QoS Catalyst 6500/6000 - Domande frequenti

Sommario

Introduzione
QoS è abilitato per impostazione predefinita sugli switch Catalyst 6500?
Qual è il valore DSCP (Differentiated Services Code Point) predefinito assegnato ai pacchetti?
È possibile configurare la funzionalità QoS basata su VLAN su uno switch 6500?
Quali sono le funzionalità delle porte per ogni scheda di linea e come si interpretano le funzionalità della coda?
Quali sono le configurazioni QoS predefinite su uno switch 6500 quando QoS è abilitato inizialmente?
Dove vengono eseguiti i singoli processi QoS in Catalyst 6000?
È possibile implementare le funzionalità QoS senza una Policy Feature Card (PFC)?
Qual è la differenza nella funzionalità QoS tra Policy Feature Card 1 (PFC1) e PFC2?
Quali sono le classi di servizio (CoS) predefinite per trasmettere le configurazioni di mapping delle code quando è abilitato il qos automatico?
Qual è il mapping DSCP (Differentiated Services Code Point) predefinito per la classe di servizio (CoS)?
In caso di coda di uscita, se la coda con priorità rigida è satura, il traffico viene eventualmente servito nelle code WRR (Weighted Round-Robin)?
Il WRR (Weighted Round Robin) determina l'assegnazione della larghezza di banda in base al numero di pacchetti o a un determinato numero di byte?
La mia nuova scheda di linea 65xx dice che supporta DWRR (deficit weighted round-robin). Che cos'è DWRR e cosa significa?
Quali sono i pesi predefiniti su una porta 2q2t e come è possibile modificarli?
Desidero utilizzare il protocollo SNMP (Simple Network Management Protocol) per raccogliere il numero di pacchetti scartati da un singolo policer. È possibile? In caso affermativo, quale MIB viene utilizzato?
È disponibile un comando show per visualizzare il numero di pacchetti ignorati dal policer?
Desidero utilizzare il protocollo SNMP (Simple Network Management Protocol) per modificare un policer in modo che i parametri di velocità e burst possano essere modificati in modo dinamico. Ad esempio, per ora del giorno. È possibile? In caso affermativo, quale MIB viene utilizzato?
È possibile implementare la funzionalità QoS basata sull'ora del giorno, in particolare per modificare le velocità massima e burst, tramite il software Cisco IOS sul modulo Multilayer Switch Feature Card (MSFC) in modalità ibrida? Se possibile, la QoS viene eseguita nell'hardware e non dal processore MSFC?
Non ho visto una descrizione di come vengono implementati i valori di burst e frequenza policer. Desidero completare la documentazione tecnica su questi dispositivi, in modo da poter comprendere l'impatto che hanno sulla mia rete.
Ho intenzione di sostituire i miei supervisori Sup1A con Sup2s. Le funzioni QoS, come la velocità di burst, cambiano tra Sup1A e Sup2?
Quali sono alcuni comandi che è possibile utilizzare per monitorare le impostazioni QoS?
Quando si esegue il codice del sistema operativo Catalyst (CatOS) su uno switch 6500 e il

software Cisco IOS in un modulo Multilayer Switch Feature Card (MSFC), si eseguono i comandi QoS sull'MSFC o sul supervisor?
Cosa succede se il comando **set port qos trust** non è supportato dalla scheda di linea?
Qual è la differenza tra i policer di aggregazione e di microflusso?
Quali comandi consentono di visualizzare le statistiche per i criteri di aggregazione o di microflusso?
Il traffic shaping è supportato sugli switch Catalyst 6500 (Cat6K)?
Quanti policer di aggregazione o microflusso sono supportati sullo switch Catalyst 6500 (Cat6K)?
Quale immagine Cisco IOS del sistema operativo Catalyst (CatOS) o Multilayer Switch Feature Card (MSFC) è richiesta per supportare il monitoraggio?
Dopo aver eseguito l'aggiornamento da Sup2 a Sup720, le statistiche sulla velocità del traffico controllato risultano diverse a seconda dello stesso traffico. Perché?
Come è possibile conoscere i valori da utilizzare per la velocità e la frammentazione quando si configura un policer?
Configurazione di QoS su un canale di porta. Ci sono delle restrizioni che devo sapere?
Perché non è possibile regolare il valore della soglia minima?
Non riesco a regolare i buffer della coda di trasmissione. Ci sono delle restrizioni?
Ho una scheda di linea 62xx/63xx. Impossibile applicare il comando set che considera attendibile il punto di codice dei servizi differenziati (DSCP) su una porta. Esiste un limite su questa scheda di linea per le funzionalità QoS?
Quali versioni e supervisori del sistema operativo Catalyst (CatOS) sono richiesti per supportare il monitoraggio?
Cosa devo sapere sulla configurazione di QoS su EtherChannel?
Dove posso trovare esempi di come usare gli Access Control List (ACL) QoS per contrassegnare o controllare il traffico?
Qual è la differenza tra gli elenchi di controllo di accesso (ACL) QoS basati su porta e quelli basati su VLAN?
Qual è il valore tipico delle dimensioni di burst da utilizzare per la limitazione della velocità sugli switch di layer 3?
Perché si ricevono prestazioni inferiori per il traffico TCP con limitazioni di velocità?
Qual è il vantaggio di WRED (Weighted Random Early Detection) e come è possibile stabilire se la scheda di linea supporta WRED?
Che cos'è il DSCP (Differentiated Services Code Point) interno?
Quali sono le possibili fonti del punto di codice interno dei servizi differenziati (DSCP)?
Come viene scelto il DSCP (Differentiated Services Code Point) interno?
CBWFQ (Class-Based Weighted Fair Queuing) o LLQ (Low Latency Queuing) è supportato sugli switch Catalyst 6500 (Cat6K)?
Il valore CoS (Class of Service) di layer 2 viene mantenuto per i pacchetti indirizzati?
QoS applica la stessa configurazione a tutte le porte LAN controllate dallo stesso ASIC?
Perché il comando **show traffic-shape statistics** non restituisce risultati positivi anche se il traffic shapping in è configurato?
Catalyst 6500 PFC supporta tutti i comandi QoS standard?
Perché i contatori CoPP software sono più grandi dei contatori CoPP hardware?
La configurazione QoS del comando predefinito (interfaccia) funziona su altre interfacce/porte?
È possibile configurare QoS in un'interfaccia con un IP secondario?
Informazioni correlate

