

Spiegazione degli errori di perdita del pacchetto in ACI

Sommario

[Introduzione](#)

[Oggetti gestiti](#)

[Tipi di contatori di rilascio hardware](#)

[Avanti](#)

[Errore](#)

[Buffer](#)

[Visualizzazione dello stato di eliminazione nella CLI](#)

[Oggetti gestiti](#)

[Contatori hardware](#)

[Foglia](#)

[Dorso](#)

[Errori](#)

[F112425 - Frequenza pacchetti in entrata scartati \(I2IngrPktsAg15min:dropRate\)](#)

[F100264 - Frequenza pacchetti in ingresso ignorati da buffer \(eqptIngrDropPkts5min:bufferRate\)](#)

[F100696 - Pacchetti in entrata rilasciati inoltra \(eqptIngrDropPkts5min:forwardingRate\)](#)

[Soglia statistiche](#)

[Frequenza pacchetti forward-drop in eqptIngrDropPkts](#)

[Frequenza pacchetti in ingresso ignorati in I2IngrPktsAg](#)

Introduzione

Questo documento descrive ciascun tipo di errore e la procedura da seguire quando viene visualizzato l'errore. Durante il normale funzionamento di un'infrastruttura ACI (Cisco Application Centric Infrastructure), l'amministratore può visualizzare gli errori per alcuni tipi di perdite di pacchetti.

Oggetti gestiti

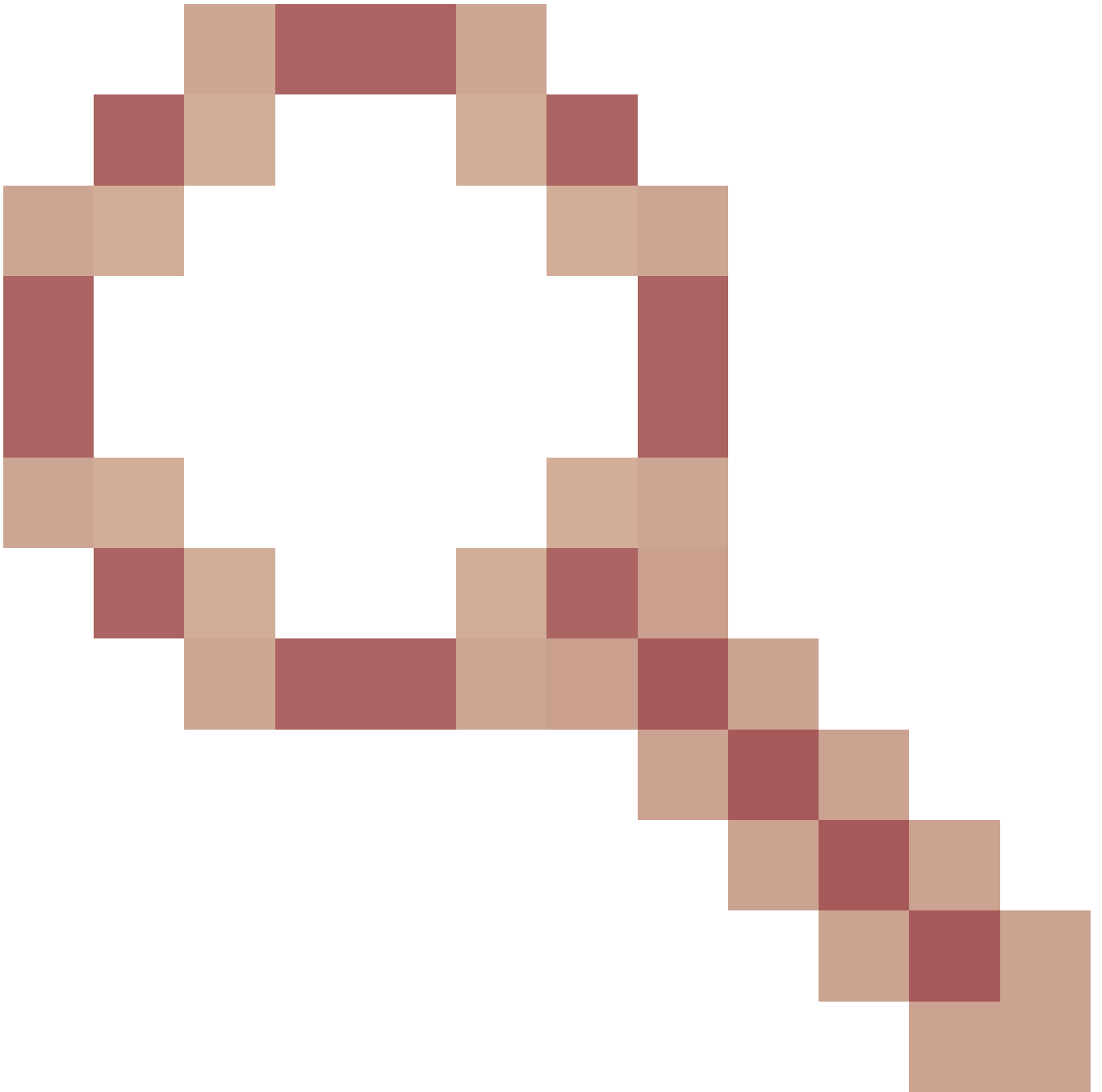
In Cisco ACI, tutti gli errori vengono generati in Oggetti gestiti (MO). Ad esempio, un errore F11245 - Incoming Drop Packets rate (I2IngrPktsAg15min:dropRate) riguarda il parametro dropRate in MO I2IngrPktsAg15min.

