

Domande frequenti - Output sugli switch Cisco Catalyst serie 9000

Introduzione

Questo documento contiene le risposte alle domande comuni relative alle perdite di output sugli switch Cisco Catalyst serie 9000.

Prerequisiti

Requisiti

Cisco raccomanda una conoscenza di base dei concetti di switching, tra cui le configurazioni QoS (Quality of Service) e il buffering dell'interfaccia.

Componenti usati

Questo documento si applica a tutti gli switch Cisco Catalyst serie 9000 e non è limitato a versioni hardware o software specifiche.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le perdite di output si verificano quando un buffer di uscita dell'interfaccia è esaurito, con conseguente perdita di pacchetti e prestazioni di rete ridotte. Le cause più comuni includono congestione della rete, micro-burst del traffico, configurazioni errate o limitazioni hardware. Questo documento Domande frequenti (FAQ) risponde alle domande frequenti sulle cadute di output sugli switch Cisco Catalyst serie 9000. Fornisce indicazioni sull'identificazione delle cause principali, sulle metodologie di risoluzione dei problemi e sulle procedure consigliate per ripristinare l'efficienza e l'affidabilità della rete.

D. Che cosa sono le perdite di output?

R. Le perdite di output sugli switch Cisco Catalyst 9000 si riferiscono al numero di pacchetti ignorati e non trasmessi da un'interfaccia, anche se i pacchetti sono stati elaborati dal dispositivo. Questo si verifica quando la coda di output dell'interfaccia è piena. L'interfaccia dello switch ha buffer hardware che memorizzano temporaneamente i pacchetti prima che vengano trasmessi o inoltrati fuori dalla porta. Quando la velocità del traffico in uscita supera la velocità alla quale l'hardware può trasmetterlo, i buffer si riempiono e gli eventuali pacchetti aggiuntivi in arrivo alla coda vengono scartati.

D. Quale comando può essere utilizzato per controllare le perdite di output?

A. Usare il comando `show interfaces <interface>` e cercare il contatore delle perdite di output totali, che indica il numero di pacchetti scartati sulla coda di output dell'interfaccia.

Esempio:

```
<#root>
```

```
GigabitEthernet1/0/1 is up, line protocol is up (connected)  
  Input queue: 0/2000/0/0 (size/max/drops/flushes);
```

```
Total output drops: 3089
```

```
  Queueing strategy: fifo  
  Output queue: 0/40 (size/max)
```

D. Quali sono le cause più comuni delle perdite di output?

R. Sugli switch Catalyst 9000 i cali di output si verificano in genere quando i pacchetti vengono scartati prima della trasmissione a causa di vari problemi di congestione o configurazione. Le cause più comuni includono:

- **Micro-burst del traffico:** Picchi improvvisi e ad alta intensità di traffico che avvengono in millisecondi. Poiché gli strumenti di monitoraggio di rete standard (come SNMP) eseguono spesso il polling a intervalli di 1 minuto o 5 minuti, questi burst sono spesso invisibili per il software di gestione ma sono sufficienti per scaricare i buffer di uscita dell'hardware.

- Sottoscrizione in eccesso: Quando la larghezza di banda aggregata del traffico in entrata supera in modo significativo la capacità dell'interfaccia in uscita, la congestione è inevitabile. Ciò è comune negli scenari in cui più porte ad alta velocità (ad esempio, 10G) inviano il traffico a un'unica porta a velocità inferiore (ad esempio, 1G).
- Vincoli buffer: Ogni interfaccia ha una quantità limitata di spazio buffer hardware. Quando la coda di uscita raggiunge la capacità massima a causa di una congestione prolungata, lo switch ignora tutti i pacchetti in arrivo finché non diventa disponibile spazio.
- Configurazione errata di Quality of Service (QoS): Criteri QoS non configurati correttamente, in particolare policy aggressive o shaping restrittivo, possono causare cadute. Se una policy è configurata per limitare il traffico al di sotto della capacità di collegamento effettiva, i pacchetti che superano tale soglia verranno scartati anche se il collegamento fisico non è congestionato.
- Mancata corrispondenza di velocità e duplex: Anche se meno comune con la negoziazione automatica moderna, una mancata corrispondenza tra la porta dello switch e il dispositivo connesso può causare una trasmissione inefficiente, un aumento delle collisioni (in half-duplex) e la successiva saturazione della coda.
- Controllo di flusso (IEEE 802.3x): Se il controllo del flusso è abilitato, lo switch può ricevere istruzioni di sospendere la trasmissione dal dispositivo ricevente. Se i frame di pausa sono frequenti, l'uscita dei buffer dello switch può riempirsi, causando perdite di dati in attesa della ripresa della trasmissione.
- Squilibrio porta-canale: se il traffico in EtherChannel/Port-Channel non è distribuito uniformemente sui collegamenti membri, un'interfaccia può diventare congestionata e le altre rimangono sottoutilizzate.