Introduzione

Questo documento contiene le domande frequenti (FAQ) sulla funzionalità QoS (Quality of Service) di Catalyst 6500/6000 con Supervisor 1 (Sup1), Supervisor 1A (Sup1A), Supervisor 2 (Sup2) e Supervisor 720 (Sup720) con Catalyst OS (CatOS). In questo documento, questi switch sono chiamati switch Catalyst 6500 (Cat6K) con software CatOS. Fare riferimento alla sezione Configurazione delle funzionalità QoS del PFC per le funzionalità QoS sugli switch Catalyst 6500/6000 con software Cisco IOS®.

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

D. Sugli switch Catalyst 6500, QoS è abilitato per impostazione predefinita?

R. Per impostazione predefinita, QoS non è abilitato. Usare il comando **set qos enable** per abilitare QoS.

D. Qual è il valore DSCP (Differentiated Services Code Point) predefinito assegnato ai pacchetti?

R. Tutto il traffico che entra in una porta non attendibile è contrassegnato con un DSCP pari a 0. In particolare, la porta di uscita reimposta il DSCP su 0.

D. È possibile configurare la funzionalità QoS basata su VLAN su uno switch 6500?

R. L'impostazione predefinita è basata sulla porta. Per modificare questa impostazione, usare il comando **set port qos** *mod*/*porta* ***basata su vlan***.

D. Quali sono le funzionalità delle porte per ciascuna scheda di linea e come si interpretano le funzionalità della coda?

A. Fare riferimento alla tabella sulle funzionalità delle porte nella sezione Informazioni sulle funzionalità di coda di una porta di QoS Output Scheduling sugli switch Catalyst serie 6500/6000 con software CatOS.

D. Quali sono le configurazioni QoS predefinite su uno switch 6500 quando QoS è abilitato inizialmente?

R. Fare riferimento alla sezione Configurazione predefinita per QoS sugli switch Catalyst 6000 della programmazione dell'output QoS sugli switch Catalyst serie 6500/6000 con software CatOS.

D. Dove vengono eseguiti i singoli processi QoS in Catalyst 6000?

A. Input Scheduling - Eseguito da circuiti integrati specifici per le porte PINNACLE/COIL (ASIC). Solo layer 2, con o senza Policy Feature Card (PFC).

Classificazione: eseguita dal Supervisor o dalla PFC tramite il motore ACL (Access Control List). solo layer 2, senza PFC; Layer 2 o Layer 3 con PFC.

Policing: eseguito da PFC tramite il motore di inoltro di layer 3. Layer 2 o Layer 3 con PFC (richiesto).

Riscrittura pacchetto: eseguita dagli ASIC delle porte PINNACLE/COIL. Layer 2 o Layer 3 in base alla classificazione effettuata in precedenza.

Programmazione output (Output Scheduling) - Eseguita dagli ASIC delle porte PINNACLE/COIL. Layer 2 o Layer 3 in base alla classificazione effettuata in precedenza.

D. È possibile implementare le funzionalità QoS senza una Policy Feature Card (PFC)?

R. Negli switch Catalyst serie 6000, il cuore della funzionalità QoS risiede sulla PFC ed è un requisito per l'elaborazione QoS di layer 3 o layer 4. Tuttavia, un supervisore senza PFC può essere utilizzato per la classificazione e il contrassegno QoS di layer 2.

D. Qual è la differenza nella funzionalità QoS tra Policy Feature Card 1 (PFC1) e PFC2?

R. PFC2 consente di eseguire il push dei criteri QoS in una DFC (Distributed Forwarding Card). PFC2 aggiunge anche il supporto per un tasso in eccesso, che indica un secondo livello di policing al quale è possibile intraprendere azioni politiche. Per ulteriori informazioni, fare riferimento a Supporto hardware per QoS nella sezione Informazioni sulla qualità del servizio sugli switch Catalyst serie 6000.

D. Quali sono le classi di servizio (CoS) predefinite per trasmettere le configurazioni di mappatura delle code quando è abilitato il qos automatico?

R. set qos map 2q2t tx queue 2 2 cos 5,6,7

set qos map 2q2t tx queue 2 1 cos 1,2,3,4

set qos map 2q2t tx queue 1 1 cos 0

D. Qual è il mapping predefinito del punto di codice dei servizi differenziati (DSCP) alla classe di servizio (CoS)?

R. 8 a 1 (dividere DSCP per 8 per ottenere CoS).

D. Nelle code in uscita, se la coda con priorità rigida è satura, il traffico viene eventualmente servito nelle code WRR (Weighted Round-Robin)?

R. No, le code WRR non vengono servite finché la coda di priorità non è completamente vuota.

D. Il WRR (Weighted Round Robin) determina l'assegnazione della larghezza di banda in base al numero di pacchetti o a un certo numero di byte?

