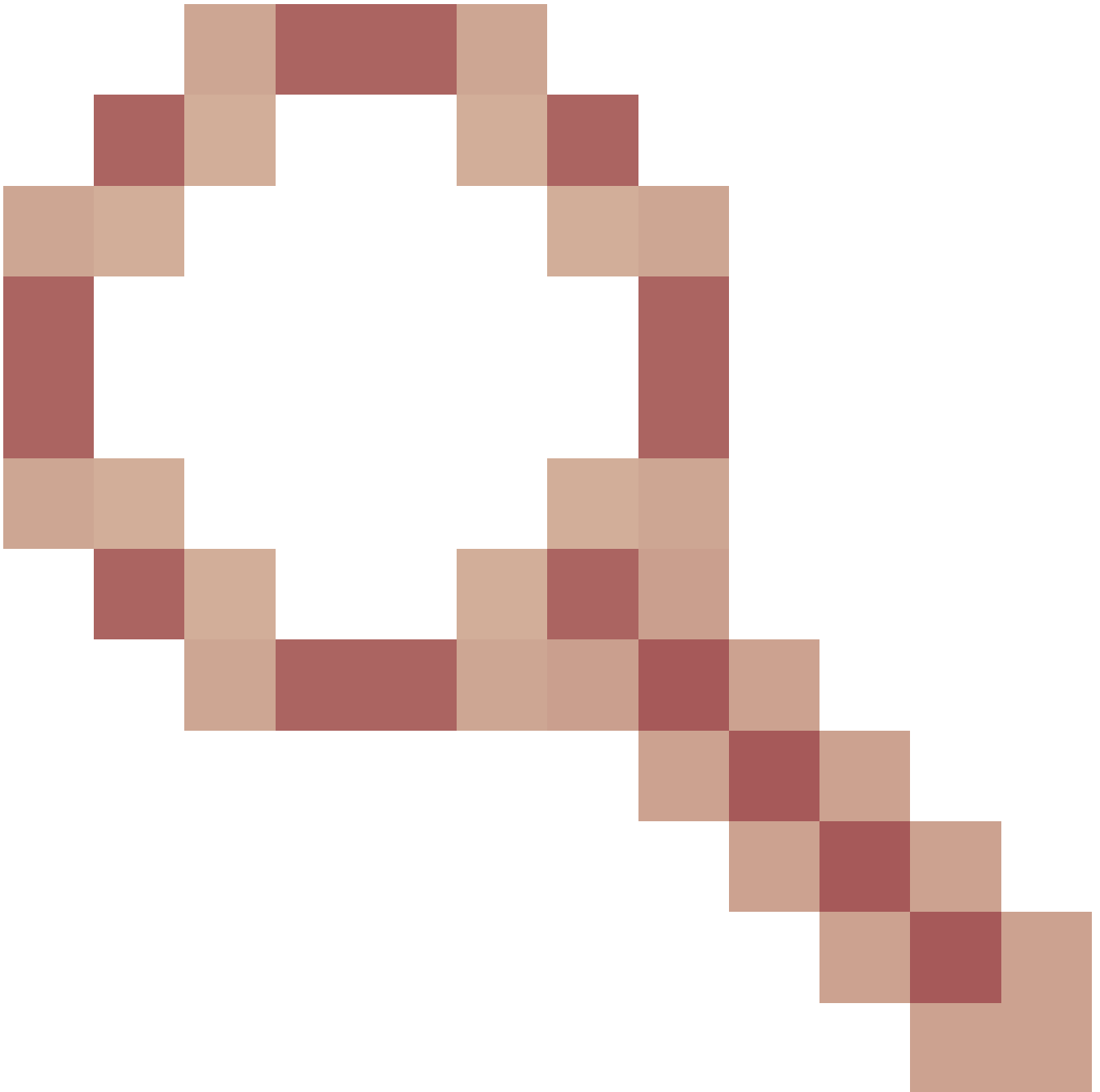
| | Ejemplo: | Descripción | Parámetros de muestra | MO de |
|--|----------|-------------|-----------------------|-------|
| | | | | |

| | | | | |
|------------------|---|--|--|--|
| | | | | muestra frente a qué fallos se generan |
| I2IngrPkts | I2IngrPkts5min I2IngrPkts15min I2IngrPkts1h etc... | Esto representa las estadísticas de paquetes de ingreso por VLAN durante cada período | dropRate floodRate multicastRate unicastRate | vlanCktEp (VLAN) |
| I2IngrPktsAg | I2IngrPktsAg15min I2IngrPktsAg1h I2IngrPktsAg1d etc... | Esto representa las estadísticas de paquetes de ingreso por EPG, BD, VRF, etc. Ej.) Las estadísticas de EPG representan la agregación de las estadísticas de VLAN que pertenecen al EPG | dropRate floodRate multicastRate unicastRate | fvAEPg (EPG) fvAp (perfil de aplicación) fvBD (BD) l3extOut (L3OUT) |
| eqptIngrDropPkts | eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d etc... | Esto representa las estadísticas de paquetes descartados de ingreso por interfaz durante cada período | *1 velocidad de reenvío Tasa de errores *1 *1 velocidad de búfer | l1PhysIf (puerto físico) pcAggrIf (canal de puerto) |

*1: Estos contadores en eqptIngrDropPkts pueden ser elevados falsamente debido a una limitación ASIC en varias plataformas Nexus 9000, porque los paquetes SUP_REDIRECT se registran como caídas de reenvío. Consulte también [CSCvo68407](#)



y [CSCvn72699](#)



para obtener más información y versiones fijas.