D. Cosa sono i micro-burst?

R. I micro-burst sono picchi di traffico di breve durata e ad alta intensità che si verificano in microsecondi o millisecondi. e causano perdite di output poiché esauriscono immediatamente i buffer hardware in uscita sugli switch Catalyst 9000. Poiché gli strumenti di monitoraggio standard registrano una media del traffico su intervalli più lunghi, questi picchi spesso rimangono invisibili. Ciò comporta la perdita di pacchetti anche quando l'utilizzo medio di un'interfaccia è nettamente superiore alla capacità. Di conseguenza, questi picchi transitori sono una causa primaria di congestione negli ambienti di rete ad alta velocità.

D. Le riduzioni dell'output sono sempre un problema?

R. No, le perdite di output possono verificarsi durante brevi picchi di traffico anche in reti sane. Gli switch moderni utilizzano l'accodamento basato su buffer e potrebbero verificarsi cali occasionali senza influire sulle applicazioni. Le cali in genere diventano problematiche quando:

- Le cadute aumentano continuamente

- Latenza o perdita di pacchetti per le applicazioni
- Aumento ritrasmissioni TCP
- Il problema riguarda le applicazioni in tempo reale (VoIP/video)

D. Perché si verificano cali di output anche quando l'interfaccia non è completamente utilizzata?

R. Le perdite di output possono verificarsi anche quando l'utilizzo dell'interfaccia è ben al di sotto della larghezza di banda massima del collegamento (ad esempio, al di sotto di 1000 MBPS su un'interfaccia Gigabit). Questo accade perché il traffico di rete non viene trasmesso in un flusso perfettamente uniforme e continuo. In uno scenario ideale, ogni bit viene trasmesso uniformemente attraverso il collegamento e tutti i dispositivi inviano il traffico a intervalli sincronizzati precisi. Tuttavia, nelle reti reali, i dispositivi trasmettono il traffico quando necessario. Di conseguenza, possono arrivare contemporaneamente più pacchetti allo switch che devono essere trasmessi tramite la stessa interfaccia in uscita. Per gestire questa situazione, gli switch usano buffer hardware su ciascuna interfaccia. In questi buffer vengono temporaneamente memorizzati i pacchetti che arrivano contemporaneamente in modo che possano essere trasmessi in sequenza sul collegamento. Se il volume dei pacchetti in arrivo all'interfaccia in un determinato momento supera la capacità del buffer disponibile, lo switch non può archivarli tutti. In questo caso, i pacchetti in eccesso vengono scartati, con una conseguente perdita di output.

Ecco perché è possibile osservare le perdite di output anche quando l'utilizzo medio della larghezza di banda è relativamente basso (ad esempio, 300 MBPS su un'interfaccia di 1 GBPS). L'utilizzo medio può sembrare basso, ma brevi picchi di traffico possono momentaneamente superare la capacità dell'interfaccia di trasmettere i pacchetti o superare la capacità del buffer disponibile.

È inoltre importante notare che i valori di utilizzo dell'interfaccia visualizzati tramite gli strumenti di monitoraggio SNMP o il comando `show interface` si basano su misurazioni medie del traffico su intervalli quali 30 secondi o 5 minuti. Queste medie non riflettono picchi di traffico molto brevi che possono verificarsi in millisecondi.