R. Basato su un determinato numero di byte, che possono rappresentare più di un pacchetto. Il pacchetto finale che supera i byte allocati non viene inviato. Con una configurazione di peso

estremo, ad esempio 1% per la coda 1 e 99% per la coda 2, il peso configurato esatto potrebbe non essere raggiunto. Lo switch usa un algoritmo WRR per trasmettere i frame da una coda alla volta. WRR utilizza un valore di rilevanza per decidere quanto trasmettere da una coda prima di passare all'altra. Maggiore è il peso assegnato a una coda, maggiore sarà la larghezza di banda di trasmissione ad essa assegnata.

Nota: Il numero effettivo di byte trasmessi non corrisponde al calcolo perché vengono trasmessi fotogrammi interi prima del passaggio all'altra coda.

D. La mia nuova scheda di linea 65xx dice che supporta DWRR (deficit weighted round-robin). Che cos'è DWRR e cosa significa?

R. DWRR trasmette dalle code senza affamare la coda a bassa priorità, in quanto tiene traccia della sottotrasmissione della coda a bassa priorità e la compensa nel ciclo successivo. Se una coda non è in grado di inviare un pacchetto perché le sue dimensioni sono superiori ai byte disponibili, i byte inutilizzati vengono accreditati al round successivo.

D. Quali sono i pesi predefiniti su una porta 2q2t e come è possibile modificarli?

A. Utilizzare il comando **set qos wrr 2q2t** *q1_weight q2_weight* per modificare i pesi predefiniti per la coda 1 (la coda a bassa priorità servita 5/260 dell'orario) e la coda 2 (la coda ad alta priorità servita 255/260 dell'orario).

D. Desidero utilizzare il protocollo SNMP (Simple Network Management Protocol) per raccogliere il numero di pacchetti scartati da un singolo policer. È possibile? In caso affermativo, quale MIB viene utilizzato?

R. Sì, il protocollo SNMP supporta CISCO-QOS-PIB-MIB e CISCO-CAR-MIB.

D. È disponibile un comando show per visualizzare il numero di pacchetti ignorati dal policer?

R. I comandi **show qos statistics aggregate-policer** e **show qos statistics l3stats** visualizzano il numero di pacchetti scartati dal policer.

D. Desidero utilizzare il protocollo SNMP (Simple Network Management Protocol) per modificare un policer in modo che la velocità e i parametri burst possano essere modificati in modo dinamico. Ad esempio, per ora del giorno. È possibile? In caso affermativo, quale MIB viene utilizzato?

R. Sì, il protocollo SNMP supporta CISCO-QOS-PIB-MIB e CISCO-CAR-MIB.

D. È possibile implementare QoS basato sull'ora del giorno—in particolare, per modificare le velocità massima e burst—tramite il software Cisco IOS sul modulo Multilayer Switch Feature Card (MSFC) in modalità ibrida? Se possibile, la QoS viene eseguita nell'hardware e non dal processore MSFC?

R. No, non è possibile. In modalità ibrida (CatOS), tutto il monitoraggio QoS viene eseguito dal

supervisore.

D. Non è stata visualizzata una descrizione di come vengono implementati i valori di burst e tasso policer. Desidero completare la documentazione tecnica su questi dispositivi, in modo da poter comprendere l'impatto che hanno sulla mia rete.

A. I valori di burst e frequenza policer vengono implementati nel modo seguente:

```
burst = sustained rate bps × 0.00025 (the leaky bucket rate) + MTU kbps
```

Ad esempio, se si desidera un policer da 20 Mbps e un'unità di trasmissione massima (MTU) (su Ethernet) di 1500 byte, la frammentazione viene calcolata nel modo seguente:

```
burst = (20,000,000 bps × 0.00025) + (1500 × 0.008 kbps)
      = 5000 bps + 12 kbps
      = 17 kbps
```

Tuttavia, a causa della granularità dell'hardware di controllo con Sup1 e Sup2, è necessario arrotondare questo a 32 kbps, che è il minimo.

Per ulteriori informazioni sull'implementazione dei valori burst e della velocità del policer, consultare i seguenti documenti:

- Pianificazione dell'output QoS sugli switch Catalyst serie 6500/6000 con software CatOS
- Configurazione di QoS

D. Ho intenzione di sostituire i miei Supervisori Sup1A con Sup2s. Le funzioni QoS, come la velocità di burst, cambiano tra Sup1A e Sup2?

R. Sì, ci sono differenze tra due supervisori quando su uno switch Catalyst 6500 è installato il protocollo SUP2/PFC2. Se è in esecuzione Cisco Express Forwarding (CEF), il comportamento è leggermente diverso quando si configura il netflow in SUP2.

D. Quali sono alcuni comandi che è possibile utilizzare per monitorare le impostazioni QoS?

A. Fare riferimento alla sezione Monitoraggio e verifica della configurazione di Classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS.

D. Quando si esegue il codice del sistema operativo Catalyst (CatOs) su uno switch 6500 e il software Cisco IOS in un modulo Multilayer Switch Feature Card (MSFC), si desidera utilizzare i comandi QoS sull'MSFC o sul supervisor?