In questa sezione vengono illustrati alcuni degli oggetti gestiti di esempio relativi agli errori dei pacchetti di destinazione.

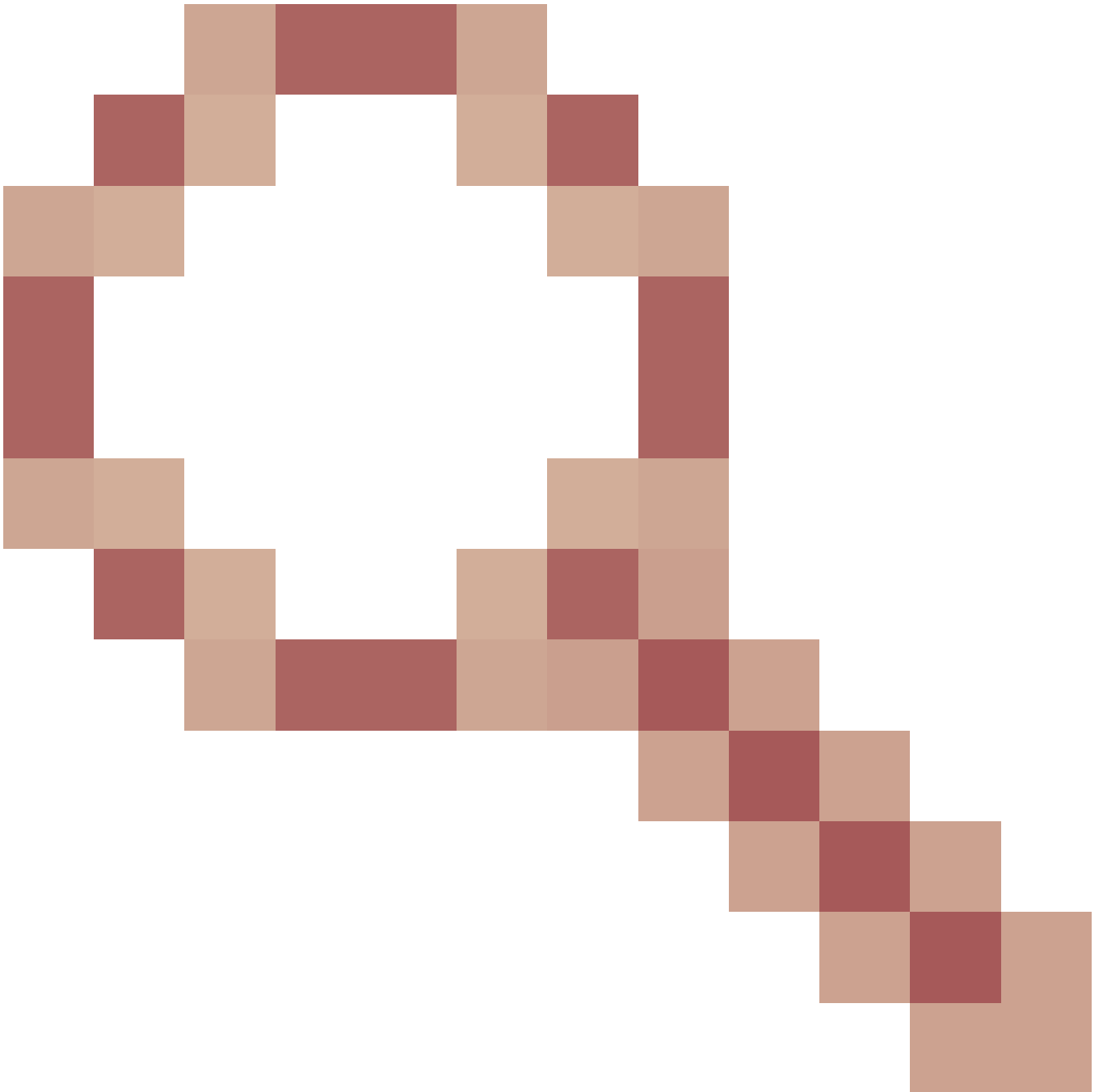
	Esempio	Descrizione	Parametri di esempio	Esempio di

				MO contro quali errori vengono generati
I2IngrPkts	I2IngrPkts5min I2IngrPkts15 min I2IngrPkts1h e così via.	Questo valore rappresenta le statistiche dei pacchetti in entrata per VLAN durante ciascun periodo.	dropRate FrequenzaInondazioni Multicast Rate velocitàunicast	vlanCktEp (VLAN)
L2IngrPktsAg	I2IngrPktsAg15 min I2IngrPktsAg1h I2IngrPktsAg1d e così via.	Questo valore rappresenta le statistiche dei pacchetti in entrata per EPG, BD, VRF e così via. Ad esempio, le statistiche EPG rappresentano l'aggregazione delle statistiche VLAN che appartengono all'EPG.	dropRate FrequenzaInondazioni Multicast Rate velocitàunicast	fvAEPg (EPG) fvAp (Profilo applicazione) fvBD (BD) l3extOut (L3OUT)
PacchettiIngrDropAcq	eqptIngrDropPkts15 min. EqptIngrDropPkts1h EqptIngrDropPkts1d e così via.	Questo valore rappresenta le statistiche dei pacchetti in entrata ignorati per interfaccia durante ciascun periodo.	*1 velocità di inoltro *1 velocità di errore *1 velocità buffer	l1PhysIf (porta fisica) pcAggrIf (canale porta)