Tipos de contadores de caídas de hardware

En los switches Nexus 9000 que se ejecutan en modo ACI, hay 3 contadores de hardware principales para el motivo de caída de la interfaz de entrada en el ASIC.

Una `dropRate` en `I2IngrPkts`, `I2IngrPktsAg` incluye esos contadores. Tres parámetros (`forwardingRate`, `errorRate`, `bufferRate`) en la tabla anterior para `eqptIngrDropPkts` representan cada tres contadores de interfaz.

Reenvío

Las caídas de reenvío son paquetes que se descartan en el bloque LookUp (LU) del ASIC. En el bloque LU, se toma una decisión de reenvío de paquetes basada en la información del

encabezado del paquete. Si la decisión es descartar el paquete, se cuenta el descarte de reenvío. Hay una variedad de razones por las que esto puede suceder, pero hablemos de las Mayores:

SECURITY_GROUP_DENY

Una baja por falta de contratos para permitir la comunicación.

Cuando un paquete entra en el fabric, el switch observa el EPG de origen y de destino para ver si existe un contrato que permita esta comunicación. Si el origen y el destino están en diferentes EPG y no hay ningún contrato que permita este tipo de paquete entre ellos, el switch descartará el paquete y lo etiquetará como SECURITY_GROUP_DENY. Esto incrementa el contador de caídas directas.

VLAN_XLATE_MISS

Una caída debido a una VLAN inapropiada.

Cuando un paquete ingresa al entramado, el switch observa el paquete para determinar si la configuración en el puerto permite este paquete. Por ejemplo, una trama ingresa al entramado con una etiqueta 802.1Q de 10. Si el switch tiene VLAN 10 en el puerto, inspeccionará el contenido y tomará una decisión de reenvío basada en la MAC de destino. Sin embargo, si la VLAN 10 no está en el puerto, la descartará y la etiquetará como VLAN_XLATE_MISS. Esto incrementará el contador de descartes directos.

La razón de "XLATE" o "Translate" es que en ACI, el switch de hoja tomará una trama con una encapsulación 802.1Q y la traducirá a una nueva VLAN que se utilizará para VXLAN y otra normalización dentro del fabric. Si la trama ingresa con una VLAN no implementada, la "traducción" fallará.

ACL_DROP

Una caída debido a sup-tcam.

sup-tcam en los switches ACI contiene reglas especiales que se deben aplicar sobre la decisión de reenvío de L2/L3 normal. Las reglas de sup-tcam están integradas y el usuario no puede configurarlas. El objetivo de las reglas sup-tcam es principalmente gestionar algunas excepciones o parte del tráfico del plano de control y no está pensado para que lo comprueben o supervisen los usuarios. Cuando el paquete está alcanzando las reglas sup-tcam y la regla es descartar el paquete, el paquete descartado se cuenta como ACL_DROP y aumentará el contador de descarte de reenvío. Cuando esto ocurrió, generalmente significa que el paquete está a punto de ser reenviado contra las principales de reenvío de ACI básicas.

Tenga en cuenta que, aunque el nombre de destino sea ACL_DROP, esta "ACL" no es la misma que la lista de control de acceso normal que se puede configurar en

dispositivos NX-OS independientes o cualquier otro dispositivo de routing/switching.

SUP_REDIRECT

Esto no es una gota.

Un paquete sup redirigido (es decir, CDP/LLDP/UDLD/BFD, etc.) puede contarse como descarte directo aunque el paquete se procese correctamente y se reenvíe a la CPU.

Esto ocurre en las plataformas -EX, -FX y -FX2 como N9K-C93180YC-EX o N9K-C93180YC-FX. Estos no se deben contar como "descartes", sin embargo, es debido a la limitación ASIC en las plataformas -EX/-FX/-FX2.

Error

Cuando el switch recibe una trama no válida en una de las interfaces del panel frontal, se descarta como un error. Ejemplos de esto incluyen tramas con errores FCS o CRC. Al observar los puertos de hoja de link ascendente/descendente, o los puertos de columna, es mejor verificar los errores FCS/CRC usando "show interface".

Sin embargo, en las operaciones normales, se espera que los paquetes de error aumenten en los puertos de link ascendente/descendente de hojas o puertos de columna, ya que este contador también incluye tramas que son eliminadas por el sistema y no se espera que sean enviadas fuera de la interfaz.

Ejemplo: fallas TTL para paquetes enrutados, mismas tramas de transmisión/inundación de interfaz.

Buffer

Cuando el switch recibe una trama y no hay créditos de buffer disponibles para ingreso o egreso, la trama se descartará con "Buffer". Esto suele indicar congestión en algún punto de la red. El link que muestra la falla podría estar lleno o el link que contiene el destino podría estar congestionado.

Visualización de estadísticas de descarte en CLI

Objetos administrados

Secure Shell (SSH) a uno de los APIC y ejecute los siguientes comandos.

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

Esto proporcionará todas las instancias de objeto para esta clase l2IngrPktsAg15min.