R. Quando si esegue il codice ibrido (CatOS), utilizzare i comandi QoS sul Supervisor/Policy Feature Card (PFC). Lo switch 6500 esegue la QoS in tre punti:

- Basato su software nell'MSFC
- Basato su hardware (basato su switching multilivello) nel PFC
- Software basato su alcune schede di linea

Questo problema si verifica quando si utilizza un sistema operativo IOS ibrido (CatOS + IOS per

MSFC). CatOS e IOS hanno due set di comandi di configurazione. Tuttavia, quando si configura QoS nel sistema operativo IOS nativo, ad esempio con i nuovi motori Sup32 o Sup720, ci si allontana dall'hardware e la parte della scheda di linea non è visibile all'utente. Questa operazione è importante perché la maggior parte del traffico è a commutazione di più livelli (commutazione di hardware). Pertanto, viene gestita dalla logica PFC. L'MSFC non vede mai quel traffico. Se non si sta configurando una QoS basata su PFC, la maggior parte del traffico viene persa.

D. Cosa succede se il comando set port qos trust non è supportato dalla scheda di linea?

R. È possibile creare un ACL (Access Control List) QoS per considerare attendibile il valore DSCP (Differentiated Services Code Point) del pacchetto in arrivo. Ad esempio, usare il comando **set qos acl ip test trust-dscp any**.

D. Qual è la differenza tra i policer di aggregato e microflusso?

A. Fare riferimento alla sezione Classificazione e controllo con il PFC di Informazioni sulla qualità del servizio sugli switch Catalyst serie 6000.

D. Quali comandi consentono di visualizzare le statistiche per i criteri di aggregazione o microflusso?

R. Con Supervisor Engine 1 e 1A, non è possibile disporre di statistiche di controllo per singoli policer aggregati. Usare il comando **show qos statistics l3stats** per visualizzare le statistiche dei criteri per sistema.

Con Supervisor Engine 2, è possibile visualizzare le statistiche di controllo aggregate per singolo policer con il comando **show qos statistics aggregate-policer**. Usare il comando **show mls entry qos short** per controllare le statistiche di controllo del microflusso.

D. Il traffic shaping è supportato sugli switch Catalyst 6500 (Cat6K)?

R. Il traffic shaping è supportato solo su alcuni moduli WAN per gli switch Catalyst serie 6500/7600, ad esempio i moduli OSM (Optical Services Module) e FlexWAN. Per ulteriori informazioni, fare riferimento a Configurazione di Traffic Shaping basato su classi e Traffic Shaping.

D. Quanti policer di aggregazione o di microflusso sono supportati sullo switch Catalyst 6500 (Cat6K)?

R. Catalyst 6500/6000 supporta fino a 63 policer di microflusso e fino a 1023 policer aggregati.

D. Quale sistema operativo Catalyst (CatOS) o Multilayer Switch Feature Card (MSFC) è richiesto per il supporto delle policy?

R. Supervisor Engine 1A supporta il controllo degli ingressi in CatOS versione 5.3(1) e successive e nel software Cisco IOS versione 12.0(7)XE e successive.

Supervisor Engine 2 supporta il monitoraggio in entrata in CatOS versione 6.1(1) e successive e

nel software Cisco IOS versione 12.1(5c)EX e successive. Tuttavia, il policy di microflusso è supportato solo nel software Cisco IOS.

D. L'aggiornamento da un Sup2 a un Sup720 è avvenuto e le statistiche sulla velocità del traffico controllato mostrano differenze a seconda dello stesso traffico. Perché?

R. Un cambiamento importante nel controllo del Supervisor Engine 720 è che può contare il traffico per la lunghezza del frame di layer 2. Questa opzione è diversa da Supervisor Engine 1 e Supervisor Engine 2, che contano i frame IP e IPX per la lunghezza del layer 3. Con alcune applicazioni, la lunghezza dei livelli 2 e 3 potrebbe non essere coerente. Un esempio è rappresentato da un piccolo pacchetto di layer 3 all'interno di un frame di layer 2 di grandi dimensioni. In questo caso, Supervisor Engine 720 potrebbe visualizzare una velocità del traffico controllata leggermente diversa rispetto a Supervisor Engine 1 e Supervisor Engine 2.

D. Come è possibile conoscere i valori da utilizzare per la velocità e la frammentazione quando si configura un policer?

A. Questi parametri controllano il funzionamento del token bucket:

- **Rate** - Definisce il numero di token da rimuovere a ogni intervallo. Questo imposta di fatto il tasso di sorveglianza. Tutto il traffico al di sotto della velocità è considerato di profilo.
- **Intervallo** - Definisce la frequenza con cui i token vengono rimossi dal bucket. L'intervallo è fissato a 0,00025 secondi, quindi i token vengono rimossi dal bucket 4.000 volte al secondo. Impossibile modificare l'intervallo.
- **Burst** - Definisce il numero massimo di token che il bucket può contenere contemporaneamente. Per mantenere la velocità di traffico specificata, la velocità di burst non deve essere inferiore alla velocità moltiplicata per l'intervallo. Un'altra considerazione è che il pacchetto di dimensioni massime deve essere contenuto nel bucket.

Utilizzare questa equazione per determinare il parametro di frammentazione:

```
Burst = (rate bps * 0.00025 sec/interval) or (maximum packet size bits) [whichever is greater]
```

Ad esempio, se si desidera calcolare il valore minimo di burst necessario per sostenere una velocità di 1 Mbps su una rete Ethernet, la velocità viene definita come 1 Mbps e la dimensione massima del pacchetto Ethernet è 1518 byte. Questa è l'equazione:

```
Burst = (1,000,000 bps * 0.00025) or (1518 bytes * 8 bits/byte) = 250 or 12144
```

Il risultato più grande è 12144, arrotondato a 13 kbps.

Nota: nel software Cisco IOS, la velocità di controllo è definita in bit al secondo (bps). Nel sistema operativo Catalyst (CatOS), è definito in kbps. Inoltre, nel software Cisco IOS, la velocità di burst è definita in byte, mentre nel software CatOs è definita in kilobit.