*1 : questi contatori in eqptIngrDropPkts possono essere alzati erroneamente a causa di un limite ASIC in diverse piattaforme Nexus 9000, perché i pacchetti SUP_REDIRECT vengono registrati come cadute in avanti. Per ulteriori informazioni e per le versioni corrette, vedere anche l'ID bug Cisco [CSCvo68407](https://www.cisco.com/c/en-us/bugtools/bugtools/bugtools.html?bugid=CSCvo68407)



e l'ID bug Cisco [CSCvn72699](#)



Tipi di contatori di rilascio hardware

Sugli switch Nexus 9000 in modalità ACI, sono disponibili tre contatori hardware principali per il motivo della perdita di interfacce in entrata sull'ASIC.

Un dropRate in I2IngrPkts, I2IngrPktsAg include questi contatori. Tre parametri (forwardingRate, errorRate, bufferRate) nella tabella per eqptIngrDropPkts rappresentano ogni tre contatori di interfaccia.

Avanti

Le gocce di inoltro sono pacchetti che vengono scartati nel blocco di ricerca (LU, LookUp Block) dell'ASIC. Nel blocco LU, la decisione di inoltro del pacchetto viene presa in base alle

informazioni dell'intestazione del pacchetto. Se si decide di scartare il pacchetto, viene conteggiato il pacchetto Forward Drop. Questo può accadere per svariate ragioni, ma parliamo anche delle più importanti:

SECURITY_GROUP_DENY

Un calo dovuto a contratti mancanti per permettere la comunicazione.

Quando un pacchetto entra nell'infrastruttura, lo switch controlla l'EPG di origine e di destinazione per verificare se esiste un contratto che consente questa comunicazione. Se l'origine e la destinazione si trovano in EPG diversi e non è presente alcun contratto che consenta l'uso di questo tipo di pacchetto, lo switch scarta il pacchetto e lo etichetta come SECURITY_GROUP_DENY. In questo modo si incrementa il contatore Forward Drop.

Mancato completamento di VLAN_XLATE

Caduta a causa di VLAN non appropriata.

Quando un pacchetto entra nella struttura, lo switch lo controlla per determinare se la configurazione sulla porta lo consente. Ad esempio, un frame entra nel fabric con un tag 802.1Q di 10. Se lo switch ha la VLAN 10 sulla porta, controlla i contenuti e prende una decisione di inoltrare in base all'indirizzo MAC di destinazione. Tuttavia, se la VLAN 10 non è presente sulla porta, la elimina e la assegna come VLAN_XLATE_MISS. In questo modo si incrementa il contatore Forward Drop.

Il motivo per cui è stato scelto XLATE o Translate è che in ACI, lo switch foglia prende un frame con un'interfaccia 802.1Q e lo converte in una nuova VLAN usata per la VXLAN e per altre operazioni di normalizzazione all'interno della struttura. Se il frame viene fornito con una VLAN non distribuita, la conversione non riesce.

ACL_DROP

Una goccia a causa di sup-tcam.

sup-tcam negli switch ACI contiene regole speciali da applicare prima della normale decisione di inoltrare L2/L3. Le regole in sup-tcam sono incorporate e non configurabili dall'utente. L'obiettivo delle regole sup-tcam è principalmente quello di gestire alcune eccezioni o parte del traffico del control plane e non deve essere controllato o monitorato dagli utenti. Quando un pacchetto incontra le regole sup-tcam e la regola è di scartare il pacchetto, il pacchetto scartato viene contato come ACL_DROP e incrementa il contatore Forward Drop. Quando si verifica questa situazione, in genere il pacchetto sta per essere inoltrato rispetto alle entità di inoltrare ACI di base.

Anche se il nome di rilascio è ACL_DROP, questo ACL non è lo stesso del normale Access Control List, che può essere configurato su dispositivi NX-OS standalone o su qualsiasi altro dispositivo di routing/switching.

SUP_REINDIRIZZA

Questa non è una goccia.

Un pacchetto reindirizzato sup (ad esempio, CDP/LLDP/UDLD/BFD e così via) può essere conteggiato come Forward Drop anche se il pacchetto è elaborato correttamente e inoltrato alla CPU.

Questo si verifica nelle piattaforme -EX, -FX e -FX2, ad esempio N9K-C93180YC-EX o N9K-C93180YC-FX. Questi non possono essere conteggiati come drop, tuttavia, è a causa della limitazione ASIC nelle piattaforme -EX/-FX/-FX2.

Errore

Quando lo switch riceve un frame non valido su una delle interfacce del pannello anteriore, viene scartato come errore. Ad esempio, i frame con errori FCS o CRC. Se si utilizzano le porte foglia Uplink/Downlink o le porte Spine, è consigliabile verificare la presenza di errori FCS/CRC tramite il comando `show interface`. Tuttavia, in condizioni operative normali, si prevede che i pacchetti di errore aumentino sulle porte Uplink/Downlinks di foglie, o porte Spine, in quanto questo contatore include anche i frame che sono eliminati dal sistema e che non si prevede vengano inviati fuori dall'interfaccia.