Este es un ejemplo con un filtro para consultar un objeto específico. En este ejemplo, el filtro es mostrar solamente un objeto con los atributos dn que incluye "tn-TENANT1/ap-APP1/epg-EPG1" .

También este ejemplo utiliza egrep para mostrar solamente los atributos requeridos.

Ejemplo de salida 1: objeto de contador EPG (I2IngrPktsAg15min) del arrendatario TENANT1, perfil de aplicación APP1 , epg EPG1.

```
apic1# moquery -c I2IngrPktsAg15min -f 'I2.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 |

O podríamos utilizar otra opción -d en lugar de -c para obtener un objeto específico si conoce el dn del objeto.

Ejemplo de salida 2: objeto de contador EPG (I2IngrPktsAg15min) del arrendatario TENANT1, perfil de aplicación 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

Si observa fallas o desea verificar los paquetes descartados en los puertos de switch mediante la CLI, la mejor manera de hacerlo es ver los contadores de plataforma en el hardware. La mayoría de los contadores, pero no todos, se muestran mediante show interface. Las 3 razones principales de la caída solo se pueden ver usando los contadores de la plataforma. Para verlos, lleve a cabo estos pasos:

Hoja

SSH a la hoja y ejecute estos comandos.

```
ACI-LEAF# vsh_lc
module-1# show platform internal counters port <X>
* donde X representa el número de puerto
```

Ejemplo de salida 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 -----

Columna

Para una columna tipo caja (N9K-C9336PQ), es exactamente igual que Hoja.

Para las columnas modulares (N9K-C9504, etc.), primero debe adjuntar la tarjeta de línea concreta antes de poder ver los contadores de la plataforma. SSH a la columna y ejecute estos comandos

```
ACI-SPINE# vsh
```

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

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

* donde X representa el número de módulo de la tarjeta de línea que desea ver

Y representa el número de puerto

Ejemplo de salida para Ethernet 2/1:

```
<#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
```

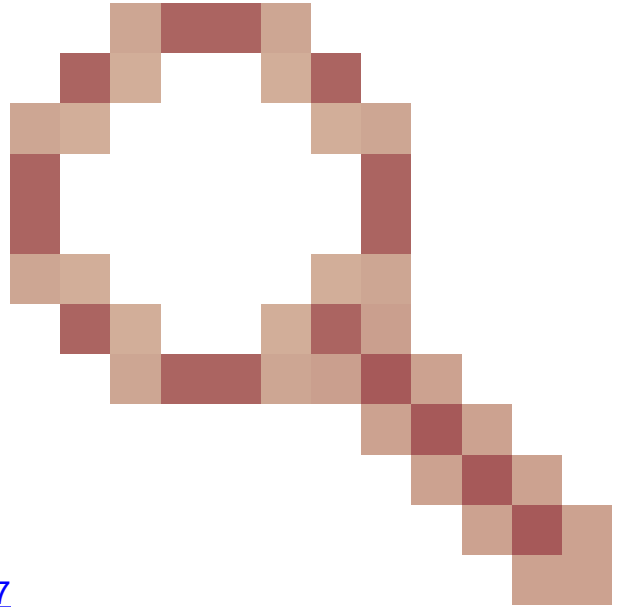
```
----- snip -----
```

Fallos

F112425 - velocidad de paquetes descartados de entrada
(`I2IngrPktsAg15min:dropRate`)

Descripción:

Una de las razones más comunes de este fallo es que los paquetes de la Capa 2 se descartan con la razón de "Descarte de reenvío". Hay una variedad de razones, pero la más común es:



En algunas plataformas (consulte [CSCvo68407](#)), existe una limitación en la que los paquetes L2 que necesitan ser redirigidos a la CPU (es decir, CDP/LLDP/UDLD/BFD, etc.), se registran como una "caída directa" y se copian en la CPU. Esto se debe a una limitación del ASIC utilizado en estos modelos.

Resolución:

Las caídas descritas anteriormente son puramente cosméticas, por lo que la recomendación de la práctica recomendada es aumentar el umbral para la falla, como se muestra en la sección Umbral de estadísticas. Para hacer esto, vea las instrucciones en el Umbral de estadísticas.

F100264 - velocidad de paquetes descartados del búfer de entrada (eqptIngrDropPkts5min:bufferRate)

Descripción:

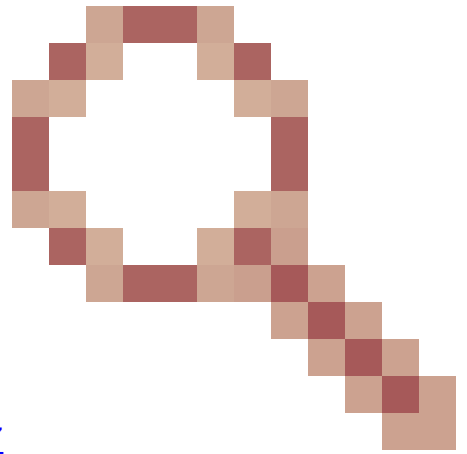
Este fallo puede aumentar cuando los paquetes se descartan en un puerto con la razón "Buffer" Como se mencionó anteriormente, esto sucede típicamente cuando hay congestión en una interfaz en la dirección de ingreso o egreso.

Resolución:

Este fallo representa los paquetes perdidos reales en el entorno debido a la congestión. Los paquetes perdidos pueden causar problemas con las aplicaciones que se ejecutan en el fabric de ACI. Los administradores de red deben aislar el flujo de paquetes y determinar si la congestión se debe a flujos de tráfico inesperados, equilibrio de carga ineficiente, etc., o a una utilización esperada en esos puertos.

F100696 - paquetes descartados de reenvío de entrada (eqptIngrDropPkts5min:forwardingRate)

 Nota: una limitación ASIC como la mencionada anteriormente para F11245 puede causar



que estos fallos también se planteen. Consulte [CSCvo68407](#) para obtener más información.

Este fallo se debe a unos pocos escenarios. El más común es:

Descripción 1) Caídas de columna vertebral

Si se observa este fallo en una interfaz de columna, podría deberse al tráfico hacia un terminal desconocido.

Cuando un paquete ARP o IP se reenvía a la columna para una búsqueda de proxy y el terminal es desconocido en el entramado, se generará un paquete de captura especial y se enviará a todas las hojas en la dirección de grupo de multidifusión BD (interna) apropiada. Esto activará una solicitud ARP de cada hoja del dominio de puente (BD) para detectar el punto final. Debido a una limitación, el paquete de recolección recibido por la hoja también se refleja de nuevo en el entramado nuevamente y activa una caída de reenvío en el link de columna conectado a la hoja. En este escenario, el descarte directo solo se incrementa en el hardware de columna de primera generación.

Resolución 1)

Dado que se sabe que el problema se debe a que un dispositivo envía una cantidad innecesaria de tráfico unidifusión desconocido al fabric de ACI, es necesario averiguar qué dispositivo está causando esto y ver si se puede evitar. Esto suele deberse a dispositivos que analizan o sondean las direcciones IP de las subredes con fines de supervisión. Para encontrar qué IP está enviando este tráfico, SSH en la hoja que está conectada a la interfaz de columna que muestra la falla.

Desde ahí, puede ejecutar este comando para ver la dirección IP de origen (sip) que está activando el paquete de captura:

```
<#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.
```

En este ejemplo de salida, el paquete de recolección es activado por 192.168.21.150 y se recomienda ver si esto se puede mitigar.

Descripción 2) Gotas de hojas

Si se observa este error en una interfaz de hoja, la causa más probable se debe a las caídas de SECURITY_GROUP_DENY mencionadas.

Resolución 2)

La hoja de ACI mantiene un registro de los paquetes denegados debido a violaciones de contratos. Este registro no los captura todos para proteger los recursos de la CPU, pero aún así le proporciona una gran cantidad de registros.

Para obtener los registros requeridos, si la interfaz en la que se ha producido el fallo es parte de un canal de puerto, es necesario utilizar este comando y grep para el canal de puerto. De lo contrario, la interfaz física puede ser gobernada.

Este registro se puede revertir rápidamente en función de la cantidad de caídas de contratos.

```
<#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
```

En este caso, 192.168.21.150 está intentando enviar mensajes ICMP (número de protocolo IP 1) a 192.168.20.3. Sin embargo, no hay ningún contrato entre los 2 EPG que permita ICMP, por lo que el paquete se descarta. Si se supone que ICMP está permitido,

se puede agregar un contrato entre los dos EPG.

Umbral de estadísticas

En esta sección se describe cómo cambiar un umbral para objetos de estadísticas que podrían generar un error en un contador de caídas.

Un umbral para las estadísticas de cada objeto (es decir, l2IngrPkts, eqptIngrDropPkts) se configura a través de la política de monitoreo contra una variedad de objetos.

Como se menciona en la tabla al principio, eqptIngrDropPkts se monitorea bajo, por ejemplo, los objetos l1Physlf a través de la política de monitoreo.

Velocidad de paquetes descartados de reenvío en eqptIngrDropPkts

Hay dos porciones para esto.