Nota: a causa della granularità dei criteri hardware, la velocità e la frammentazione esatte vengono arrotondate al valore supportato più vicino. Accertarsi che il valore di burst non sia inferiore al pacchetto di dimensioni massime. In caso contrario, tutti i pacchetti più grandi delle dimensioni della frammentazione vengono scartati.

Ad esempio, se si tenta di impostare la frammentazione su 1518 nel software Cisco IOS, viene arrotondata a 1000. In questo modo, tutti i frame più grandi di 1000 byte vengono scartati. La soluzione è configurare la frammentazione su 2000.

Quando si configura la velocità di burst, tenere presente che alcuni protocolli, ad esempio TCP, implementano un meccanismo di controllo del flusso che reagisce alla perdita di pacchetti. Ad esempio, il protocollo TCP riduce della metà il tempo di attesa per ciascun pacchetto perso. Di conseguenza, se sottoposto a policy a una determinata frequenza, l'utilizzo effettivo del collegamento è inferiore alla frequenza configurata. È possibile aumentare la frammentazione per ottenere un utilizzo migliore. Un buon inizio per questo tipo di traffico è raddoppiare le dimensioni dello burst. Nell'esempio, le dimensioni della frammentazione vengono aumentate da 13 kbps a 26 kbps. Quindi, monitorare le prestazioni e apportare ulteriori regolazioni se necessario.

Per lo stesso motivo, non è consigliabile eseguire il benchmark dell'operazione del policer con il traffico orientato alla connessione. Questo generalmente mostra prestazioni inferiori a quelle consentite dal policer.

D. Sto configurando QoS su un canale di porta. Ci sono delle restrizioni che devo sapere?

R. Quando si configura QoS sulle porte che fanno parte di un canale porta sul sistema operativo Catalyst (CatOS), è necessario applicare la stessa configurazione a tutte le porte fisiche nel canale porta. I seguenti parametri devono essere compatibili per tutte le porte nel canale della porta:

- Tipo di trust porta
- Tipo di porta di ricezione (2q2t o 1p2q2t)
- Tipo di porta di trasmissione (1q4t o 1p1q4t)
- CoS (Port Class of Service) predefinito
- QoS basata su porta o VLAN
- Access Control List (ACL) o una coppia di protocolli trasportati dalla porta

D. Perché non è possibile regolare il valore della soglia minima?

R. Nelle versioni del sistema operativo Catalyst (CatOS) precedenti alla 6.2, il comando WRED (weighted random early detection) imposta solo il valore di max-threshold, mentre il valore di min-threshold è hardcoded su 0%. Questa condizione viene corretta in CatOS 6.2 e versioni successive, che consentono la configurazione del valore di soglia minima. La soglia minima predefinita dipende dalla precedenza. La soglia minima per la precedenza IP 0 corrisponde alla metà della soglia massima. I valori delle precedenti che rimangono sono compresi tra la metà della soglia max e la soglia max a intervalli regolari.

D. Non è possibile regolare i buffer della coda di trasmissione. Ci sono delle restrizioni?

R. Se si dispone di tre code (1p2q2t), la coda WRR (High Priority Weighted Round-Robin) e la coda con priorità rigorosa devono essere impostate allo stesso livello.

D: Ho una scheda di linea 62xx/63xx. Impossibile applicare il comando set che considera attendibile il punto di codice dei servizi differenziati (DSCP) su una porta.

Esiste un limite su questa scheda di linea per le funzionalità QoS?

R. Sì, perché non è possibile eseguire i comandi **trust-dscp**, **trust-ipprec** o **trust-cos** sulle schede di linea WS-X6248-xx, WS-X6224-xx e WS-X6348-xx. Il metodo più semplice in questo caso è lasciare tutte le porte non attendibili e modificare l'elenco di controllo di accesso (ACL) predefinito con il comando **trust-dscp**:

```
set qos enable

set port qos 2/1-16 trust untrusted

set qos acl default-action ip trust-dscp
```

Per ulteriori informazioni sulle limitazioni specifiche delle schede di linea WS-X6248-xx, WS-X6224-xx e WS-X6348-xx, consultare la sezione Classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS.

D. Quali versioni e supervisori del sistema operativo Catalyst (CatOS) sono richiesti per supportare il monitoraggio?

R. Il Supervisor Engine 1A supporta il controllo degli ingressi in CatOS versione 5.3(1) e successive e nel software Cisco IOS versione 12.0(7)XE e successive.

Nota: per il controllo con Supervisor Engine 1A è necessaria una scheda secondaria PFC (Policy Feature Card).

Supervisor Engine 2 supporta il monitoraggio in entrata in CatOS versione 6.1(1) e successive e nel software Cisco IOS versione 12.1(5c)EX e successive. Supervisor Engine 2 supporta il parametro di controllo della velocità in eccesso.

Supervisor 720 supporta il controllo degli ingressi a livello di porta e di interfaccia VLAN. Per ulteriori informazioni sulle funzionalità di policy di Sup720, fare riferimento alla sezione Aggiornamento delle funzionalità di policy per Supervisor Engine 720 di QoS Policing sugli switch Catalyst serie 6500/6000.