D. Come posso controllare le cadute di uscita senza aumentare la velocità del collegamento?

R. È possibile gestire e ridurre le perdite di output sugli switch Catalyst 9000 tramite diverse tecniche senza aggiornare la velocità del collegamento fisico:

- Aumentare il Moltiplicatore SoftMax (mitigazione rapida): per aumentare il numero di buffer che una coda può richiedere al pool di buffer condiviso, è possibile regolare la soglia SoftMax utilizzando il comando di configurazione globale `qos queue-softmax-multiplier <100-1200>`. Il valore predefinito è 100. Se si imposta questo valore su 1200, la capacità della coda di assorbire i microburst aumenta di un fattore di 12 rispetto alla configurazione predefinita.

Questo comando aumenta le soglie della coda delle porte in modo che la coda possa utilizzare unità buffer aggiuntive dal pool di buffer condiviso quando necessario. Questa tecnica viene in genere utilizzata come tecnica di mitigazione rapida per ridurre le perdite di output causate da picchi di traffico. Tuttavia, poiché i buffer sono risorse condivise, la configurazione presuppone che i microburst non si verifichino contemporaneamente su tutte le porte.

Modifica buffer per coda (regolazione criteri QoS): se il moltiplicatore SoftMax è insufficiente, è possibile regolare l'allocazione del buffer a livello di coda utilizzando le mappe dei criteri QoS. Ciò consente agli amministratori di allocare più spazio del buffer a classi di traffico specifiche, modificare le percentuali del buffer della coda e configurare le code di priorità per il traffico critico. Questo approccio è utile quando tipi di traffico specifici richiedono risorse buffer dedicate o quando i profili di traffico variano in modo significativo.

Esempio:

```
policy-map QOS-POLICY
class VOICE
  priority level 1
  queue-buffers ratio 50
class class-default
  queue-buffers ratio 50
```

- Implementazione QoS (Quality of Service): Aiuta a controllare la perdita di pacchetti dando la priorità al traffico di rete critico durante i periodi di congestione. Consente alle reti di assegnare priorità al traffico sensibile alla latenza, ad esempio voce e video, proteggere il traffico del control plane e garantire che i dati importanti vengano trasmessi prima del traffico con priorità inferiore. I meccanismi QoS tipici includono la classificazione del traffico, la definizione delle priorità delle code, l'allocazione dei buffer delle code e la gestione delle congestioni. Applicando queste tecniche, la rete può garantire che venga prima interrotto il traffico meno importante, proteggendo le applicazioni business-critical e mantenendo le prestazioni complessive della rete.
- Traffic Shaping: configurare il traffic shaping sull'interfaccia per attenuare i picchi di traffico. Limitando la velocità di trasmissione leggermente al di sotto della velocità della linea fisica, si forza il traffico da memorizzare nel buffer e da inviare a una velocità costante e prevedibile. Questo previene il comportamento della caduta della coda causato da improvvisi micro-

scoppio ad alta velocità.

Esempio:

```
policy-map SHAPE-POLICY
class class-default
shape average
```

- Ottimizza distribuzione del carico (bilanciamento porta-canale): In una configurazione EtherChannel o Port-Channel, l'hashing non uniforme può causare la congestione di collegamenti membri specifici, mentre altri rimangono sottoutilizzati. Ottimizzando gli algoritmi di bilanciamento del carico, è possibile garantire una distribuzione uniforme del traffico tra tutti i collegamenti membro, evitando congestione sulle singole interfacce e riducendo le perdite di output.

Esempio:

```
port-channel load-balance src-dst-ip
```

D. Qual è la soluzione definitiva per le perdite di output?

R. Le soluzioni più efficaci per eliminare le perdite di output sono:

- Aumento della velocità della linea di interfaccia: aggiornare la velocità dell'interfaccia per fornire una maggiore larghezza di banda in uscita e ridurre l'oversubscription. Ad esempio, passare da un'interfaccia 1G a un'interfaccia 10G se disponibile sullo switch.
- Use Port Bundling (EtherChannel): consente di aggregare più collegamenti fisici in un singolo collegamento logico utilizzando il bundling delle porte, a condizione che il dispositivo connesso supporti questa funzionalità. In questo modo si aumenta la larghezza di banda complessiva e si distribuisce il carico del traffico.
- Aggiornamento hardware quando necessario: se un'interfaccia a velocità più elevata non è disponibile sullo switch e il bundling delle porte non è supportato dal dispositivo connesso, valutare l'opportunità di aggiornare la piattaforma hardware a un'interfaccia con capacità superiore o buffer di dimensioni maggiori.

D. Come è possibile controllare le statistiche di coda su

un'interfaccia?

R. Per gli switch Catalyst 9000, è possibile controllare le statistiche dettagliate della coda dell'hardware usando il comando `show platform hardware fed active qos queue stats interface<port>`. Questo comando fornisce statistiche dettagliate, tra cui l'utilizzo del buffer, i conteggi di accodamento e i contatori di rilascio per coda sull'interfaccia specificata, consentendo di monitorare le prestazioni della coda e di identificare la congestione o le perdite di pacchetti.

Esempio:

<#root>

```
show platform hardware fed switch active qos queue stats interface Gig 1/0/1
```

DATA Port:0 Enqueue Counters

Q	Buffers (Count)	Enqueue-TH0 (Bytes)	Enqueue-TH1 (Bytes)	Enqueue-TH2 (Bytes)	Qpolicer (Bytes)
---	--------------------	------------------------	------------------------	------------------------	---------------------

0	0	0	0	0	
---	---	---	---	---	--

384251797

1	0	0	0	0	
---	---	---	---	---	--

488393930284

0

...

DATA Port:0 Drop Counters

Q	Drop-TH0 (Bytes)	Drop-TH1 (Bytes)	Drop-TH2 (Bytes)	SBufDrop (Bytes)
---	---------------------	---------------------	---------------------	---------------------

0	0	0	0	0
1	0	0		

192308101

0

0

0

...

D. Come verificare se QoS sta causando cali di output?

R. Per verificare se QoS è responsabile delle interruzioni dell'output, controllare le statistiche dei criteri QoS usando il comando `show policy-map interface <interface>` e i contatori della coda. Se i contatori delle interruzioni aumentano in una classe QoS specifica, le interruzioni possono essere causate da limiti della coda QoS o dal monitoraggio dei criteri. Se possibile, durante una finestra di manutenzione, rimuovere temporaneamente i criteri QoS dall'interfaccia usando il comando `no service-policy output <policy-name>` e controllare se le interruzioni dell'output continuano. Se le eliminazioni si interrompono dopo la rimozione del criterio, è probabile che la configurazione QoS contribuisca alle eliminazioni.

Esempio:

```
<#root>
```

```
sh policy-map interface gigabitEthernet 1/0/1
```

```
GigabitEthernet1/0/1  
Service-policy output: TEST  
Class-map: class-default (match-any)  
0 packets  
Match: any  
Queueing
```

```
(total drops) 587230
```

```
(bytes output) 834545
```

```
...
```

D. Le interfacce ad alta velocità come 10G o 40G possono causare cadute nell'output?

R. Sì, anche le interfacce ad alta velocità come 10G o 40G possono sperimentare perdite di output quando più flussi ad alta velocità convergono su una singola porta, causando il sovraccarico dei buffer di interfaccia. Inoltre, i microburst, ovvero brevi picchi di traffico che superano la larghezza di banda dell'interfaccia, possono esaurire rapidamente i buffer delle porte e causare la perdita dei pacchetti.

D. Le perdite di output possono essere causate da guasti hardware?

R. Le perdite di output non sono generalmente causate da errori hardware. In genere sono il risultato di una congestione del traffico, in cui i buffer di interfaccia vengono sovraccaricati a causa di alte velocità di traffico o microburst. Possono verificarsi cali legati all'hardware, ma in genere

sono legati a condizioni di errore specifiche, che sono rare rispetto alle cali dovute alla congestione. Pertanto, le riduzioni dell'output sono per la maggior parte associate a condizioni del traffico di rete piuttosto che a guasti hardware. Il monitoraggio degli errori dell'interfaccia, come gli errori FCS/CRC, può aiutare a identificare eventuali problemi hardware, ma questi sono diversi dalle perdite di output causate dalla congestione.

D. I bug del software possono causare perdite di output?

R. Le cadute di output causate da difetti del software sono molto rare e per lo più estetiche, e non incidono in modo sostanziale sul traffico. La maggior parte delle perdite di output è causata principalmente da congestione del traffico e esaurimento dei buffer.

D. L'ECMP o il bilanciamento del carico possono ridurre la congestione?

R. Sì, il routing ECMP (Equal-Cost Multi-Path) e il bilanciamento del carico riducono la congestione distribuendo il traffico in modo uniforme su più percorsi a costo uguale a una destinazione. Questo approccio aumenta l'utilizzo della larghezza di banda e impedisce che un singolo percorso diventi un collo di bottiglia.

D. Le perdite di output influiscono sul traffico UDP in modo diverso rispetto al protocollo TCP?

R. Sì, le perdite di output influiscono sul traffico UDP in modo diverso rispetto al TCP perché UDP è un protocollo senza connessione che non ritrasmette i pacchetti persi, quindi qualsiasi perdita di pacchetto influisce direttamente su applicazioni quali voce o video, che si basano sulla consegna puntuale. Il protocollo TCP, al contrario, include meccanismi di ritrasmissione che tentano di recuperare i pacchetti persi, riducendo l'impatto delle perdite. Pertanto, le perdite di output possono causare un peggioramento più evidente nelle applicazioni in tempo reale basate su UDP, in quanto i pacchetti persi non vengono recuperati e possono causare problemi di qualità.

D. Qual è la differenza tra le perdite di input e le perdite di output?

R. Le interfacce perdono l'input quando le code di input si sovraccaricano e non sono in grado di elaborare i pacchetti abbastanza velocemente, causando l'eliminazione selettiva dei pacchetti in base all'algoritmo di coda. Le perdite di output si verificano quando i pacchetti vengono scartati

mentre si esce da un'interfaccia a causa di una congestione della coda di output o dell'esaurimento del buffer. Le perdite di input sono correlate ai limiti di elaborazione in entrata, mentre le perdite di output sono causate principalmente dalla congestione in uscita e dall'overflow del buffer. Queste cadute possono essere influenzate da fattori come i picchi di traffico, le limitazioni della piattaforma e le configurazioni QoS (Quality of Service) che gestiscono la congestione e l'allocazione dei buffer.

D. Processi di backup di grandi dimensioni possono causare perdite di output?

R. Sì, i processi di backup di grandi dimensioni, ad esempio i backup dei dati, la replica o i trasferimenti in blocco, spesso generano traffico bursty che può sovraccaricare i buffer di interfaccia, con conseguenti perdite di output. Questi burst possono causare una congestione temporanea sull'interfaccia in uscita, in particolare quando la larghezza di banda in uscita è inferiore alla velocità del traffico in entrata o quando più flussi ad alta velocità convergono su una singola porta.

D. Come è possibile stabilire se i picchi di traffico stanno causando cali di output?

R. Per confermare le perdite di output causate da picchi di traffico, è possibile usare una sessione SPAN insieme a Wireshark per catturare e analizzare il traffico in uscita sull'interfaccia interessata mentre si verificano cali di output. Attenersi alla seguente procedura per verificare le perdite di output causate da picchi di traffico.

- Collegare un notebook con Wireshark installato a una porta inutilizzata dello switch.
- Configurare SPAN sullo switch in modo che esegua il mirroring del traffico in uscita dell'interfaccia che ha generato l'output sulla porta a cui è connesso il laptop.

```
monitor session 1 source interface
```

Tx

```
monitor session 1 destination interface
```

Replce

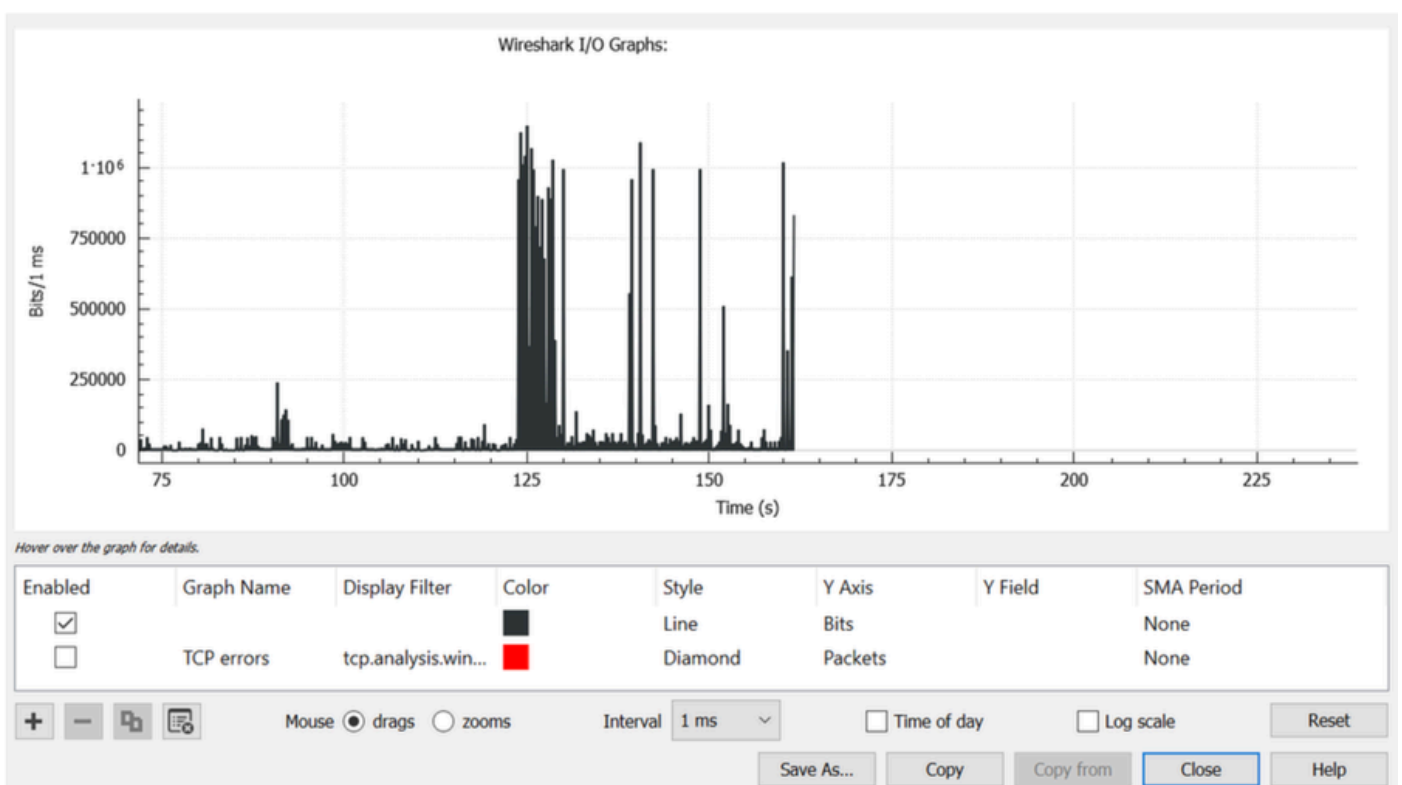
with the interface where output drops are seen for the source.

Replace

with the interface connected to the laptop for the destination.

- Avviare l'acquisizione SPAN sullo switch mentre le interruzioni dell'output aumentano attivamente per assicurare l'acquisizione del traffico rilevante.
- Aprire il file di acquisizione in Wireshark, quindi selezionare Statistiche > Grafico I/O.
- Modificare l'intervallo predefinito da 1 secondo a 1 millisecondo (1 ms).
- Per aggiornare il grafico con il nuovo intervallo, fate clic su Reimposta (Reset).
- Il grafico visualizzerà il traffico in bit per millisecondo.

Cercare i picchi di traffico che superano la velocità di inoltro dell'interfaccia su una scala di millisecondi (ad esempio, 1.000.000 bit/ms per un'interfaccia di 1 GBPS). Quando il traffico supera questa velocità di inoltro, lo switch memorizza nel buffer i pacchetti e ciò può causare congestione e perdite di output. Identificare i picchi di traffico (microburst) osservando i picchi seguiti da periodi di traffico basso o assente. A Wireshark, cliccando su un picco si selezionano i pacchetti corrispondenti, permettendo un'ulteriore analisi del traffico che ha innescato le gocce. L'immagine seguente mostra il grafico I/O aggiornato di un'interfaccia che ha sperimentato cali di output.



Considerazioni importanti

- Accertarsi che le porte di origine e di destinazione SPAN abbiano la stessa velocità o una velocità compatibile, in modo da evitare l'introduzione di cadute aggiuntive.
- Acquisire il traffico mentre le perdite di output sono in aumento per acquisire i picchi rilevanti.
- Non è consigliabile l'uso dell'EPC (Embedded Packet Capture), in quanto limita le velocità di acquisizione e può evitare picchi di attività.

Concetti errati comuni sulle perdite di output

Concezione errata: Qualsiasi perdita di output indica un malfunzionamento della rete.

Realtà: Nelle reti ad alta velocità, un piccolo numero di perdite di output è normale a causa di microburst o brevi picchi di traffico.

Concezione errata: Se l'utilizzo dell'interfaccia è basso, non devono verificarsi cali.

Realtà: L'utilizzo è misurato come media nel tempo. I microburst possono temporaneamente superare la larghezza di banda dell'interfaccia, causando cali anche quando l'utilizzo medio è basso.

Concezione errata: Le perdite di output indicano che l'hardware dello switch è difettoso.

Realtà: Le interruzioni dell'output sono in genere causate da traffico congestionato o bursty, non da problemi hardware.

Concezione errata: Aumentando l'allocazione del buffer si eviteranno tutte le cadute.

Realtà: I buffer assorbono solo burst temporanei. La congestione persistente provocherà comunque la perdita dei pacchetti.

Concezione errata: Solo le interfacce 1G registrano una riduzione dell'output.

Realtà: Le interfacce a 10G, 25G, 40G o velocità superiore possono subire cadute quando i picchi di traffico superano la larghezza di banda o la capacità del buffer disponibili.

Concezione errata: QoS deve eliminare tutte le perdite di dati/impedire la perdita di pacchetti.

Realtà: QoS assegna priorità al traffico importante, ma può eliminare intenzionalmente il traffico con priorità inferiore durante la congestione.

Concezione errata: Qualsiasi perdita di output causerà l'impatto sull'utente.

Realtà: Molte applicazioni utilizzano la ritrasmissione TCP, che consente di ripristinare i dati in caso di cadute di pacchetti occasionali senza alcun impatto visibile.

Concezione errata: Le riduzioni si verificano solo quando le interfacce raggiungono il 100% di utilizzo.

Realtà: Le cadute possono verificarsi durante brevi picchi di traffico, anche se l'utilizzo medio rimane basso.

Concezione errata: La configurazione QoS è sempre la causa di cadute.

Realtà: La maggior parte delle cadute è causata da modelli di traffico o da sottoscrizioni eccessive, non da criteri QoS.

Concezione errata: Una rete integra non deve mai avere perdite di output.

Realtà: Negli ambienti di switching ad alte prestazioni, si prevedono cali occasionali e normali.

Guide alla risoluzione dei problemi

- [Risoluzione dei problemi relativi ai pacchetti eliminati nella coda di output sui dispositivi Catalyst 9000 Switch](#)
- [Informazioni sull'allocazione dei buffer di coda sugli switch Catalyst 9000](#)
- [Supporto tecnico Cisco e download](#)

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).