- + Políticas de acceso (puertos hacia dispositivos externos, también conocidos como puertos del panel frontal)

- + Políticas de fabric (puertos entre los puertos de fabric LEAF y SPINE, también conocidos como puertos de fabric)

Front Panel Ports (ports towards external devices)



Fabric Ports (ports between LEAF and SPINE)



A cada objeto de puerto (l1Physlf, pcAggrlf) se le podría asignar su propia política de monitoreo a través del grupo de políticas de interfaz, como se muestra en la imagen anterior.

De forma predeterminada, hay una política de supervisión predeterminada tanto en Fabric > Access Policies como en Fabric > Fabric Policies en la GUI de APIC. Estas políticas de monitoreo predeterminadas se asignan a todos los puertos respectivamente. La política de supervisión predeterminada en Políticas de acceso es para puertos del panel frontal y la

política de supervisión predeterminada en Políticas de fabric es para puertos de fabric.

A menos que sea necesario cambiar los umbrales por puerto, la política de monitoreo predeterminada en cada sección se puede modificar directamente para aplicar el cambio en todos los puertos del panel frontal y/o puertos de entramado.

El ejemplo siguiente se utiliza para cambiar los umbrales de descarte directo en eqptIngrDropPkts en los puertos de fabric (políticas de fabric). Realice lo mismo en Fabric > Access Policies para los puertos del panel frontal.

1. Vaya a Fabric >Políticas de Fabric>Políticas de supervisión.

2. Haga clic con el botón derecho y seleccione "Crear política de supervisión".

(Si el cambio de umbral se puede aplicar a todos los puertos de fabric, navegue hasta default en lugar de crear uno nuevo)

3. Expanda la nueva política de supervisión o la predeterminada y acceda a Políticas de recopilación de estadísticas.

4. Haga clic en el icono del lápiz para el Objeto de Monitoreo en el panel derecho, seleccione Configuración de la Interfaz Física de Capa 1 (I1.PhysIf).

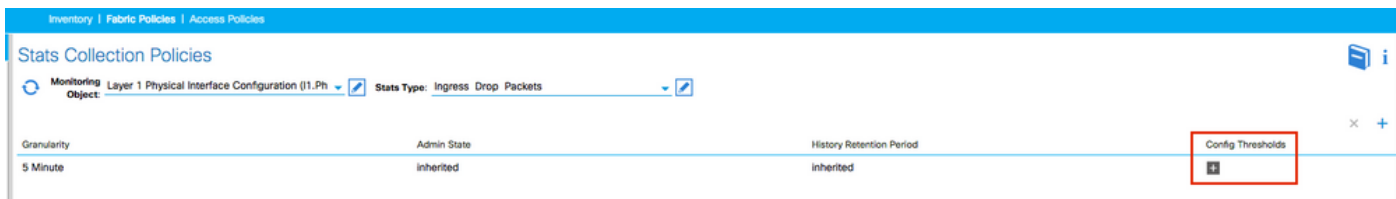
(Este paso 4 se puede omitir cuando se utiliza la política predeterminada)

5. En la lista desplegable Objeto de Control del panel derecho, seleccione Configuración de la Interfaz Física de Capa 1 (I1.PhysIf) y Tipo de Estado, elija Paquetes de Borrado de Entrada

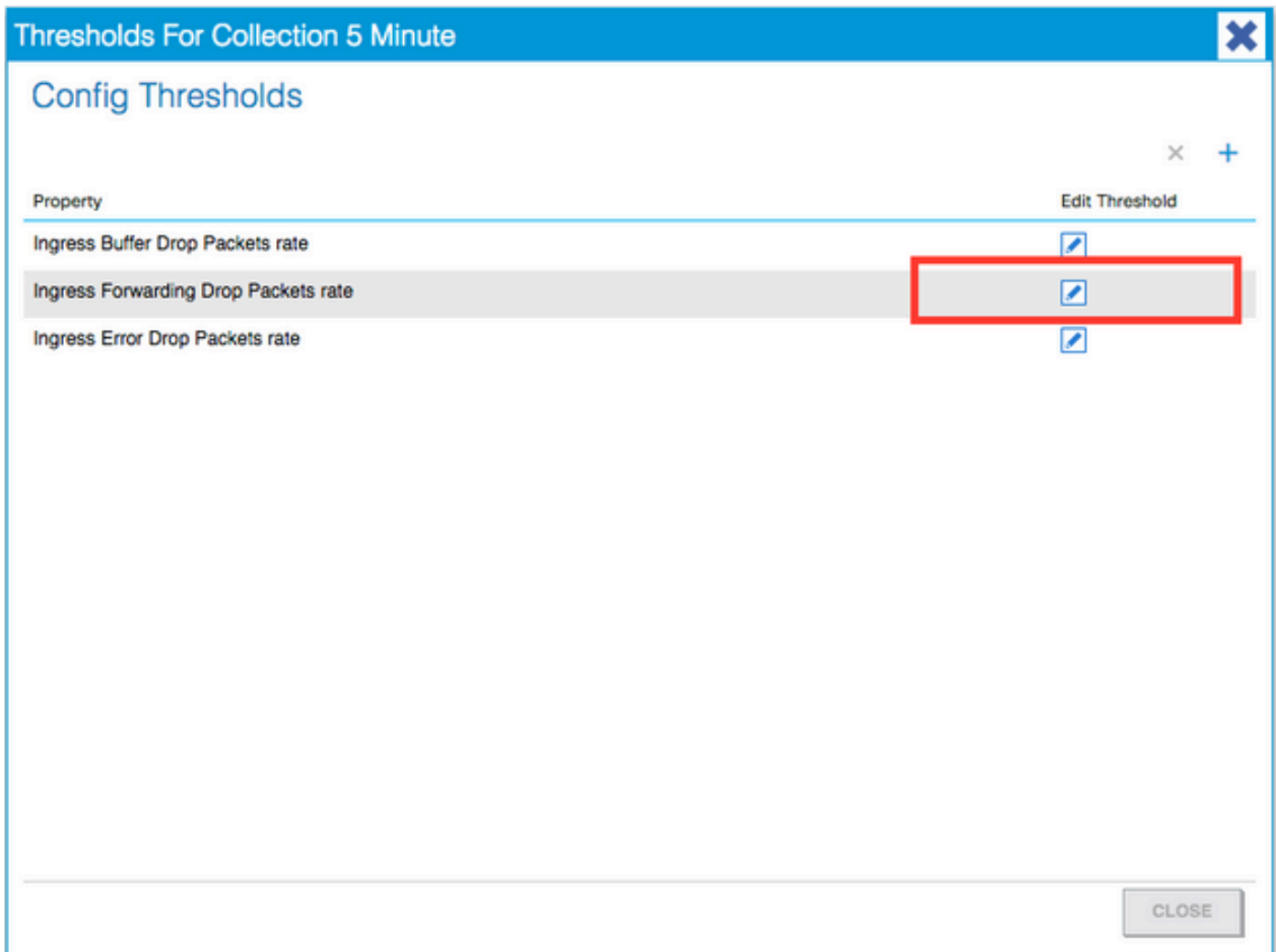
The screenshot shows the Cisco Fabric Policy configuration interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'VM Networking', 'L4-L7 Services', 'Admin', and 'Operations'. The breadcrumb trail is 'Inventory | Fabric Policies | Access Policies'. The left sidebar shows a tree view of policies, with 'Stats Collection Policies' selected. The main content area is titled 'Stats Collection Policies' and contains the following configuration:

| | | | |
|--------------------|---|-------------|----------------------|
| Monitoring Object: | Layer 1 Physical Interface Configuration (I1.Ph | Stats Type: | Ingress Drop Packets |
| Granularity | Admin State | | |
| 5 Minute | inherited | | |

6. Haga clic en el botón + junto a Umbrales de configuración



7. Edite el umbral para el desvío de reenvío



8. Se recomienda desactivar los umbrales de subida para configurar la velocidad de bajada de reenvío crítica, principal, secundaria y de advertencia.

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 | ⬆️⬇️⬆️ |

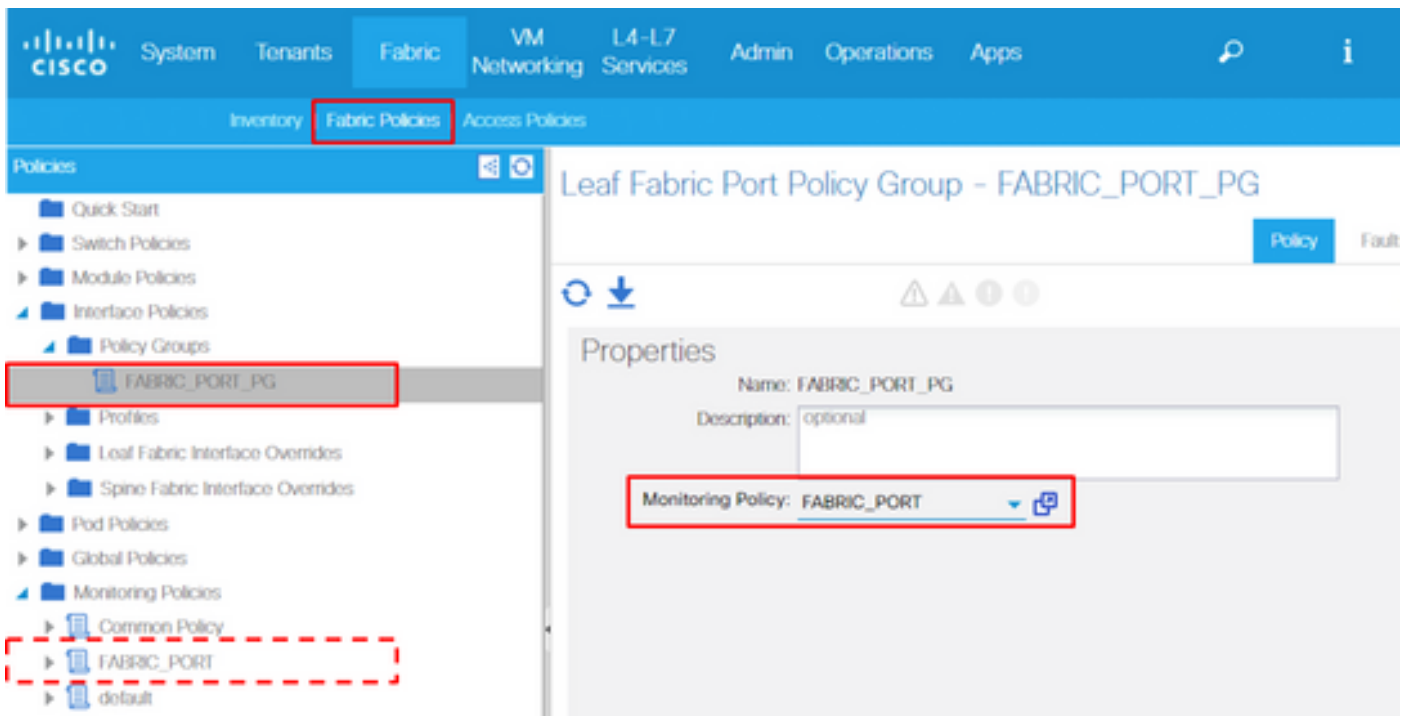
Falling

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

SUBMIT
CANCEL

9. Aplique esta nueva política de supervisión al grupo de políticas de interfaz para los puertos necesarios. No olvide configurar el perfil de interfaz, el perfil del switch, etc. en las políticas de fabric según corresponda.

(Este paso 9 se puede omitir cuando se utiliza la política predeterminada)



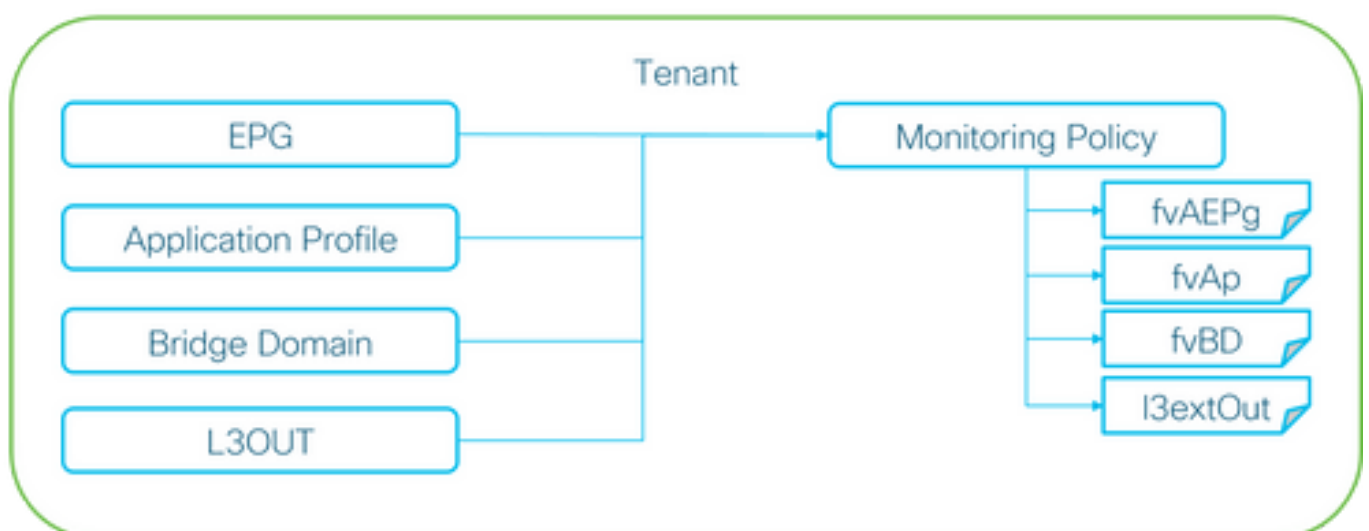
10. Si se trata de puertos del panel frontal (políticas de acceso), realice lo mismo para la interfaz agregada (pc.AggrIf) que para la configuración de la interfaz física de capa 1 (I1.PhysIf), de modo que esta nueva política de supervisión se pueda aplicar al canal de puerto y al puerto físico.

(Este paso 10 se puede omitir cuando se utiliza la política predeterminada)

Tasa de paquetes descartados de entrada en I2IngrPktsAg

Hay varias partes para esto.

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 se muestra en la imagen anterior, I2IngrPktsAg se monitorea bajo muchos objetos. La

imagen superior sólo muestra algunos ejemplos, pero no todos los objetos para I2IngrPktsAg. Sin embargo, el umbral para las estadísticas se configura a través de la política de monitoreo, así como eqptIngrDropPkts bajo I1PhysIf o pcAggrIf.

A cada objeto (EPG(fvAEPg), Bridge Domain(fvBD), etc...) se le podría asignar su propia política de supervisión, como se muestra en la imagen anterior.

De forma predeterminada, todos estos objetos bajo el arrendatario utilizan la política de monitoreo predeterminada bajo Arrendatario > Común > Políticas de monitoreo > predeterminada a menos que se configure de otra manera.

A menos que sea necesario cambiar los umbrales por cada componente, la política de monitoreo predeterminada bajo el arrendatario común se puede modificar directamente para aplicar el cambio para todos los componentes relacionados.

El siguiente ejemplo es para cambiar los umbrales para la velocidad de paquetes descartados de entrada en I2IngrPktsAg15min en el dominio de puente.

1. Vaya a Arrendatario > (nombre del arrendatario) > Políticas de supervisión.

(el arrendatario debe ser común si se utiliza la política de supervisión predeterminada o si la nueva política de supervisión debe aplicarse a todos los arrendatarios)

2. Haga clic con el botón derecho y seleccione "Crear política de supervisión".

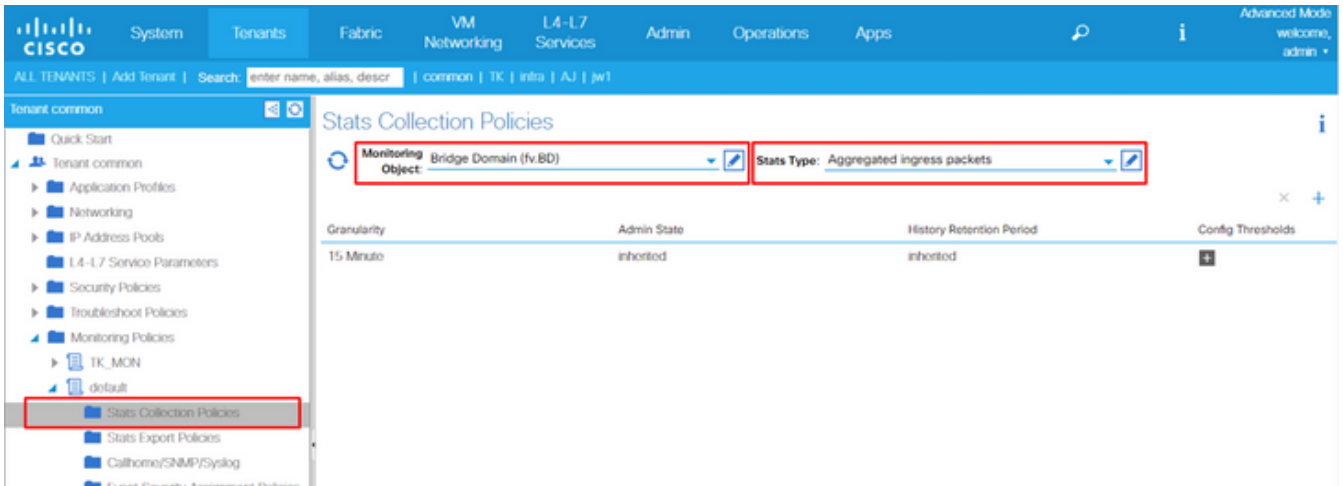
(Si el cambio de umbral se puede aplicar a todos los componentes, navegue hasta default en lugar de crear uno nuevo)

3. Expanda la nueva política de supervisión o la predeterminada y acceda a Políticas de recopilación de estadísticas.

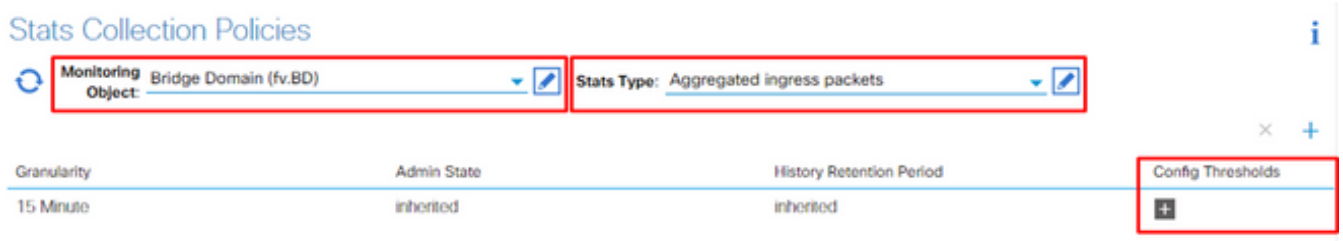
4. Haga clic en el icono del lápiz para el Objeto de Monitoreo en el panel derecho, seleccione Dominio de Bridge (fv.BD).

(Este paso 4 se puede omitir cuando se utiliza la política predeterminada)

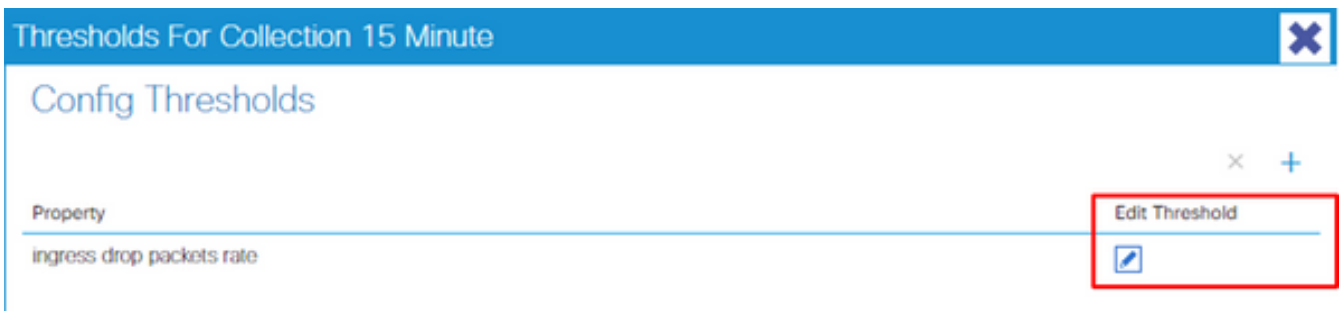
5. En el menú desplegable Monitoring Object del panel derecho, seleccione Bridge Domain (fv.BD) y Stats Type, elija Aggregated ingress packets.



6. Haga clic en el botón + junto a Umbrales de configuración



7. Edite el umbral para el desvío de reenvío



8. Se recomienda desactivar los umbrales de subida para configurar la velocidad de bajada de reenvío crítica, principal, secundaria y de advertencia.

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 nueva directiva de supervisión al dominio de puente que requiere un cambio de umbral.

(Este paso 9 se puede omitir cuando se utiliza la política predeterminada)

The screenshot shows the Cisco DNA Center interface for configuring a Bridge Domain (BD1). The left sidebar shows the navigation tree with 'Bridge Domains' expanded to 'BD1'. The main content area shows the 'Policy' tab for 'Bridge Domain - BD1'. A red box highlights the 'Monitoring Policy' dropdown menu, which is currently set to 'TK_MON'. 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'.

NOTA

La política de monitoreo no predeterminada puede no tener configuraciones que estén presentes en la política de monitoreo predeterminada. Si es necesario mantener la misma

 configuración que la política de monitoreo predeterminada, los usuarios deben verificar la configuración de la política de monitoreo predeterminada y configurar manualmente las mismas políticas en la política de monitoreo no predeterminada.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).