Esempio: errori TTL per pacchetti instradati, stesso frame di broadcast/flooded dell'interfaccia.

Buffer

Quando lo switch riceve un frame e non sono disponibili crediti buffer per l'ingresso o l'uscita, il frame viene scartato con il buffer. Ciò suggerisce che in qualche punto della rete vi è congestione. Il collegamento che mostra l'errore potrebbe essere pieno oppure il collegamento contenente la destinazione potrebbe essere congestionato.

Visualizzazione dello stato di eliminazione nella CLI

Oggetti gestiti

Collegare Secure Shell (SSH) a uno degli APIC ed eseguire questi comandi.

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

Fornisce tutte le istanze di oggetto per questa classe `l2IngrPktsAg15min`.

Di seguito è riportato un esempio con un filtro per eseguire una query su un oggetto specifico. In questo esempio, il filtro consente di visualizzare solo un oggetto con attributi `dn` che include `tn-TENANT1/ap-APP1/epg-EPG1`.

In questo esempio viene inoltre utilizzato `egrep` per visualizzare solo gli attributi obbligatori.

Output di esempio 1 : oggetto contatore EPG (l2IngrPktsAg15min) di TENANT1, profilo applicazione APP1 , epg EPG1.

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

Oppure possiamo usare un'altra opzione -d invece di -c per ottenere un oggetto specifico, se conoscete il dn dell'oggetto.

Output di esempio 2 : oggetto contatore EPG (l2IngrPktsAg15min) di TENANT1, profilo applicazione 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
```

Contatori hardware

Se si verificano errori o si desidera controllare le perdite di pacchetti sulle porte degli switch dalla CLI, il modo migliore per farlo è visualizzare i contatori della piattaforma nell'hardware. La maggior parte dei contatori, ma non tutti, vengono visualizzati tramite il comando show interface. I 3 principali motivi di perdita possono essere visualizzati solo utilizzando i contatori della piattaforma. Per visualizzarli, effettuare le seguenti operazioni:

Foglia

SSH sulla foglia ed eseguire questi comandi.

```
ACI-LEAF# vsh_lc
module-1# show platform internal counters port <X>
                * dove X rappresenta il numero della porta
```

Output di esempio per 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 -----

Dorso

Per un box type spine (N9K-C9336PQ), è esattamente uguale a Leaf.

Per i dorsi modulari (N9K-C9504 e così via), è necessario collegare la scheda di linea specifica prima di poter visualizzare i contatori della piattaforma. SSH sul dorso ed eseguire questi comandi:

```
ACI-SPINE# vsh
```

```
ACI-SPINE# modulo di collegamento <X>
```

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

* dove X rappresenta il numero del modulo per la scheda di linea che si desidera visualizzare

Y rappresenta il numero di porta

Output di esempio per 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 -----				

Errori

F112425 - Frequenza pacchetti in entrata scartati (l2IngrPktsAg15min:dropRate)

Descrizione:

Una delle ragioni più comuni di questo errore è che i pacchetti di layer 2 vengono scartati con il motivo del Forward Drop. Le ragioni sono molteplici, ma la più comune è:

In alcune piattaforme (vedere l'ID bug Cisco [CSCvo68407](#)), è previsto un limite per il reindirizzamento dei pacchetti L2 alla CPU (ad esempio, CDP/LLDP/UDLD/BFD e così via), la registrazione come forward-drop e la copia sulla CPU. Ciò è dovuto a una

limitazione dell'ASIC utilizzato in questi modelli.

Risoluzione:

Le gocce descritte sono puramente cosmetiche, pertanto la procedura consigliata consiste nell'aumentare la soglia per l'errore, come mostrato nella sezione Soglia statistiche. A tale scopo, vedere le istruzioni in Soglia stati.

F100264 - Frequenza pacchetti in ingresso ignorati da buffer (eqptIngrDropPkts5min:bufferRate)

Descrizione:

L'errore può aumentare quando i pacchetti vengono scartati su una porta con un motivo buffer. Come accennato in precedenza, ciò si verifica in genere quando sull'interfaccia è presente una congestione in entrata o in uscita.

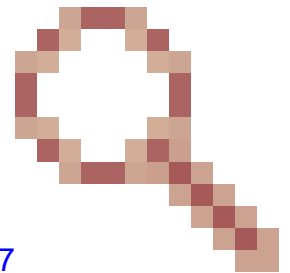
Risoluzione:

Questo errore rappresenta i pacchetti effettivamente scartati nell'ambiente a causa della congestione. I pacchetti ignorati possono causare problemi con le applicazioni in esecuzione nell'infrastruttura ACI. Gli amministratori di rete possono isolare il flusso del pacchetto e determinare se la congestione è dovuta a flussi di traffico imprevisti, bilanciamento del carico inefficiente e così via, o all'utilizzo previsto su tali porte.

F100696 - Pacchetti in entrata rilasciati inoltrati (eqptIngrDropPkts5min:forwardingRate)

 Nota: un limite ASIC come indicato in precedenza per F11245 può causare l'innalzamento di

questi errori. Per ulteriori informazioni, vedere l'ID bug Cisco [CSCvo68407](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvo68407)



L'errore è causato da alcuni scenari. La più comune è:

Descrizione 1) Gocce di colonna

Se l'errore viene rilevato su un'interfaccia Spine, potrebbe essere dovuto al traffico verso un endpoint sconosciuto. Quando un pacchetto ARP o IP viene inoltrato al dorso per una ricerca proxy e l'endpoint non è noto nell'infrastruttura, viene generato un pacchetto speciale di tipo Glean che viene inviato a tutte le foglie sull'indirizzo di gruppo multicast BD (interno) appropriato. In questo modo viene attivata una richiesta ARP da ogni foglia

nel dominio di Bridge (BD) per individuare l'endpoint. A causa di un limite, il pacchetto di glean ricevuto dalla foglia viene riflesso nuovamente nel tessuto e innesca una goccia di inoltro sul collegamento dorso collegato alla foglia. La riduzione in avanti in questo scenario viene incrementata solo su hardware dorso di generazione 1.

Risoluzione 1)

Poiché è noto che il problema è causato da un dispositivo che invia una quantità non necessaria di traffico Unicast sconosciuto all'infrastruttura ACI, è necessario individuare il dispositivo che causa il problema e verificare se è possibile prevenirlo. Questo problema è in genere causato da dispositivi che eseguono la scansione o la ricerca di indirizzi IP nelle subnet a scopo di monitoraggio. Per conoscere l'indirizzo IP con cui viene inviato il traffico, controllare il protocollo SSH sulla foglia collegata all'interfaccia della spine e verificare la presenza del guasto.

A questo punto, è possibile eseguire questo comando per visualizzare l'indirizzo IP di origine (sip) che attiva il pacchetto pulito:

```
<#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.
```

Nell'output di questo esempio, il pacchetto verde viene attivato entro 192.168.21.150 e si consiglia di verificare se questa condizione può essere mitigata.

Descrizione 2) Gocce di foglia

Se l'errore si verifica su un'interfaccia foglia, la causa più probabile è dovuta alle perdite di SECURITY_GROUP_DENY indicate.

Risoluzione 2)

ACI leaf tiene un registro dei pacchetti rifiutati a causa di violazioni. Questo log non ne acquisisce tutti per proteggere le risorse della CPU, ma fornisce comunque una grande quantità di log.

Per ottenere i log richiesti, se l'interfaccia su cui è stato generato l'errore fa parte di un

canale porta, è necessario utilizzare questo comando e grep per il canale porta. In caso contrario, l'interfaccia fisica può essere saltata.

È possibile eseguire rapidamente il rollover di questo log a seconda della quantità di perdite di contratto.

```
<#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
```

In questo caso, la versione 192.168.21.150 sta tentando di inviare messaggi ICMP (numero di protocollo IP 1) alla versione 192.168.20.3. Tuttavia, non esiste alcun contratto tra i 2 EPG che consenta l'ICMP, quindi il pacchetto viene scartato. Se si suppone che sia consentito l'ICMP, è possibile aggiungere un contratto tra i due EPG.

Soglia statistiche

In questa sezione viene descritto come modificare una soglia per un oggetto di statistiche che potrebbe generare un errore durante il contatore di rilascio.

Una soglia per le statistiche di ogni oggetto (ad esempio, l2IngrPkts, eqptIngrDropPkts) viene configurata tramite Criteri di monitoraggio su diversi oggetti.

Come indicato nella tabella all'inizio, eqptIngrDropPkts viene monitorato, ad esempio, in oggetti l1PhysIf tramite Criteri di monitoraggio.

Frequenza pacchetti forward-drop in eqptIngrDropPkts

Ci sono due parti per questo.

- + Criteri di accesso (porte verso dispositivi esterni, dette anche porte del pannello anteriore)

- + Fabric Policies (porte tra le porte FOGLIA e SPINE. alias fabric)

Front Panel Ports (ports towards external devices)



Fabric Ports (ports between LEAF and SPINE)



A ogni oggetto porta (l1Physlf, pcAggrlf) è possibile assegnare un criterio di monitoraggio specifico tramite il gruppo di criteri di interfaccia, come illustrato nella figura precedente.