D. Cosa devo sapere sulla configurazione di QoS su EtherChannel?

R. Quando si configura QoS su una porta che fa parte di EtherChannel su CatOS, è necessario configurarla sempre per ciascuna porta. Inoltre, è necessario assicurarsi di applicare la stessa configurazione QoS a tutte le porte, in quanto EtherChannel può includere solo porte con le stesse configurazioni QoS. Ciò significa che è necessario configurare gli stessi parametri:

- Tipo di trust porta
- Tipo di porta di ricezione (2q2t o 1p2q2t)
- Tipo di porta di trasmissione (1q4t o 1p1q4t)
- CoS (Port Class of Service) predefinito
- QoS basata su porta o VLAN
- Access Control List (ACL) o una coppia di protocolli trasportati dalla porta

D. Dove posso trovare esempi sull'uso degli Access Control List (ACL) QoS per contrassegnare o controllare il traffico?

A. Fare riferimento al caso 1: Contrassegno nella sezione Edge della classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS, per un esempio di contrassegno del traffico.

Per un esempio di policy sul traffico, consultare la sezione Configurazione e monitoraggio del policy nel software CatOS degli switch Catalyst serie 6500/6000.

D. Qual è la differenza tra gli Access Control List (ACL) QoS basati su porta e quelli basati su VLAN?

R. Ciascun ACL QoS può essere applicato a una porta o a una VLAN, ma è disponibile un parametro di configurazione aggiuntivo di cui tenere conto: il tipo di porta ACL. Una porta può essere configurata per essere basata su VLAN o su porta. Esistono due tipi di configurazione:

1. Se una porta VLAN con un ACL applicato viene assegnata a una VLAN a cui è associato anche un ACL, l'ACL basato sulla VLAN ha priorità sull'ACL basato sulla porta.
2. Se una porta basata su una porta con un ACL applicato viene assegnata a una VLAN a cui è associato anche un ACL, l'ACL basato sulla porta ha priorità sull'ACL basato sulla VLAN.

Per ulteriori informazioni, vedere Quale delle quattro possibili origini per il DSCP interno verrà utilizzato? per ulteriori informazioni, consultare la sezione Classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS.

D. Qual è il valore tipico delle dimensioni di burst da utilizzare per la limitazione della velocità sugli switch di layer 3?

A. Gli switch di layer 3 implementano un'approssimazione dell'algoritmo a bucket singolo nel firmware. Una dimensione di burst ragionevole per l'intervallo di velocità del traffico è di circa 64000 byte. Le dimensioni della frammentazione devono includere almeno un pacchetto di dimensioni massime. Con ciascun pacchetto in arrivo, l'algoritmo di controllo determina l'intervallo di tempo tra il pacchetto e l'ultimo pacchetto e calcola il numero di token generati durante il tempo trascorso. Quindi, aggiunge questo numero di token al bucket e determina se il pacchetto in arrivo è conforme o supera i parametri specificati.

D. Perché ricevo prestazioni inferiori per il traffico TCP con limitazione della velocità?

R. Le applicazioni TCP non funzionano correttamente quando i pacchetti vengono scartati a causa della limitazione della velocità. Ciò è dovuto allo schema a finestre intrinseco utilizzato nel controllo del flusso. È possibile regolare il parametro relativo alla dimensione della frammentazione o alla velocità per ottenere il throughput richiesto.

D. Qual è il vantaggio di WRED (Weighted Random Early Detection) e come è possibile stabilire se la scheda di linea supporta WRED?

R. Per evitare le congestioni nella pianificazione dell'output, lo switch Catalyst 6500 (Cat6K) supporta WRED su alcune code in uscita. Ogni coda ha una dimensione e una soglia configurabili.

Alcuni hanno WRED. WRED è un meccanismo di prevenzione della congestione che scarta in modo casuale i pacchetti con una certa precedenza IP quando i buffer raggiungono una determinata soglia di riempimento. WRED è una combinazione di due funzioni: tail drop e random early detection (RED). L'implementazione del primo sistema operativo Catalyst (CatOS) di WRED ha impostato solo la soglia massima, mentre la soglia minima è stata hardcoded su 0%. La probabilità di perdita per un pacchetto è sempre non null, in quanto supera sempre la soglia minima. Questo comportamento viene corretto in CatOS 6.2 e versioni successive. WRED è un meccanismo molto utile per evitare le congestioni quando il tipo di traffico è basato su TCP. Per altri tipi di traffico, il protocollo RED non è molto efficiente in quanto il protocollo RED sfrutta il meccanismo a finestre utilizzato dal protocollo TCP per gestire la congestione.

Per stabilire se una scheda di linea o la struttura della coda possono supportare WRED, fare riferimento alla sezione Descrizione della funzionalità di coda di una porta di QoS Output Scheduling sugli switch Catalyst serie 6500/6000 con software CatOS. È possibile anche usare il comando **show port capabilities** per verificare la struttura della coda della scheda di linea.

D. Qual è il punto di codice interno dei servizi differenziati (DSCP)?

R. A ciascun frame è assegnata una classe di servizio interna (CoS), sia quella ricevuta sia quella predefinita. Sono incluse le cornici senza tag che non hanno un CoS reale. Questo CoS interno e il DSCP ricevuto vengono scritti in un'intestazione speciale del pacchetto (chiamata intestazione del bus di dati) e inviati al motore di commutazione tramite il bus di dati. Ciò accade nella scheda in entrata. A questo punto, non è ancora noto se questo CoS interno venga trasportato nel circuito integrato specifico dell'applicazione in uscita (ASIC) e inserito nel frame in uscita. Quando l'intestazione raggiunge il motore di commutazione, la logica di riconoscimento degli indirizzi codificati (EARL, Encoded Address Recognition Logic) assegna a ciascun frame un DSCP interno. Questo DSCP interno è una priorità interna assegnata al frame dalla Policy Feature Card (PFC) durante il transito sullo switch. Questo non è il DSCP nell'intestazione IPv4. Deriva da un'impostazione CoS o Type of service (ToS) esistente e viene utilizzata per ripristinare il CoS o il ToS all'uscita del frame dallo switch. Questo DSCP interno viene assegnato a tutti i frame commutati (o instradati) dal PFC, anche ai frame non IP.