Per impostazione predefinita, esiste un criterio di monitoraggio predefinito sia in Fabric > Criteri di accesso che in Fabric > Criteri fabric nella GUI APIC. Questi criteri di monitoraggio predefiniti vengono assegnati rispettivamente a tutte le porte. Il criterio di monitoraggio predefinito in Criteri di accesso è per le porte del pannello anteriore, mentre il criterio di monitoraggio predefinito in Criteri infrastruttura è per le porte dell'infrastruttura.

A meno che non sia necessario modificare le soglie per le porte, il criterio di monitoraggio predefinito in ciascuna sezione può essere modificato direttamente in modo da applicare la modifica a tutte le porte del pannello anteriore e/o a tutte le porte della struttura.

In questo esempio vengono modificate le soglie per Forward Drop in eqptIngrDropPkts sulle porte fabric (criteri fabric). Eseguire la stessa operazione in Fabric > Criteri di accesso per le porte del pannello anteriore.

1. Passare a Fabric > Criteri fabric>Criteri di monitoraggio.
2. Fare clic con il pulsante destro del mouse e selezionare Crea criterio di monitoraggio.

Se la modifica della soglia può essere applicata a tutte le porte dell'infrastruttura, passare alle porte predefinite anziché crearne una nuova.

3. Espandere il nuovo criterio di controllo o l'impostazione predefinita e passare a Criteri raccolta statistiche.
4. Fare clic sull'icona a forma di matita per l'oggetto di monitoraggio nel riquadro di destra, quindi selezionare Configurazione interfaccia fisica layer 1 (l1.Physlf).

È possibile ignorare il passaggio 4 quando si utilizza il criterio predefinito.

5. Dal menu a discesa Oggetto di monitoraggio nel riquadro di destra, scegliere Configurazione interfaccia fisica di layer 1 (I1.PhysIf) e Tipo di stato, scegliere Pacchetti in ingresso scartati

The screenshot shows the Cisco Fabric Policy configuration interface. The top navigation bar includes System, Tenants, Fabric (selected), VM Networking, L4-L7 Services, Admin, and Operations. Below the navigation bar, the breadcrumb trail is Inventory | Fabric Policies | Access Policies. On the left, a 'Policies' sidebar lists various policy categories, with 'Stats Collection Policies' selected. The main content area is titled 'Stats Collection Policies' and features two dropdown menus: 'Monitoring Object' set to 'Layer 1 Physical Interface Configuration (I1.Ph)' and 'Stats Type' set to 'Ingress Drop Packets'. Below these, a table displays configuration details:

Granularity	Admin State
5 Minute	inherited

6. Fare clic su + Accanto a Soglie di configurazione.




This screenshot shows the same configuration page as above, but with a 'Config Thresholds' button highlighted in a red box. The button is located in the bottom right corner of the configuration area, next to a close (X) and expand (+) icon. The table below the configuration details remains the same:

Granularity	Admin State	History Retention Period
5 Minute	inherited	inherited

7. Modificare la soglia per il rilascio dell'inoltro.

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. Si consiglia di disabilitare le soglie crescenti da configurare per la velocità di rilascio critica, maggiore, minore e di inoltro.

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

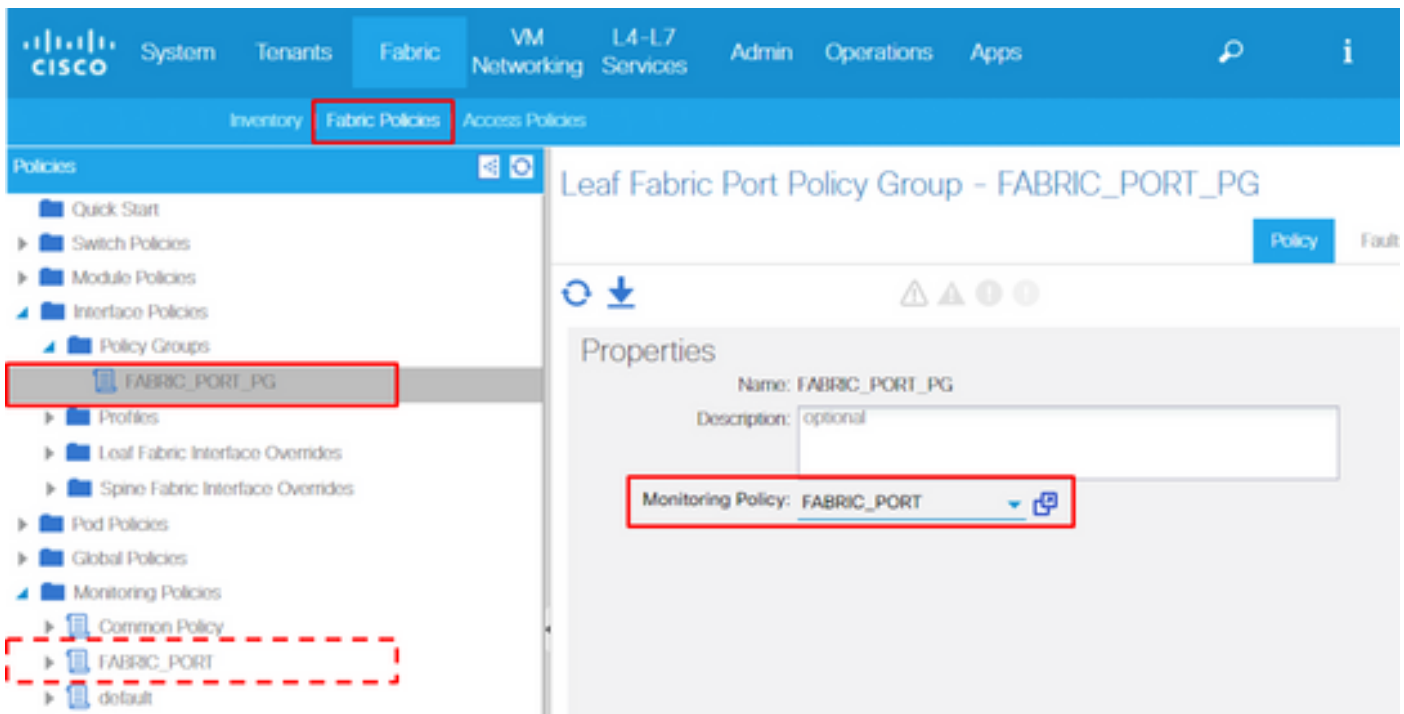
	Set	Reset
Critical	10000	9000
Major	5000	4900
Minor	500	490
Warning	10	9

	Reset	Set
Warning	0	0
Minor	0	0
Major	0	0
Critical	0	0

SUBMIT CANCEL

9. Applicare questo nuovo criterio di monitoraggio al gruppo di criteri di interfaccia per le porte richieste. Non dimenticare di configurare il profilo dell'interfaccia, il profilo dello switch e così via in Criteri fabric di conseguenza.

(Il passaggio 9 può essere ignorato quando si utilizza il criterio predefinito).



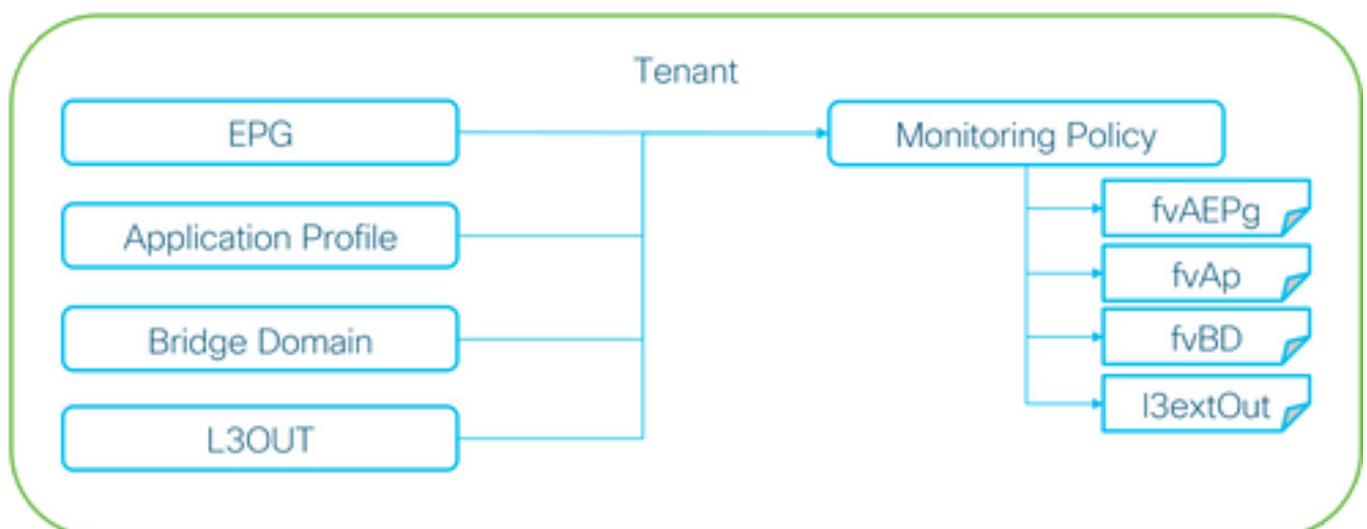
10. Se ciò è vero per le porte del pannello anteriore (criteri di accesso), eseguire la stessa operazione per l'interfaccia aggregata (pc.AggrIf) anziché per la configurazione dell'interfaccia fisica di layer 1 (I1.PhysIf) in modo che questo nuovo criterio di monitoraggio possa essere applicato sia alla porta-canale che alla porta fisica.

È possibile ignorare il passaggio 10 quando si utilizza il criterio predefinito.

Frequenza pacchetti in ingresso ignorati in I2IngrPktsAg

Ci sono più parti per questo.

VLAN or any aggregation of VLAN stats



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

Come illustrato nella figura precedente, I2IngrPktsAg è monitorato sotto molti oggetti.

Nell'immagine precedente sono illustrati solo alcuni esempi, ma non tutti gli oggetti per I2IngrPktsAg. Tuttavia, la soglia per le statistiche è configurata tramite Criteri di monitoraggio e eqptIngrDropPkts in I1PhysIf o pcAggrIf.

A ogni oggetto (EPG(fvAEPg), Bridge Domain(fvBD) e così via) può essere assegnato un proprio criterio di monitoraggio, come mostrato nella figura precedente.

Per impostazione predefinita, tutti questi oggetti nel tenant utilizzano il criterio di monitoraggio predefinito in Tenant > comune > Criteri di monitoraggio > predefinito, se non diversamente configurato.

A meno che non sia necessario modificare le soglie per ogni componente, il criterio di monitoraggio predefinito in tenant comune può essere modificato direttamente per applicare la modifica a tutti i componenti correlati.

In questo esempio vengono modificate le soglie per la frequenza dei pacchetti in ingresso scartati in I2IngrPktsAg15min nel dominio del bridge.

1. Passare a Tenant > (nome tenant) > Criteri di controllo.

(il tenant deve essere comune se si utilizza il criterio di monitoraggio predefinito o se il nuovo criterio di monitoraggio deve essere applicato tra tenant)

2. Fare clic con il pulsante destro del mouse e selezionare Crea criterio di monitoraggio.

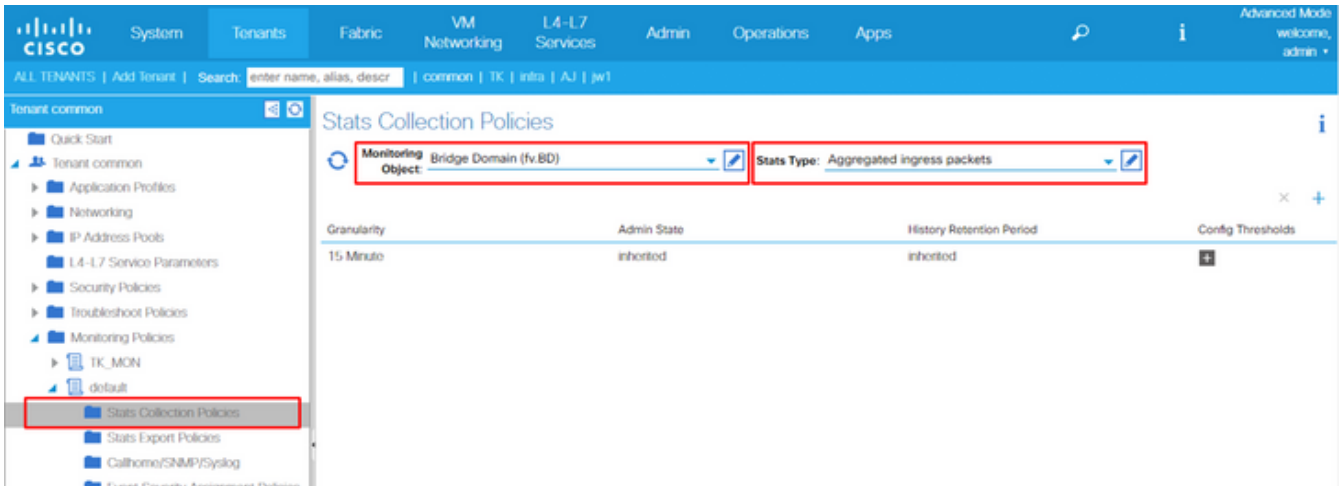
Se la modifica della soglia può essere applicata a tutti i componenti, passare a default anziché crearne uno nuovo.

3. Espandere il nuovo criterio di controllo o l'impostazione predefinita e passare a Criteri raccolta statistiche.

4. Fare clic sull'icona a forma di matita per l'oggetto di monitoraggio nel riquadro di destra, quindi selezionare Dominio Bridge (fv.BD).

È possibile ignorare il passaggio 4 quando si utilizza il criterio predefinito.

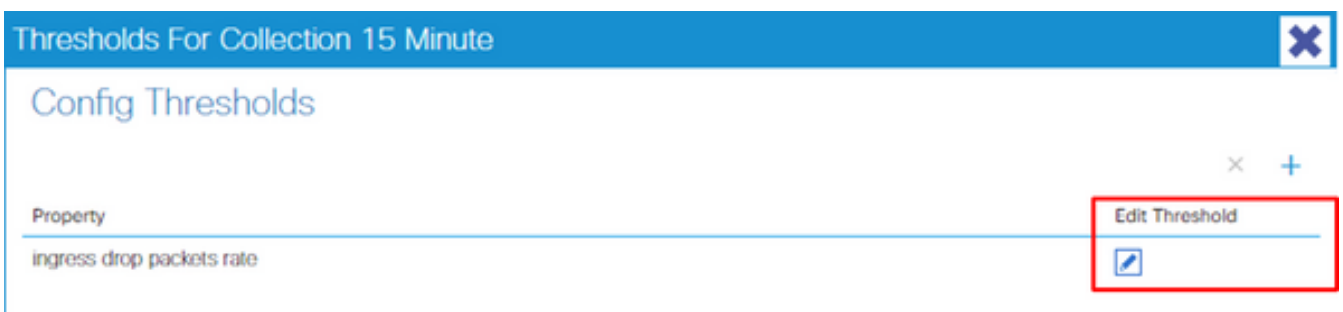
5. Dal menu a discesa Oggetto di monitoraggio nel riquadro di destra, scegliere Dominio bridge (fv.BD) e Tipo di statistiche, scegliere Pacchetti in entrata aggregati.



6. Fare clic su + Accanto a Soglie di configurazione.



7. Modificare la soglia per il rilascio dell'inoltro.



8. Si consiglia di disabilitare le soglie crescenti da configurare per la velocità di rilascio critica, maggiore, minore e di inoltro.

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. Applicare questo nuovo criterio di monitoraggio al dominio bridge che richiede la modifica della soglia.


(Il passaggio 9 può essere ignorato quando si utilizza il criterio predefinito).

The screenshot shows the Cisco SD-WAN GUI for a Bridge Domain (BD1). The 'Monitoring Policy' is set to 'TK_MON', which is highlighted with a red box. The 'Properties' section shows the following details:

- Unknown Unicast Traffic Class ID: 32770
- Segment: 15826915
- Multicast Address: 225.1.26.128
- NetFlow Monitor Policies: (empty)

NOTA:

I criteri di monitoraggio non predefiniti non possono includere configurazioni presenti nei criteri di monitoraggio predefiniti. Se è necessario mantenere queste configurazioni uguali a

 quelle predefinite, gli utenti dovranno controllare la configurazione predefinita dei criteri di monitoraggio e configurare manualmente gli stessi criteri per i criteri di monitoraggio non predefiniti.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).