D. Quali sono le possibili fonti del DSCP (Differentiated Services Code Point) interno?

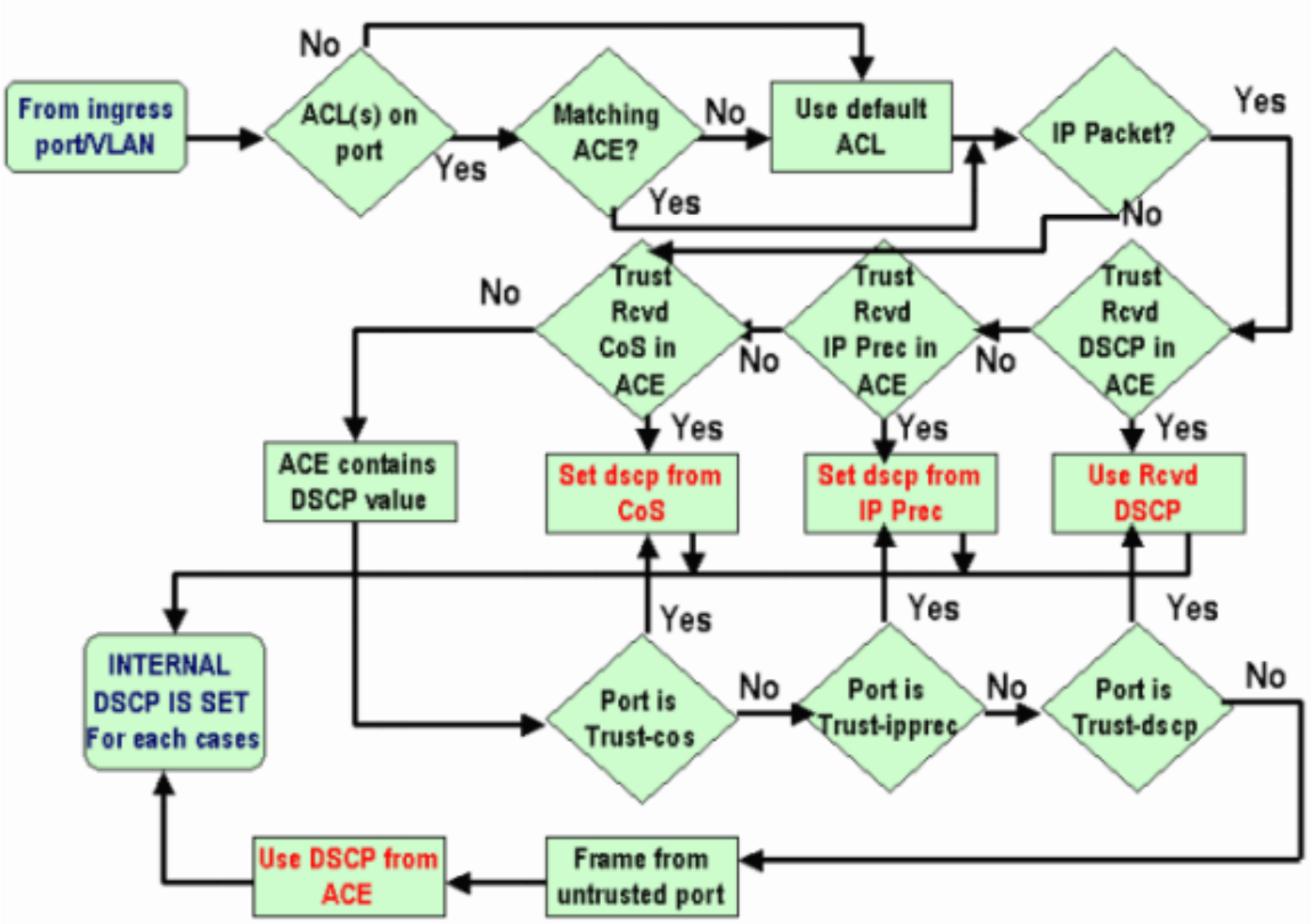
A. Fare riferimento alla sezione Quattro possibili origini per il DSCP interno di Classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS.

D. Come viene scelto il DSCP (Differentiated Services Code Point) interno?

R. Il DSCP interno dipende da questi fattori:

- Stato trust porta
- Access Control List (ACL) collegato alla porta
- ACL predefinito
- Basato su VLAN o su porta, per quanto riguarda l'ACL

Questo diagramma di flusso riepiloga come viene scelto il DSCP interno in base alla configurazione:



D. Lo switch Catalyst 6500 (Cat6K) supporta il protocollo CBWFQ (Class-Based Weighted Fair Queuing) o LLQ (Low Latency Queuing)?

R. Sì, CBWFQ consente di definire una classe di traffico e assegnarle una garanzia di larghezza di banda minima. L'algoritmo alla base di questo meccanismo è WFQ (Weighted Fair Queuing), che spiega il nome. Per configurare CBWFQ, è necessario definire classi specifiche nelle istruzioni map-class. Assegnare quindi un criterio a ogni classe in una mappa dei criteri. Questa mappa dei criteri viene quindi collegata al traffico in entrata/in uscita di un'interfaccia.

D. Il valore CoS (Class of Service) di layer 2 viene mantenuto per i pacchetti indirizzati?

R. Sì, il DSCP (Differentiated Services Code Point) interno viene utilizzato per reimpostare il CoS sui frame in uscita.

D. QoS applica la stessa configurazione a tutte le porte LAN controllate dallo stesso ASIC?

R. Sì, quando questi comandi sono configurati, QoS applica la stessa configurazione a tutte le porte LAN/routing controllate dallo stesso ASIC (Application Specific Integrated Circuit). Le impostazioni QoS vengono propagate alle altre porte che appartengono allo stesso ASIC, a prescindere dal fatto che la porta sia una porta di accesso, una porta trunk o una porta indirizzata.

- rcv-queue-random-detect

- **rcv-queue-limit**
- **wrr-queue-limit**
- **larghezza di banda della coda di lavoro** (ad eccezione delle porte LAN Gigabit Ethernet)
- **priority-queue-cos-map**
- **rcv-queue-cos-map**
- **wrr-queue-cos-map**
- **soglia della coda di lavoro**
- **soglia coda rcv**
- **wrr-queue random-detect**
- **wrr-queue random-detect soglia minima**
- **wrr-queue random-detect max-threshold**

Quando il comando **default *interface*** viene eseguito su una delle porte, l'ASIC che controlla la porta specifica reimposta la configurazione QoS per tutte le porte da essa controllate.

D. Perché il comando show traffic-shape statistics non restituisce risultati positivi anche se il traffic shapping in è configurato?

```
Router#show traffic-shape statistics
          Access Queue     Packets   Bytes     Packets   Bytes     Shaping
I/F       List   Depth                        Delayed   Delayed   Active
Et0       101    0         2         180       0         0         no
Et1              0         0         0         0         0         no
```

R. L'attributo Shaping Active ha il valore **yes** quando i timer indicano che il traffic shaping ha luogo e **no** se il traffic shaping non ha luogo.

Per verificare se il traffico configurato funziona, è possibile usare il comando **show policy-map**.

```
Router#show policy-map
  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)
  Policy Map MQC-SHAPE-LLQ1
    Class class-default
      Traffic Shaping
         Average Rate Traffic Shaping
                 CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
                 Adapt to 8000 (bps)
                 Voice Adapt Deactivation Timer 30 Sec
      service-policy VSD1
```

D. Catalyst 6500 PFC supporta tutti i comandi QoS standard?

R. Cisco Catalyst 6500 PFC QoS ha alcune restrizioni e non supporta alcuni comandi relativi a QoS. Per un elenco completo dei comandi non supportati, consultare i seguenti documenti.

- Restrizioni comando mappa classi
- Restrizioni comandi mappa criteri

- Restrizioni comando classe mappa criteri

D. Perché i contatori CoPP software sono più grandi dei contatori CoPP hardware?

R. I contatori CoPP (Software Control Plane Policing) sono la somma dei pacchetti che attraversano il protocollo CoPP e la limitazione della velocità dell'hardware. I pacchetti vengono prima gestiti da limitatori di velocità hardware e, se non corrispondono, il CoPP hardware viene rappresentato. Se il limitatore di velocità hardware consente i pacchetti, il pacchetto viene inviato al software dove viene elaborato dal programma CoPP del software. A causa di questo software, CoPP può essere più grande dei contatori CoPP hardware.

Esistono inoltre alcune limitazioni per le quali CoPP non è supportato nell'hardware. Alcuni di essi sono:

- CoPP non è supportato nell'hardware per i pacchetti multicast. La combinazione di ACL, limitatori di velocità della CPU multicast e protezione software CoPP assicura la protezione dagli attacchi DoS multicast.
- CoPP non è supportato nell'hardware per i pacchetti broadcast. La combinazione di ACL, controllo delle tempeste di traffico e protezione software CoPP assicura la protezione contro gli attacchi DoS broadcast.
- Le classi che corrispondono a multicast non vengono applicate nell'hardware ma nel software.
- Il protocollo CoPP non è abilitato nell'hardware a meno che QoS MLS non sia abilitato globalmente con il comando **mls qos**. Se il comando **mls qos** non viene immesso, il protocollo CoPP funziona solo nel software e non fornisce alcun vantaggio per l'hardware.

per ulteriori informazioni, fare riferimento a Configurazione di Control Plane Policing (CoPP).

D. La configurazione del comando QoS predefinito (interfaccia) funziona su altre interfacce/porte?

A. Quando si esegue il comando **default *interface*, viene raccolta la configurazione non predefinita, simile a quella visualizzata in show running-config interface x/y** , e ognuna di esse viene impostata sui relativi valori predefiniti. Anche questa può essere una semplice negazione di un comando.

Se sull'interfaccia sono configurate QoS o altre funzionalità e questi comandi vengono negati, possono essere propagati ad altre interfacce della scheda di linea.

si consiglia di controllare l'output del comando **show interface *x/y* capabilities** prima di procedere con l'impostazione predefinita di un'interfaccia. Fare riferimento alla sezione QoS applica la stessa configurazione a tutte le porte LAN controllate dallo stesso ASIC? per ulteriori informazioni.

L'output del comando **default *interface*** visualizza anche (se presenti) altre interfacce interessate da QoS e da altre funzionalità implementate nell'ASIC della porta.

D. È possibile configurare QoS in un'interfaccia con IP secondario?

R. Sì. È possibile configurare QoS su un IP secondario.

Informazioni correlate

- Pianificazione dell'output QoS sugli switch Catalyst serie 6500/6000 con software CatOS
- Classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS
- Policing QoS sugli switch Catalyst serie 6500/6000
- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems