Conoscenza delle funzionalità QoS sugli switch della famiglia Catalyst 6000

Sommario

Introduzione

Questo documento illustra le funzionalità QoS (Quality of Service) disponibili sugli switch Catalyst serie 6000. Questo documento descrive le funzionalità di configurazione QoS e fornisce alcuni esempi di come è possibile implementare QoS.

Questo documento non deve essere una guida alla configurazione. Nel presente documento vengono utilizzati esempi di configurazione per illustrare le funzionalità QoS dell'hardware e del software della famiglia Catalyst 6000. Per la sintassi di riferimento delle strutture di comando QoS, consultare le seguenti guide di configurazione e comando per la famiglia Catalyst 6000:

- Catalyst serie 6500 Switch

Definizione di QoS di layer 2

Anche se molti possono pensare che QoS negli switch di layer 2 (L2) significhi semplicemente dare la priorità ai frame Ethernet, pochi si rendono conto che comporta molto di più. QoS L2 comporta quanto segue:

1. **Programmazione delle code di input:** quando il frame entra nella porta, può essere assegnato a una delle code basate su porta prima di essere pianificato per la commutazione a una porta di uscita. In genere, vengono utilizzate code multiple quando traffico diverso richiede livelli di servizio diversi o quando la latenza dello switch deve

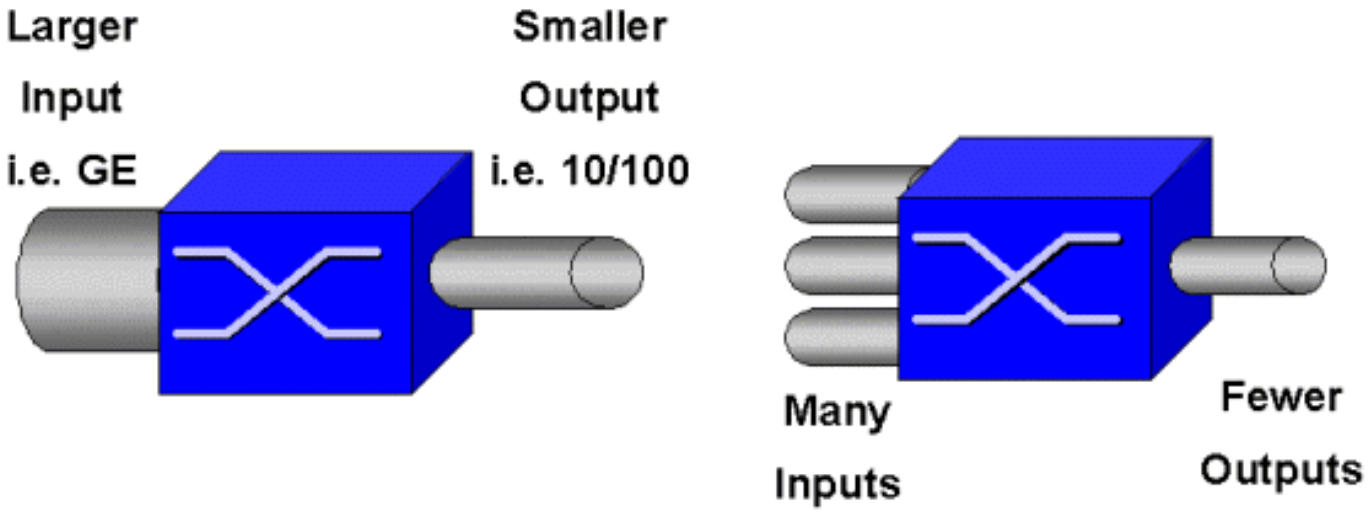
essere ridotta al minimo. Ad esempio, i dati vocali e video basati su IP richiedono una bassa latenza, quindi potrebbe essere necessario modificare questi dati prima di passare ad altri, quali FTP (File Transfer Protocol), Web, e-mail, Telnet e così via.

2. **Classificazione:** il processo di classificazione comporta l'ispezione di diversi campi nell'intestazione Ethernet L2, insieme ai campi nell'intestazione IP (Layer 3 (L3)) e nell'intestazione TCP/UDP (Transmission Control Protocol/User Datagram Protocol) (Layer 4 (L4)), per aiutare a determinare il livello di servizio che verrà applicato al frame durante il transito sullo switch.
3. **Traffic policing:** il policing è il processo di ispezione di un frame Ethernet per verificare se ha superato una velocità di traffico predefinita in un determinato intervallo di tempo (in genere, questo intervallo di tempo è un numero fisso interno allo switch). Se il frame è fuori profilo, ovvero fa parte di un flusso di dati che supera il limite di velocità predefinito, è possibile eliminarlo o contrassegnare il valore CoS (Class of Service).
4. **Riscrittura:** il processo di riscrittura consiste nella capacità dello switch di modificare il CoS nell'intestazione Ethernet o i bit del tipo di servizio (ToS) nell'intestazione IPV4.
5. **Programmazione coda di output:** dopo i processi di riscrittura, lo switch inserisce il frame Ethernet in una coda in uscita (in uscita) appropriata per lo switching. Lo switch eseguirà la gestione del buffer su questa coda verificando che il buffer non sia in overflow. In genere, questo avviene utilizzando un algoritmo Random Early Discard (RED), in base al quale i fotogrammi casuali vengono rimossi dalla coda. Il Weighted RED (WRED) è un derivato del RED (usato da alcuni moduli della famiglia Catalyst 6000), per cui i valori CoS vengono ispezionati per determinare quali frame verranno scartati. Quando i buffer raggiungono le soglie predefinite, i frame con priorità inferiore vengono in genere eliminati, mantenendo i frame con priorità più alta nella coda.

Questo documento illustra in dettaglio i singoli meccanismi e le loro relazioni con la famiglia Catalyst 6000 nelle sezioni seguenti.

Esigenza di QoS in uno switch

Al giorno d'oggi, molti switch usano backplane ingenti, milioni di pacchetti scambiati al secondo e switch non bloccanti. Perché è necessario QoS? La risposta è a causa della congestione.



Uno switch può essere lo switch più veloce al mondo, ma se si verifica uno dei due scenari illustrati nella figura precedente, lo switch subirà una congestione. Nei momenti di congestione, se le funzionalità di gestione delle congestioni non sono disponibili, i pacchetti verranno scartati.

Quando i pacchetti vengono scartati, si verificano ritrasmissioni. Quando si verificano ritrasmissioni, il carico di rete può aumentare. Nelle reti già congestionate, ciò può causare problemi di prestazioni e ridurre ulteriormente le prestazioni.

Con le reti convergenti, la gestione della congestione è ancora più critica. Il traffico sensibile alla latenza, come quello vocale e video, può subire un grave impatto in caso di ritardi. Inoltre, la semplice aggiunta di più buffer a uno switch non riduce necessariamente i problemi di congestione. Il traffico sensibile alla latenza deve essere commutato il più rapidamente possibile. Innanzitutto, è necessario identificare questo traffico importante tramite tecniche di classificazione e quindi implementare le tecniche di gestione dei buffer per evitare che il traffico con priorità superiore venga scartato durante la congestione. Infine, è necessario incorporare tecniche di pianificazione per passare il più rapidamente possibile pacchetti importanti dalle code. Come potrete leggere in questo documento, la famiglia Catalyst 6000 implementa tutte queste tecniche, rendendo il sottosistema QoS uno dei più completi del settore.

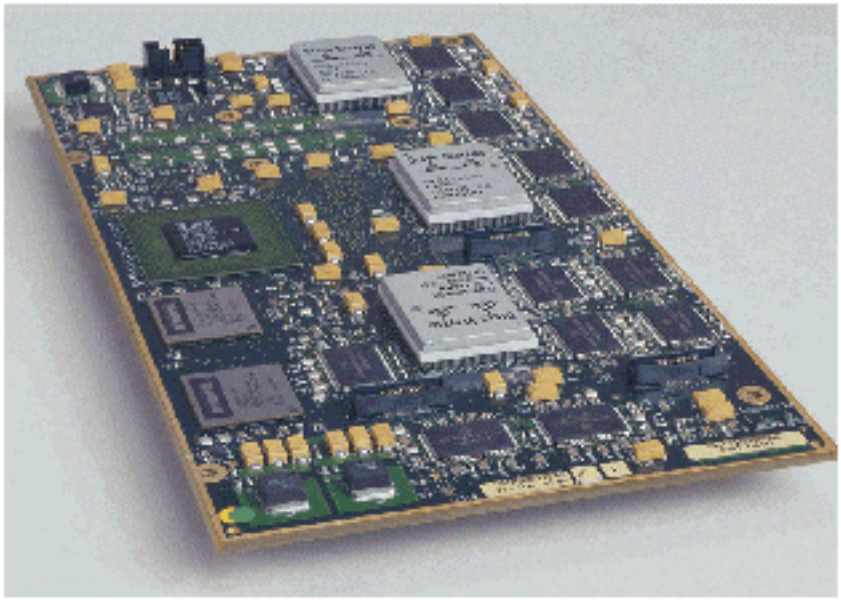
Tutte le tecniche QoS descritte nella sezione precedente verranno esaminate più dettagliatamente in questo documento.

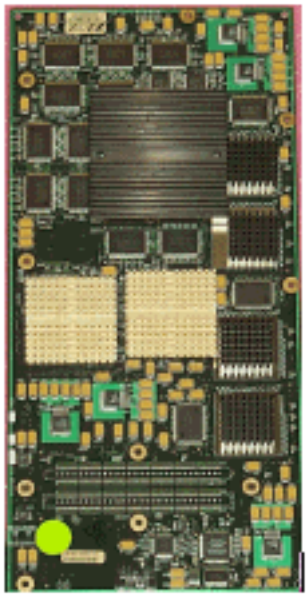
Supporto hardware per QoS nella famiglia Catalyst 6000

Per supportare QoS nella famiglia Catalyst 6000, è necessario disporre di un supporto hardware specifico. L'hardware che supporta QoS include il modulo Multilayer Switch Feature Card (MSFC), la Policy Feature Card (PFC) e i circuiti integrati specifici delle porte (ASIC) sulle schede di linea stesse. In questo documento non verranno esaminate le funzionalità QoS dell'MSFC, ma ci si concentrerà sulle funzionalità QoS del PFC e degli ASIC sulle schede di linea.

PFC

La PFC versione 1 è una scheda secondaria che si trova sul Supervisor I (SupI) e sul Supervisor IA (SupIA) della famiglia Catalyst 6000. Il PFC2 è una nuova rotazione del PFC1 e viene fornito con il nuovo Supervisor II (SupII) e alcuni nuovi ASIC integrati. Sebbene sia PFC1 che PFC2 siano principalmente noti per l'accelerazione hardware della commutazione L3, QoS è uno degli altri scopi. Di seguito sono riportati i PFC.





Mentre il PFC 1 e il PFC2 sono essenzialmente gli stessi, esistono alcune differenze nelle funzionalità QoS. In particolare, il PFC2 aggiunge quanto segue:

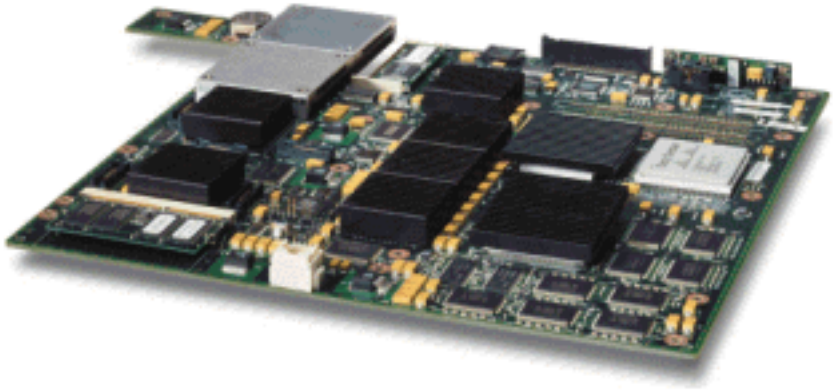
1. La capacità di spingere i criteri QoS verso un DFC (Distributed Forwarding Card).
2. Le decisioni di sorveglianza sono leggermente diverse. Sia PFC1 che PFC2 supportano il normale controllo in base al quale i frame vengono eliminati o contrassegnati se un criterio di aggregazione o microflusso restituisce una decisione fuori profilo. Tuttavia, il PFC2 aggiunge il supporto per un tasso in eccesso, il che indica un secondo livello di policing al quale è possibile intraprendere azioni politiche.

Quando viene definito un policer di velocità in eccesso, i pacchetti possono essere ignorati o contrassegnati quando superano la velocità in eccesso. Se viene impostato un livello di polizia in eccesso, il mapping DSCP in eccesso viene utilizzato per sostituire il valore DSCP originale con un valore contrassegnato. Se viene impostato solo un livello di polizia normale, viene utilizzata la mappatura DSCP normale. Il livello di polizia in eccesso avrà la precedenza per la selezione delle regole di mappatura quando sono impostati entrambi i livelli di polizia.

Èimportante notare che le funzioni QoS descritte in questo documento eseguite dagli ASIC citati offrono elevati livelli di prestazioni. Le prestazioni QoS di una famiglia Catalyst 6000 di base (senza modulo fabric switch) garantiscono 15 MPPS. Se si utilizzano DFC, è possibile ottenere ulteriori miglioramenti delle prestazioni per QoS.

DFC

Èpossibile collegare il DFC al WS-X6516-GBIC come opzione. Si tratta tuttavia di uno staffaggio standard della scheda WS-X6816-GBIC. Può essere supportato anche su altre future schede di linea fabric, come la scheda di linea 10/100 (WS-X6548-RJ45) di recente introduzione, la scheda di linea RJ21 di fabric (WS-X6548-RJ21) e la scheda di linea 100FX (WS-X6524-MM-FX). La DFC è illustrata di seguito.



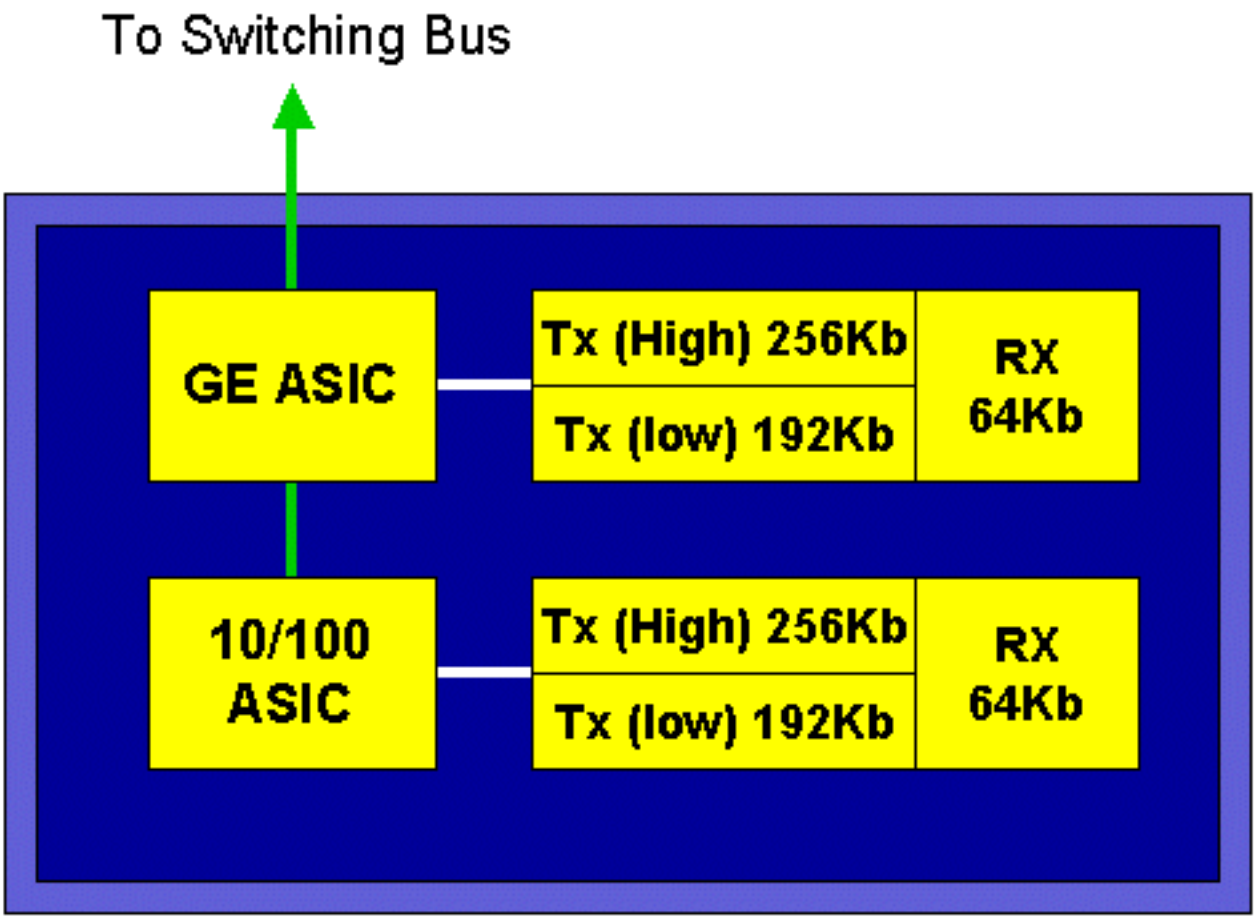
La DFC consente alla scheda di linea fabric (collegata a crossbar) di eseguire la commutazione locale. A tale scopo, deve supportare anche i criteri QoS definiti per lo switch. L'amministratore non può configurare direttamente DFC; al contrario, è sotto il controllo del master MSFC/PFC sul supervisore attivo. Il PFC primario esegue il push di una tabella Forwarding Information Base (FIB), che fornisce alla DFC le tabelle di inoltro L2 e L3. Inoltre, spingerà verso il basso una copia delle politiche QoS in modo che siano anche locali alla scheda di linea. Successivamente, le decisioni di switching locale possono fare riferimento alla copia locale di qualsiasi policy QoS che fornisce velocità di elaborazione QoS per l'hardware e fornisce livelli di prestazioni più elevati tramite switching distribuito.

ASIC basati sulle porte

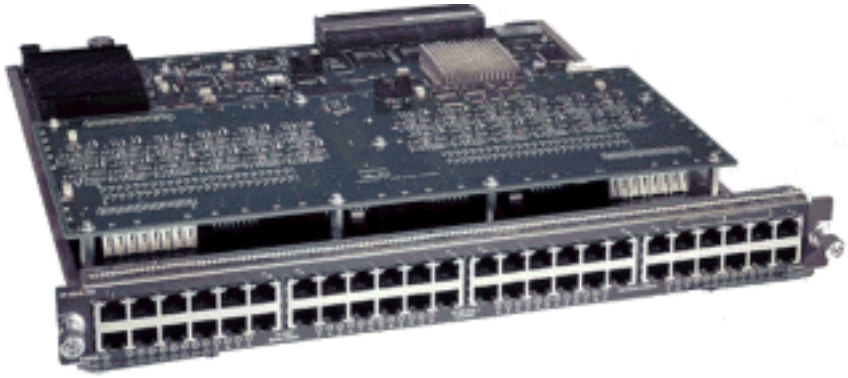
Per completare l'immagine dell'hardware, ciascuna scheda di linea implementa una serie di ASIC. Questi ASIC implementano le code, il buffering e le soglie utilizzate per la memorizzazione temporanea dei frame durante il transito sullo switch. Sulle schede 10/100, viene utilizzata una combinazione di ASIC per il provisioning delle 48 porte 10/100.

Schede di linea 10/100 originali (WS-X6348-RJ45)

Gli ASIC 10/100 forniscono una serie di code di ricezione (Rx) e trasmissione (TX) per ciascuna porta 10/100. Gli ASIC offrono buffer a 128 K per porta 10/100. Per ulteriori informazioni sul buffer per porta disponibile su ciascuna scheda di linea, consultare le note sulla versione. Ogni porta su questa scheda di linea supporta una coda Rx e due code TX indicate come alta e bassa. come mostrato nel diagramma sottostante.



Nel diagramma riportato sopra, ogni ASIC 10/100 fornisce un'interruzione per 12 porte 10/100. Per ciascuna porta 10/100, vengono forniti buffer da 128 K. I 128 K di buffer vengono suddivisi tra ciascuna delle tre code. Le figure mostrate nella coda precedente non sono le impostazioni predefinite, tuttavia, sono piuttosto una rappresentazione di ciò che potrebbe essere configurato. La singola coda Rx ottiene 16 K e la memoria rimanente (112 K) viene suddivisa tra le due code Tx. Per impostazione predefinita (in CatOS), la coda alta ottiene il 20% di questo spazio e la coda bassa l'80%. Per impostazione predefinita, in Catalyst IOS alla coda alta viene assegnato il 10% e alla coda bassa il 90%.

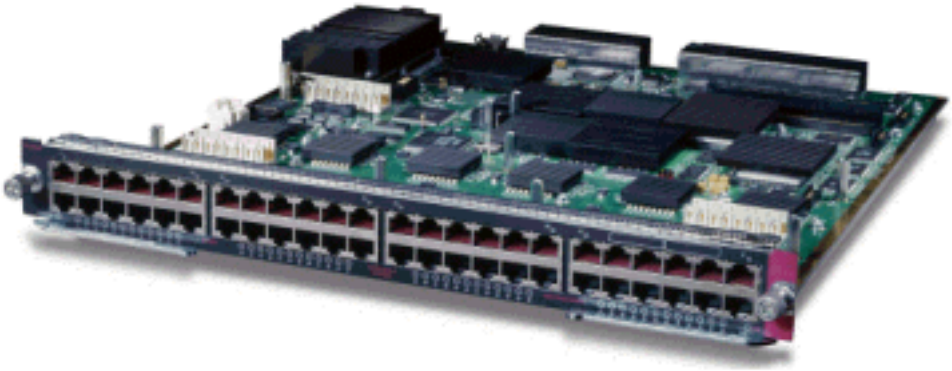


Mentre la scheda fornisce un buffering a due fasi, solo il buffering 10/100 ASIC è disponibile per essere manipolato durante la configurazione QoS.

Schede di linea 10/100 fabric (WS-X6548-RJ45)

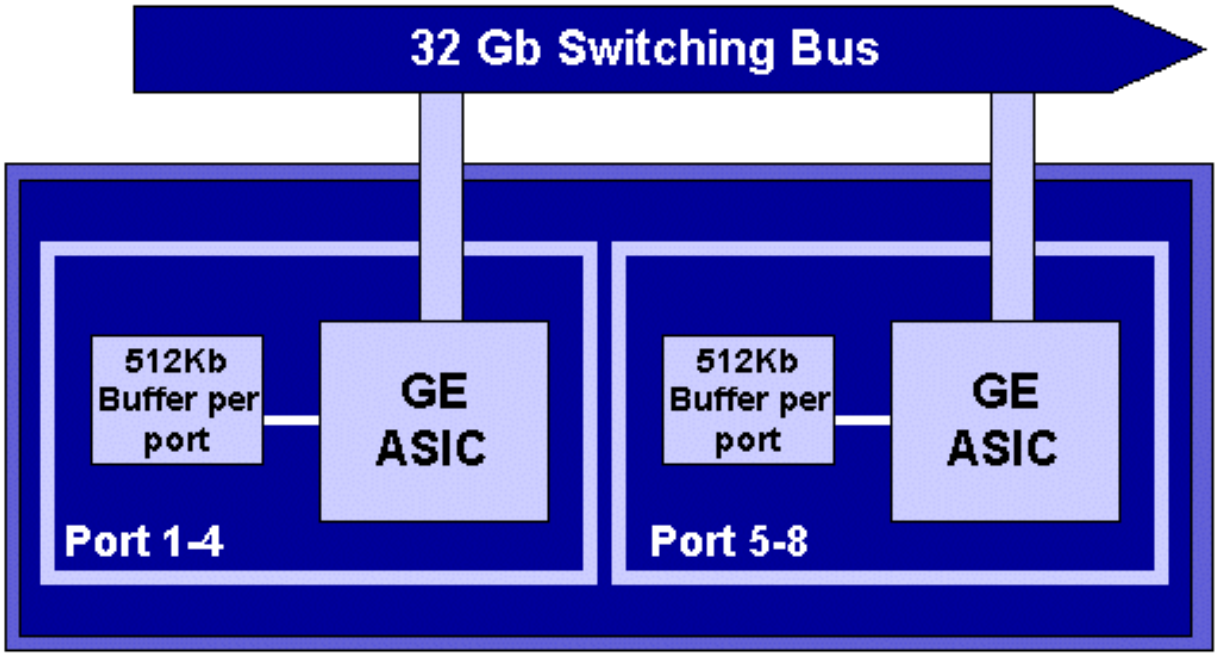
I nuovi ASIC 10/100 forniscono una serie di code Rx e TX per ciascuna porta 10/100. Gli ASIC forniscono un pool condiviso di memoria disponibile sulle porte 10/100. Per ulteriori informazioni sul buffer per porta disponibile su ciascuna scheda di linea, consultare le note sulla versione. Ogni

porta su questa scheda di linea supporta due code Rx e tre code TX. Una coda Rx e una coda TX sono indicate ciascuna come coda con priorità assoluta. Funziona come una coda a bassa latenza, ideale per il traffico sensibile alla latenza come il traffico Voice over IP (VoIP).

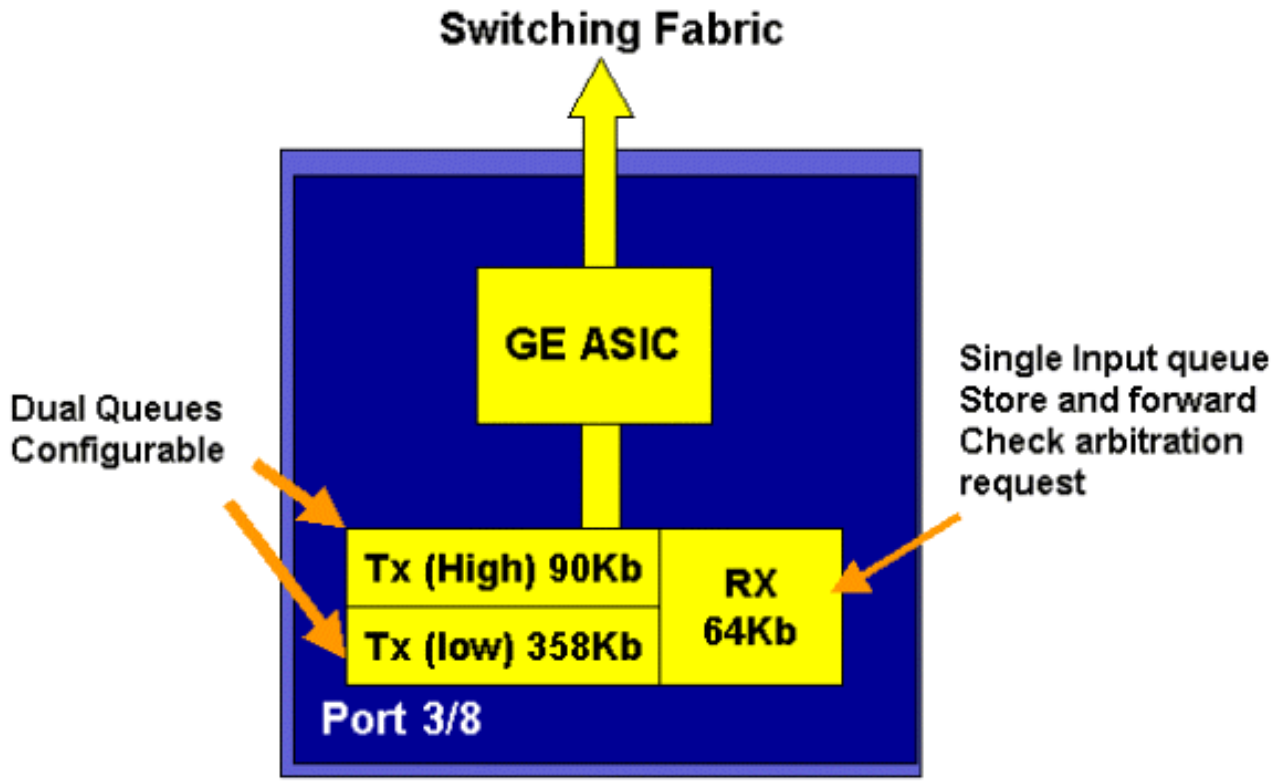


Schede di linea GE (WS-X6408A, WS-X6516, WS-X6816)

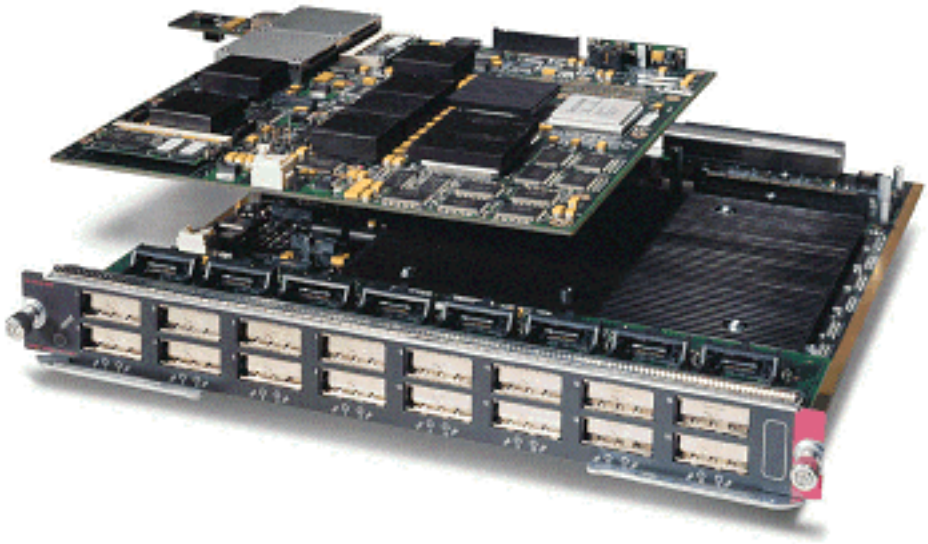
Per le schede di linea GE, l'ASIC fornisce 512 K di buffer per porta. Una rappresentazione della scheda di linea GE a otto porte è illustrata nel diagramma seguente.



Come per le porte 10/100, ciascuna porta GE ha tre code, una Rx e due code TX. Questa è l'impostazione predefinita della scheda di linea WS-X6408-GBIC ed è mostrata nel diagramma sottostante.



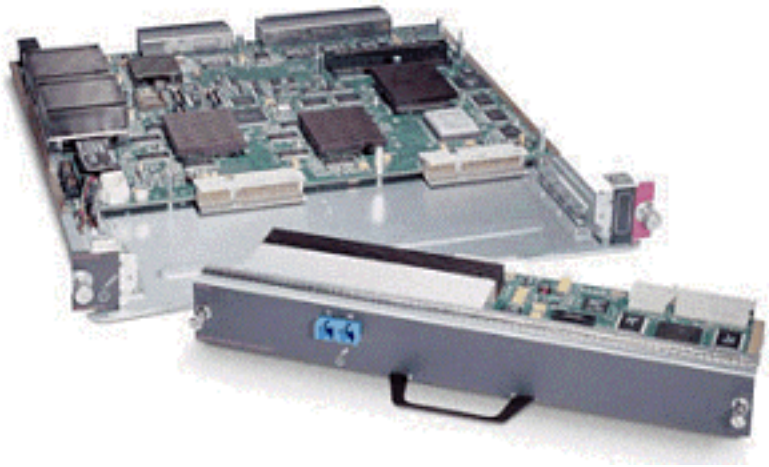
Sulla nuova linea schede GE a 16 porte, le porte GBIC su SupIA e SupII e la scheda GE a 8 porte WS-X6408A-GBIC, vengono fornite due code SP (Strict Priority) aggiuntive. Una coda SP viene assegnata come coda Rx e l'altra come coda TX. Questa coda SP viene utilizzata principalmente per l'accodamento del traffico sensibile alla latenza, ad esempio la voce. Con la coda SP, tutti i dati inseriti in questa coda verranno elaborati prima dei dati nelle code alta e bassa. Solo quando la coda SP è vuota le code alta e bassa saranno servite.



Schede di linea 10 GE (WS-X6502-10GE)

Nella seconda metà del 2001, Cisco ha introdotto una serie di schede di linea 10 GE che forniscono una porta di 10 GE per scheda di linea. Questo modulo occupa uno slot dello chassis 6000. La scheda di linea 10 GE supporta QoS. Per la porta 10 GE, fornisce due code Rx e tre code TX. Una coda Rx e una coda TX sono designate ciascuna come coda SP. Per la porta è inoltre disponibile il buffering, per un totale di 256 K di buffering Rx e 64 MB di buffering TX.

Questa porta implementa una struttura di coda 1p1q8t per il lato Rx e una struttura di coda 1p2q1t per il lato TX. Le strutture delle code sono descritte più avanti in questo documento.



Riepilogo dell'hardware QoS per la famiglia Catalyst 6000

Nella tabella seguente vengono descritti in dettaglio i componenti hardware che eseguono le funzioni QoS descritte in precedenza nella famiglia Catalyst 6000.

QoS Process	Catalyst 6500 Component that performs function
Input Scheduling	Performed by port ASIC's L2 only with or without the PFC
Classification	Performed by Supervisor or PFC L2 only is done by Supervisor L2/3 is done by PFC
Policing	Done by PFC via L3 forwarding Engine
Packet Re-write	Done by port ASIC's L2/L3 based on classification done in point 2 above
Output Scheduling	Done by port ASIC's L2/L3 based on classification done in point 2 above

Supporto software della famiglia Catalyst 6000 per QoS

La famiglia Catalyst 6000 supporta due sistemi operativi. La piattaforma software originale, CatOS, è stata derivata dalla base di codice utilizzata sulla piattaforma Catalyst 5000. Più recentemente, Cisco ha introdotto Cisco IOS ® (modalità nativa) integrata (in precedenza nota come Native IOS), che utilizza una base di codice derivata dal router IOS Cisco. Entrambe le piattaforme OS (CatOS e Cisco IOS (modalità nativa) integrata) implementano il supporto software per abilitare la funzionalità QoS sulla piattaforma della famiglia di switch Catalyst 6000 usando l'hardware descritto nelle sezioni precedenti.

Nota: In questo documento vengono usati esempi di configurazione di entrambe le piattaforme del sistema operativo.

Meccanismi di priorità in IP e Ethernet

Per applicare un servizio QoS ai dati, è necessario creare un tag o assegnare una priorità a un pacchetto IP o a un frame Ethernet. A tale scopo, vengono utilizzati i campi ToS e CoS.

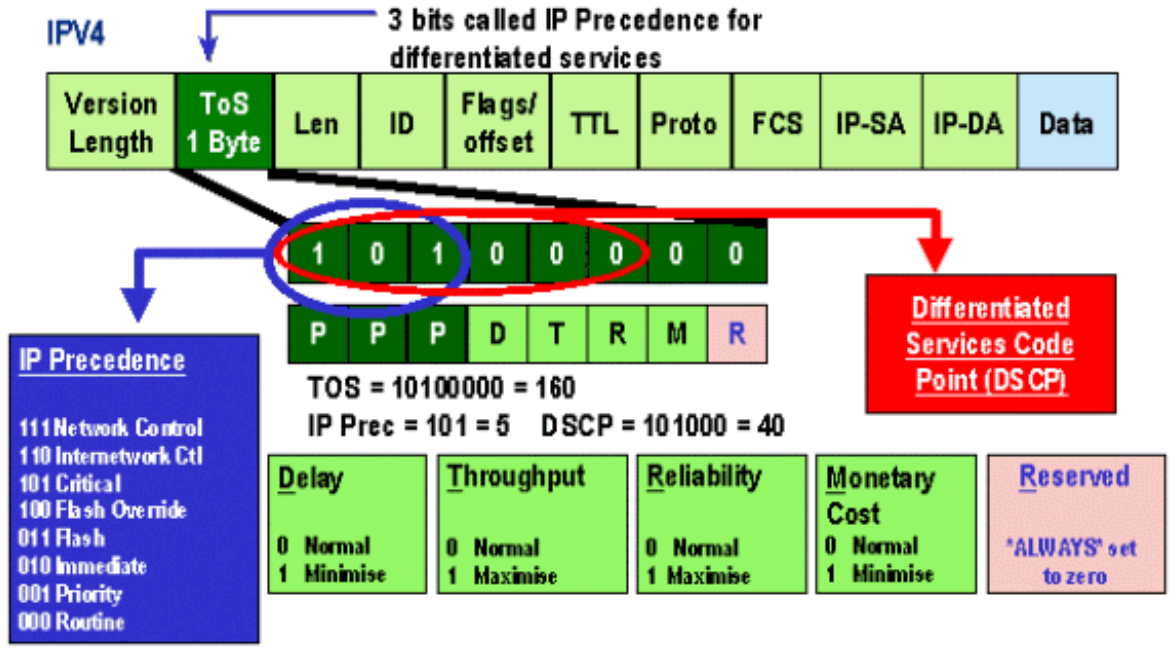
A

ToS è un campo a un byte presente in un'intestazione IPV4. Il campo ToS è composto da otto bit, dei quali i primi tre bit vengono usati per indicare la priorità del pacchetto IP. I primi tre bit sono denominati bit di precedenza IP. Questi bit possono essere impostati da zero a sette, dove zero rappresenta la priorità più bassa e sette la priorità più alta. Il supporto per l'impostazione della precedenza IP in IOS è disponibile da molti anni. Il supporto per la reimpostazione della precedenza IP può essere eseguito dall'MSFC o dal PFC (indipendente dall'MSFC). Un'impostazione di trust di untrusted può inoltre cancellare qualsiasi impostazione di precedenza IP su un frame in ingresso.

I valori che è possibile impostare per la precedenza IP sono i seguenti:

IP Precedence bits	IP Precedence Value
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

Il diagramma seguente è una rappresentazione dei bit di precedenza IP nell'intestazione ToS. I tre bit più significativi (MSB) vengono interpretati come bit di precedenza IP.



Più di recente, l'utilizzo del campo ToS è stato ampliato per includere i sei MSB, denominati DSCP. Il protocollo DSCP determina 64 valori di priorità (due alla potenza di sei) che possono

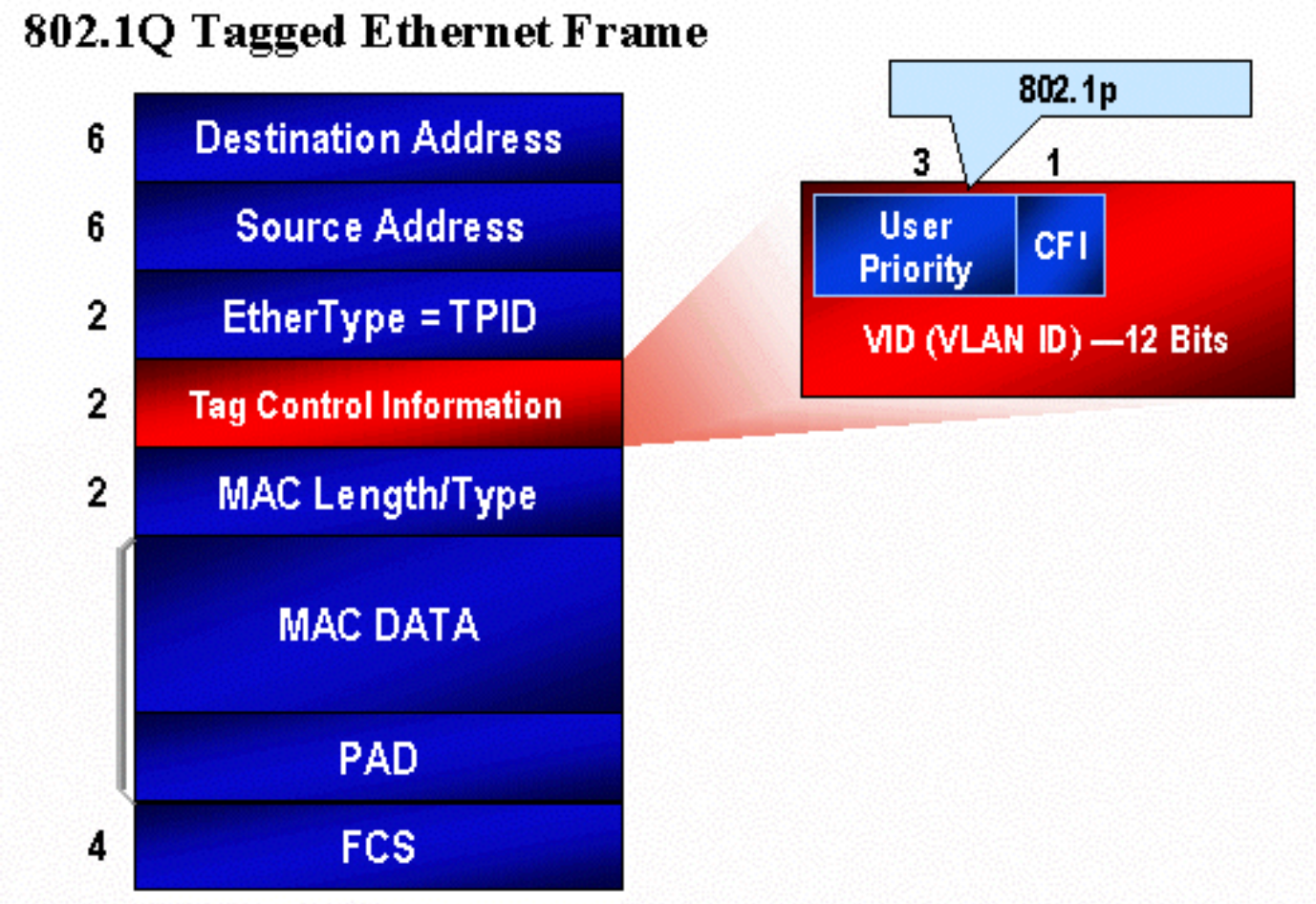
essere assegnati al pacchetto IP.

La famiglia Catalyst 6000 può modificare il tipo di servizio. A tale scopo, è possibile utilizzare sia il PFC sia l'MSFC. Quando un frame entra nello switch, gli viene assegnato un valore DSCP. Questo valore DSCP viene utilizzato internamente nello switch per assegnare i livelli di servizio (criteri QoS) definiti dall'amministratore. Il DSCP può essere già presente in un frame ed essere utilizzato oppure può essere derivato dal CoS, dalla precedenza IP o dal DSCP esistente nel frame (se la porta è attendibile). Una mappa viene utilizzata internamente nello switch per derivare il DSCP. Con otto valori di precedenza CoS/IP possibili e 64 valori DSCP possibili, la mappa predefinita mappa CoS/IPPrec 0 a DSCP 0, CoS/IPPrec 1 a DSCP 7, CoS/IPPrec 2 a DSCP 15 e così via. Questi mapping predefiniti possono essere sostituiti dall'amministratore. Quando il frame è pianificato su una porta in uscita, il CoS può essere riscritto e il valore DSCP viene utilizzato per derivare il nuovo CoS.

CoS

Il termine CoS si riferisce a tre bit di un'intestazione ISL o 802.1Q che vengono utilizzati per indicare la priorità del frame Ethernet mentre passa attraverso una rete a commutazione. Ai fini di questo documento, si fa riferimento solo all'utilizzo dell'intestazione 802.1Q. I bit CoS nell'intestazione 802.1Q sono comunemente chiamati bit 802.1p. Non sorprende che esistano tre bit CoS, che corrispondono al numero di bit utilizzati per la precedenza IP. In molte reti, per mantenere QoS end-to-end, un pacchetto può attraversare sia i domini L2 che L3. Per mantenere la qualità del servizio, è possibile mappare il tipo di servizio al tipo di servizio e il tipo di servizio al tipo di servizio.

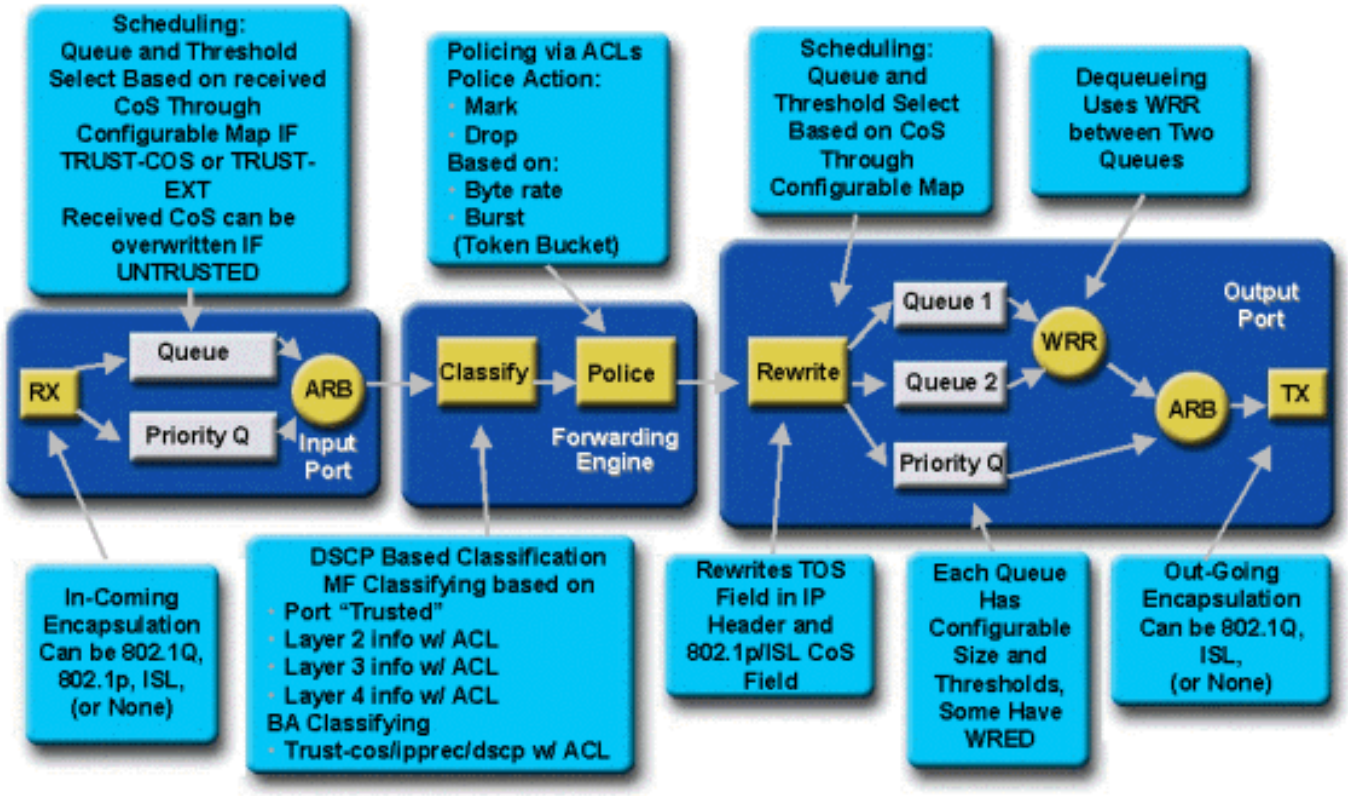
Il diagramma seguente è un frame Ethernet contrassegnato da un campo 802.1Q, composto da un Ethertype di due byte e da un tag di due byte. All'interno del tag a due byte si trovano i bit di priorità utente (noti come 802.1p).



Flusso QoS nella famiglia Catalyst 6000

QoS nella famiglia Catalyst 6000 è l'implementazione più completa di QoS in tutti gli switch Cisco Catalyst attuali. Le sezioni seguenti descrivono come i vari processi QoS vengono applicati a un frame durante il passaggio attraverso lo switch.

Nelle sezioni precedenti di questo documento, è stato osservato che molti switch L2 e L3 possono offrire una serie di elementi QOS. Tali elementi sono la classificazione, la pianificazione delle code di input, la definizione dei criteri, la riscrittura e la pianificazione delle code di output. La differenza con la famiglia Catalyst 6000 è che questi elementi QoS vengono applicati da un motore L2 che ha una visione dettagliata dei dettagli L3 e L4, oltre che solo delle informazioni dell'intestazione L2. Il diagramma seguente riepiloga il modo in cui la famiglia Catalyst 6000 implementa questi elementi.



Un frame entra nello switch e viene inizialmente elaborato dall'ASIC della porta che ha ricevuto il frame. Il frame verrà inserito in una coda Rx. A seconda della scheda di linea Catalyst 6000, saranno presenti una o due code Rx.

L'ASIC della porta utilizzerà i bit CoS come indicatore della coda in cui posizionare il frame (se sono presenti più code di input). Se la porta è classificata come non attendibile, l'ASIC della porta può sovrascrivere i bit CoS esistenti in base a un valore predefinito.

Il frame viene quindi trasmesso al motore di inoltro L2/L3 (PFC), che lo classifica e, facoltativamente, lo controlla (limite di velocità). La classificazione è il processo di assegnazione al frame di un valore DSCP, utilizzato internamente dallo switch per elaborare il frame. Il DSCP verrà derivato da uno dei seguenti elementi:

1. Un valore DSCP esistente impostato prima che il frame entri nello switch
2. I bit di precedenza IP ricevuti sono già impostati nell'intestazione IPV4. Poiché sono presenti 64 valori DSCP e solo otto valori di precedenza IP, l'amministratore configurerà un mapping utilizzato dallo switch per derivare il DSCP. Se l'amministratore non configura le mappe, verranno attivate le associazioni predefinite.
3. I bit CoS ricevuti sono già stati impostati prima che il frame entrasse nello switch. Analogamente alla precedenza IP, esistono un massimo di otto valori CoS, ognuno dei quali deve essere mappato a uno dei 64 valori DSCP. È possibile configurare questa mappa oppure lo switch può utilizzare la mappa predefinita.
4. Impostato per il frame utilizzando un valore predefinito DSCP in genere assegnato tramite una voce dell'elenco di controllo di accesso (ACL, Access Control List).

Dopo l'assegnazione di un valore DSCP al frame, viene applicato il policing (limitazione della velocità), se esiste una configurazione di policing. Il monitoraggio limiterà il flusso di dati attraverso la PFC riducendo o contrassegnando il traffico fuori profilo. Fuori profilo è un termine utilizzato per indicare che il traffico ha superato un limite definito dall'amministratore come la quantità di bit al secondo che il PFC invierà. Il traffico esterno al profilo può essere interrotto o il valore CoS può

essere ridotto. PFC1 e PFC2 attualmente supportano solo il policing di input (limitazione della velocità). Il supporto per il controllo di input e output sarà disponibile con il rilascio di un nuovo PFC.

Il PFC passerà quindi il frame alla porta di uscita per l'elaborazione. A questo punto, viene richiamato un processo di riscrittura per modificare i valori CoS nel frame e il valore ToS nell'intestazione IPV4. Deriva dal DSCP interno. Il frame verrà quindi inserito in una coda di trasmissione in base al valore CoS, pronto per la trasmissione. Mentre il frame è in coda, l'ASIC della porta monitora i buffer e implementa WRED per evitare che i buffer fuoriescano. Per programmare e trasmettere i frame dalla porta di uscita viene quindi utilizzato un algoritmo di programmazione WRR

In ognuna delle sezioni riportate di seguito questo flusso verrà analizzato in modo più dettagliato e verranno forniti esempi di configurazione per ciascuno dei passaggi descritti in precedenza.

Code, buffer, soglie e mapping

Prima di descrivere in dettaglio la configurazione QoS, è necessario spiegare ulteriormente alcuni termini per essere certi di comprendere appieno le funzionalità di configurazione QoS dello switch.

Code

Ogni porta dello switch dispone di una serie di code di input e output utilizzate come aree di archiviazione temporanea per i dati. Le schede di linea Catalyst 6000 implementano un numero diverso di code per ciascuna porta. Le code vengono in genere implementate negli ASIC hardware per ogni porta. Nelle schede di linea della prima generazione Catalyst 6000, la configurazione tipica era una coda di input e due code di output. Sulle schede di linea più recenti (10/100 e GE), l'ASIC implementa un ulteriore set di due code (una di input e una di output), risultante in due code di input e tre di output. Queste due code aggiuntive sono code SP speciali utilizzate per il traffico sensibile alla latenza, ad esempio VoIP. Vengono serviti in modalità SP. In altre parole, se un frame arriva nella coda SP, la pianificazione dei frame dalle code inferiori viene interrotta per elaborare il frame nella coda SP. Solo quando la coda SP è vuota, la pianificazione dei pacchetti dalle code inferiori ricomincia.

Quando un frame arriva a una porta (per l'input o l'output) in momenti di congestione, viene messo in coda. La decisione dietro quale coda viene inserita nel frame viene in genere presa in base al valore CoS nell'intestazione Ethernet del frame in ingresso.

In uscita verrà utilizzato un algoritmo di programmazione per svuotare la coda TX (output). WRR è la tecnica impiegata per ottenere questo risultato. Per ogni coda viene utilizzata una ponderazione per determinare la quantità di dati che verrà svuotata dalla coda prima di passare alla coda successiva. Il peso assegnato dall'amministratore è un numero compreso tra 1 e 255 e viene assegnato a ciascuna coda TX.

Buffer

A ogni coda viene assegnata una determinata quantità di spazio del buffer per memorizzare i dati di transito. L'ASIC della porta è una memoria suddivisa e allocata per singola porta. A ciascuna porta GE, l'ASIC GE assegna 512 K di spazio del buffer. Per le porte 10/100, l'ASIC della porta riserva 64 K o 128 K (a seconda della scheda di linea) di buffer per porta. Questo spazio del buffer viene quindi suddiviso tra la coda Rx (in entrata) e le code TX (in uscita).

Soglie

Un aspetto della normale trasmissione dei dati è che se un pacchetto viene scartato, la ritrasmissione del pacchetto (flussi TCP). Nei momenti di congestione, questo può aumentare il carico sulla rete e potenzialmente causare un sovraccarico ancora maggiore dei buffer. Per evitare l'overflow dei buffer, la famiglia di switch Catalyst 6000 utilizza diverse tecniche per evitare che ciò si verifichi.

Le soglie sono livelli immaginari assegnati dallo switch (o dall'amministratore) che definiscono i punti di utilizzo ai quali l'algoritmo di gestione della congestione può iniziare a eliminare i dati dalla coda. Sulle porte della famiglia Catalyst 6000, in genere sono presenti quattro soglie associate alle code di input. Alle code di output sono in genere associate due soglie.

Queste soglie vengono anche distribuite, nel contesto di QoS, come modo per assegnare a queste soglie frame con priorità diverse. Quando il buffer inizia a riempirsi e le soglie vengono superate, l'amministratore può mappare priorità diverse a soglie diverse che indicano allo switch quali frame devono essere scartati quando viene superata una soglia.

Mapping

Nelle precedenti sezioni relative alle code e alle soglie, è stato indicato che il valore CoS nel frame Ethernet viene utilizzato per determinare in quale coda posizionare il frame e in quale punto del buffer che riempie il frame può essere eliminato. Questo è lo scopo dei mapping.

Quando QoS è configurato sulla famiglia Catalyst 6000, vengono abilitati i mapping predefiniti che definiscono quanto segue:

- a quali soglie i frame con valori CoS specifici possono essere eliminati
- la coda in cui viene inserito un frame (in base al relativo valore CoS)

Sebbene esistano i mapping predefiniti, questi possono essere sostituiti dall'amministratore. Mapping esistente per:

- Valori CoS di un frame in ingresso in un valore DSCP
- Valori di precedenza IP su un frame in ingresso su un valore DSCP
- Valori DSCP in un valore CoS per un frame in uscita
- Valori CoS per eliminare le soglie nelle code di ricezione
- Valori CoS per eliminare le soglie nelle code di trasmissione
- Valori di markdown DSCP per frame che superano le istruzioni di policing
- Valori CoS in un frame con un indirizzo MAC di destinazione specifico

WRED e WRR

WRED e WRR sono due algoritmi estremamente potenti della famiglia Catalyst 6000. Sia WRED che WRR utilizzano il tag di priorità (CoS) all'interno di un frame Ethernet per fornire una gestione avanzata del buffer e una pianificazione in uscita. B

WRED

WRED è un algoritmo di gestione dei buffer utilizzato dalla famiglia Catalyst 6000 per ridurre al minimo l'impatto della perdita di traffico ad alta priorità in momenti di congestione. WRED è basato sull'algoritmo RED.

Per comprendere RED e WRED, rivedere il concetto di gestione del flusso TCP. La gestione del flusso garantisce che il mittente TCP non sovraccarichi la rete. L'algoritmo TCP slow start fa parte della soluzione per risolvere questo problema. Stabilisce che quando un flusso ha inizio, un singolo pacchetto viene inviato prima di attendere un riconoscimento. Due pacchetti vengono quindi inviati prima di ricevere un ACK, aumentando gradualmente il numero di pacchetti inviati prima di ricevere ogni ACK. Questo continuerà finché il flusso non raggiunge un livello di trasmissione (ossia, invia un numero *x* di pacchetti) che la rete può gestire senza che il carico causi congestione. In caso di congestione, l'algoritmo slow start riduce le dimensioni della finestra (ovvero il numero di pacchetti inviati prima di attendere un riconoscimento), riducendo in tal modo le prestazioni complessive per la sessione TCP (flusso).

RED monitora una coda mentre inizia a riempirsi. Una volta superata una determinata soglia, i pacchetti verranno eliminati casualmente. Non si tiene conto dei flussi specifici; piuttosto, i pacchetti casuali verranno scartati. Questi pacchetti potrebbero provenire da flussi con priorità alta o bassa. I pacchetti ignorati possono far parte di un singolo flusso o di più flussi TCP. Se vengono coinvolti più flussi, come descritto in precedenza, ciò può avere un impatto notevole su ciascuna dimensione della finestra dei flussi.

A differenza di RED, WRED non è casuale quando si rilasciano fotogrammi. WRED prende in considerazione la priorità dei frame (nel caso della famiglia Catalyst 6000 utilizza il valore CoS). Con WRED, l'amministratore assegna frame con determinati valori CoS a soglie specifiche. Una volta superate queste soglie, i frame con valori CoS mappati a queste soglie possono essere eliminati. Gli altri frame con valori CoS assegnati alle soglie più alte vengono mantenuti nella coda. Questo processo consente di mantenere intatti i flussi con priorità più alta mantenendo intatte le dimensioni delle finestre più grandi e riducendo al minimo la latenza richiesta per ottenere i pacchetti dal mittente al destinatario.

Come è possibile stabilire se la scheda di linea supporta WRED? Eseguire il comando seguente. Nell'output, controllare la sezione che indica il supporto per WRED su quella porta.

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        40% 100%
```

```
2        40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ---------------
--------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ----------------------------------- 1 100 2 255 Console> (enable)
```

Nel caso in cui WRED non sia disponibile su una porta, quest'ultima utilizzerà un metodo di gestione del buffer basato sul rilascio finale. Come suggerisce il nome stesso, la coda di caduta elimina semplicemente i frame in arrivo una volta che i buffer sono stati completamente utilizzati.

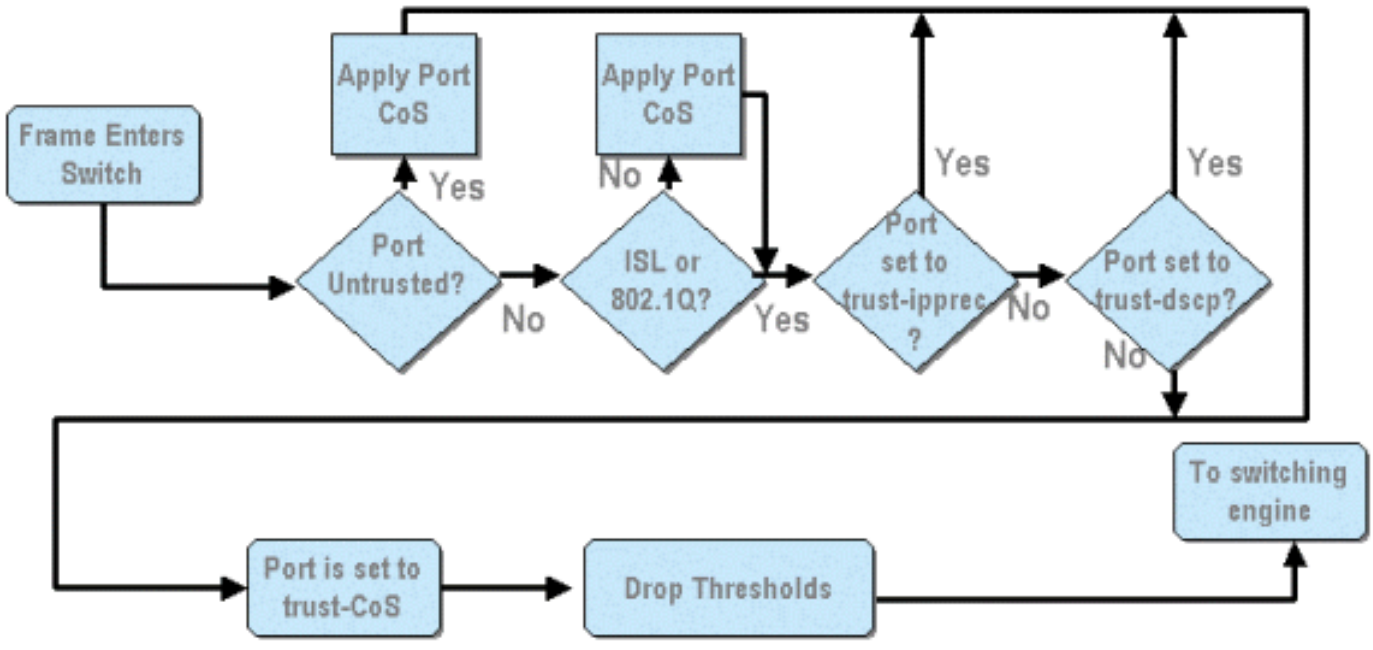
WRR

WRR viene utilizzato per pianificare il traffico in uscita dalle code TX. Un normale algoritmo round robin alternerà le code TX che inviano un numero uguale di pacchetti da ciascuna coda prima di passare alla coda successiva. L'aspetto ponderato del WRR consente all'algoritmo di programmazione di ispezionare una ponderazione assegnata alla coda. Ciò consente alle code definite di accedere a una quantità maggiore della larghezza di banda. L'algoritmo di pianificazione WRR svuoterà dalle code identificate un numero maggiore di dati rispetto alle altre code, fornendo così una distorsione per le code designate.

La configurazione per WRR e gli altri aspetti descritti in precedenza sono spiegati nelle sezioni seguenti.

Configurazione della QoS basata su ASIC per la famiglia Catalyst 6000

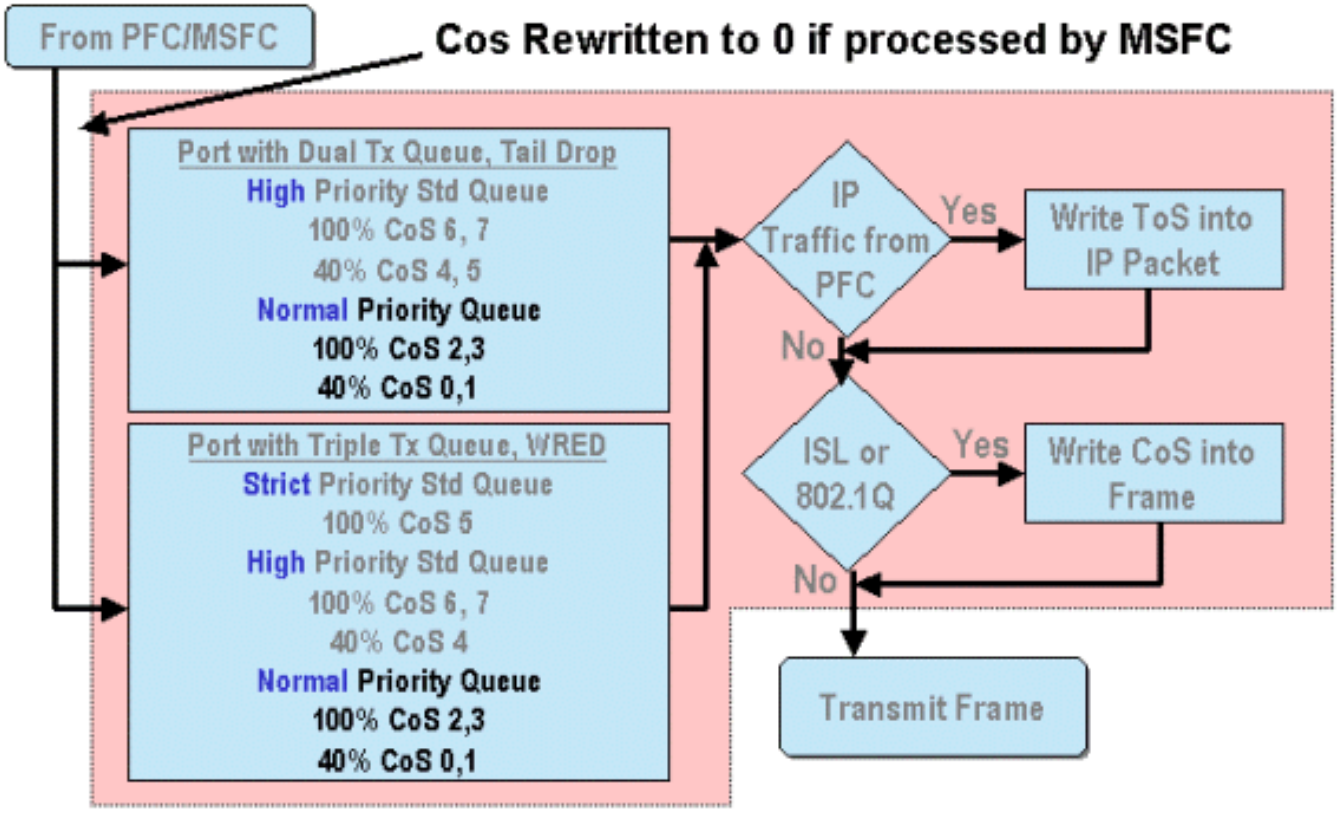
La configurazione QoS indica all'ASIC della porta o alla PFC di eseguire un'azione QoS. Nelle sezioni seguenti verrà esaminata la configurazione QoS per entrambi i processi. Sull'ASIC della porta, la configurazione QoS influisce sui flussi di traffico in entrata e in uscita.



Come si evince dallo schema precedente, si applicano i seguenti processi di configurazione QoS:

1. stati di attendibilità delle porte

2. applicazione di CoS basato su porta
3. Assegnazione soglia rilascio Rx
4 Mappe soglia rilascio CoS a Rx



Quando un frame viene elaborato dall'MSFC o dal PFC, viene passato all'ASIC della porta in uscita per un'ulteriore elaborazione. I valori CoS dei frame elaborati dall'MSFC verranno reimpostati su zero. Occorre tenerne conto per l'elaborazione QoS sulle porte in uscita.

Il diagramma precedente mostra l'elaborazione QoS eseguita dall'ASIC della porta per il traffico in uscita. Alcuni dei processi richiamati nell'elaborazione QoS in uscita includono:

1. Assegnazioni di coda TX e soglia WRED

2. Mappe da CoS a TX tail drop e WRED

Inoltre, il processo di riassegnazione del CoS al frame in uscita mediante una mappa da DSCP a CoS non è illustrato nel diagramma precedente.

Nelle sezioni seguenti vengono esaminate in dettaglio le funzionalità di configurazione QoS degli ASIC basati sulle porte.

Nota: Un aspetto importante da sottolineare è che i comandi QoS richiamati tramite CatOS vengono in genere applicati a tutte le porte con il tipo di coda specificato. Ad esempio, se viene applicata una soglia di perdita WRED alle porte con tipo di coda 1p2q2t, questa soglia viene applicata a tutte le porte su tutte le schede di linea che supportano questo tipo di coda. Con Cat IOS, i comandi QoS sono in genere applicati a livello di interfaccia.

Abilitazione di QoS

Prima di poter eseguire qualsiasi configurazione QOS sulla famiglia Catalyst 6000, è necessario abilitare QoS sullo switch. A tale scopo, eseguire il comando seguente:

CatOS

```
Console> (enable) set qos enable
!-- QoS is enabled. Console> (enable)
```

Cisco IOS integrato (modalità nativa)

```
Cat6500(config)# mls qos
```

Quando QoS è abilitato nella famiglia Catalyst 6000, lo switch imposta una serie di valori QoS predefiniti per lo switch. Le impostazioni predefinite includono:

QoS Feature	Default setting
Trust state of each port	Un-trusted
Receive Queue drop threshold percentages	Threshold 1 – 50% Threshold 2 – 60% Threshold 3 – 80% Threshold 4 – 100%
Transmit Queue drop threshold percentages	Low priority queue threshold 1 – 80% Low priority queue threshold 2 – 100% High priority queue threshold 1 – 80% High priority queue threshold 2 – 100%
CoS value to Drop threshold mapping	Receive queue 1/drop threshold 1: CoS 0 and 1 Transmit queue 1/drop threshold 1: CoS 0 and 1 Receive queue 1/drop threshold 2: CoS 2 and 3 Transmit queue 1/drop threshold 2: CoS 2 and 3 Receive queue 1/drop threshold 3: CoS 4 and 5 Transmit queue 2/drop threshold 1: CoS 4 and 5 Receive queue 1/drop threshold 4: CoS 6 and 7

	Transmit queue 2/drop threshold 2: CoS 6 and 7
CoS to DSCP Mapping (DSCP set from CoS value)	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP Precedence to DSCP Map (DSCP set from IP Precedence value)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to CoS map (CoS set from DSCP values)	DSCP 0-7 = CoS 0 DSCP 8-15 = CoS 1 DSCP 16-23 = CoS 2 DSCP 24-31 = CoS 3 DSCP 32-39 = CoS 4 DSCP 40-47 = CoS 5 DSCP 48-55 = CoS 6 DSCP 56-63 = CoS 7

Porte attendibili e non attendibili

Èpossibile configurare qualsiasi porta della famiglia Catalyst 6000 come trusted o non trusted. Lo stato di attendibilità della porta determina il modo in cui contrassegna, classifica e pianifica il frame durante il transito sullo switch. Per impostazione predefinita, tutte le porte sono in stato non attendibile.

Porte non attendibili (impostazione predefinita per le porte)

Se la porta è configurata come porta non attendibile, il valore CoS e ToS di un frame all'ingresso iniziale della porta verrà reimpostato su zero dall'ASIC della porta. Ciò significa che allo switch verrà assegnato il servizio con priorità più bassa sul suo percorso.

In alternativa, l'amministratore può ripristinare il valore CoS di qualsiasi frame Ethernet che immette una porta non attendibile a un valore predeterminato. La configurazione di questa funzionalità verrà illustrata in una sezione successiva.

Se la porta viene impostata come non attendibile, lo switch non eseguirà alcuna operazione di prevenzione delle congestioni. La prevenzione della congestione è il metodo utilizzato per eliminare i frame in base ai relativi valori CoS una volta superate le soglie definite per quella coda. Tutti i frame che entrano in questa porta possono essere eliminati anche quando i buffer raggiungono il 100%.

In CatOS, una porta 10/100 o GE può essere configurata come non attendibile usando il seguente comando:

CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

Questo comando imposta la porta 16 del modulo 3 su uno stato non attendibile.

Nota: Per Cisco IOS integrato (modalità nativa), il software attualmente supporta solo l'impostazione dell'attendibilità per le porte GE.

Cisco IOS integrato (modalità nativa)

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

Nell'esempio precedente, viene immessa la configurazione dell'interfaccia e viene applicata la forma **no** del comando per impostare la porta come non attendibile perché è IOS.

Porte attendibili

A volte, i frame Ethernet che entrano in uno switch hanno un'impostazione CoS o ToS che l'amministratore desidera mantenere mentre il frame passa attraverso lo switch. Per questo traffico, l'amministratore può impostare come attendibile lo stato di attendibilità di una porta a cui il traffico arriva allo switch.

Come accennato in precedenza, lo switch utilizza un valore DSCP internamente per assegnare un livello di servizio predeterminato a tale frame. Quando un frame entra in una porta attendibile, l'amministratore può configurare la porta in modo che controlli il CoS esistente, la precedenza IP o il valore DSCP per impostare il valore DSCP interno. In alternativa, l'amministratore può impostare un DSCP predefinito per ciascun pacchetto che entra nella porta.

Per impostare lo stato di attendibilità di una porta su attendibile, eseguire il comando seguente:

CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

Questo comando è applicabile alla scheda di linea WS-X6548-RJ45 e imposta lo stato di attendibilità della porta 3/16 su trusted. Lo switch utilizzerà il valore CoS impostato nel frame in ingresso per impostare il DSCP interno. Il DSCP deriva da una mappa predefinita creata quando QoS è stato abilitato sullo switch o, in alternativa, da una mappa definita dall'amministratore. Anziché la parola chiave trust-COs, l'amministratore può utilizzare anche la parola chiave trust-dscp o trust-ipprec.

Sulle schede a 10/100 linee precedenti (WS-X6348-RJ45 e WS-X6248-RJ45), l'attendibilità della porta deve essere impostata usando il comando **set qos acl**. In questo comando, uno stato di attendibilità può essere assegnato da un sottoparametro del comando **set qos acl**. L'impostazione di trust CoS sulle porte di queste schede di linea non è supportata, come illustrato di seguito.

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to
turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so
port is set to untrusted.
```

Il comando precedente indica che è necessario per abilitare la pianificazione della coda di input. Pertanto, per le porte 10/100 sulle schede di linea WS-X6248-RJ45 e WS-X6348-RJ45, il comando **set port qos x/y trust-COs** deve essere ancora configurato, anche se per impostare gli stati di attendibilità, è necessario usare l'ACL.

Con Cisco IOS integrato (modalità nativa), è possibile impostare il trust su un'interfaccia GE e porte 10/100 sulla nuova scheda di linea WS-X6548-RJ45.

Cisco IOS integrato (modalità nativa)

```
Cat6500(config)# interface gigabitethernet 5/4
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

In questo esempio lo stato di attendibilità della porta GE 5/4 viene impostato su trusted. Il valore di precedenza IP del frame verrà utilizzato per derivare il valore DSCP.

CoS basato sulla porta di classificazione e impostazione dell'input

All'ingresso di una porta dello switch, il CoS di un frame Ethernet può essere modificato se soddisfa uno dei due criteri seguenti:

1. la porta è configurata come non attendibile oppure
2. per il frame Ethernet non è già impostato un valore CoS esistente

Per riconfigurare il CoS di un frame Ethernet in ingresso, usare il comando seguente:

CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

Questo comando imposta i CO dei frame Ethernet in ingresso sulla porta 16 del modulo 3 su un valore di 3 quando arriva un frame non contrassegnato o se la porta è impostata su non attendibile.

Cisco IOS integrato (modalità nativa)

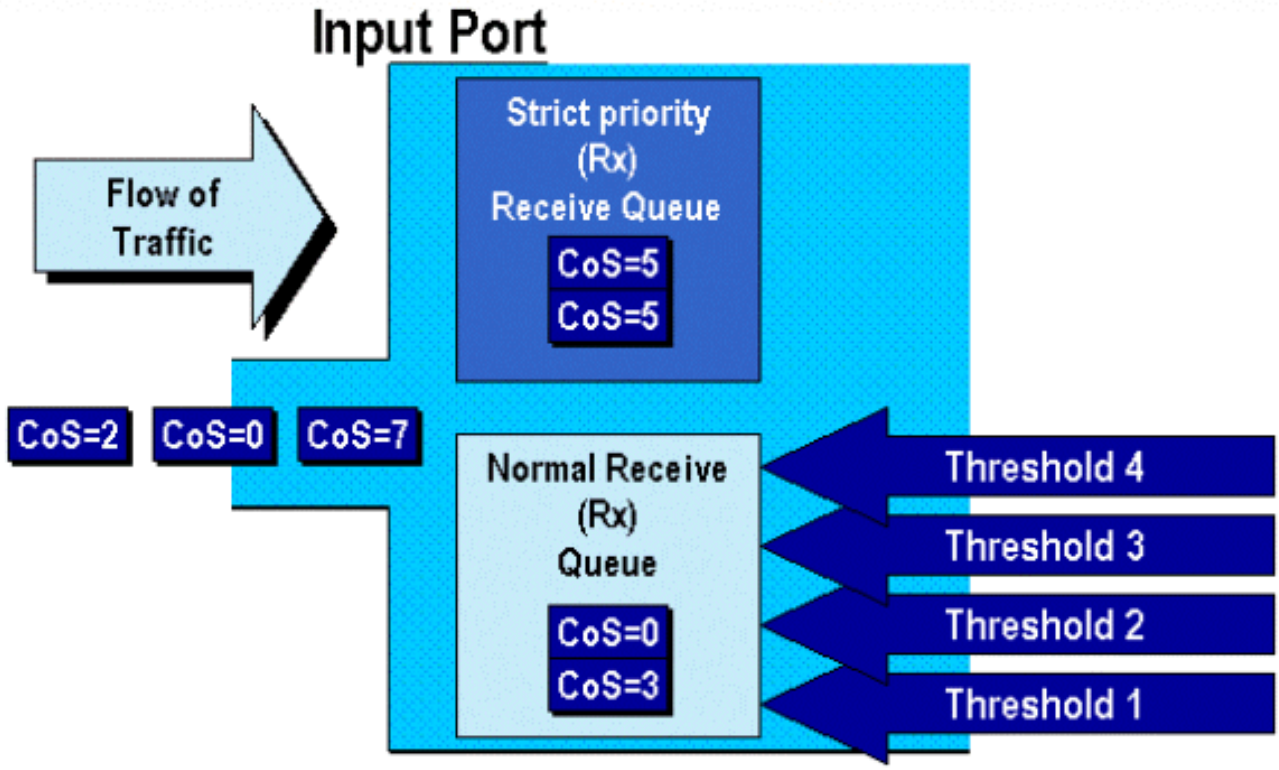
```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

Questo comando imposta i CO dei frame Ethernet in ingresso sulla porta 13 del modulo 5 su un valore di 4 quando arriva un frame non contrassegnato o se la porta è impostata su non

attendibile.

Configura soglie di rilascio Rx

All'ingresso alla porta dello switch, il frame viene inserito in una coda Rx. Per evitare il sovraccarico del buffer, l'ASIC della porta implementa quattro soglie su ciascuna coda Rx e utilizza queste soglie per identificare i frame che possono essere eliminati una volta superate tali soglie. L'ASIC della porta utilizzerà il valore CO impostato per i frame per identificare i frame che possono essere scartati quando viene superata una soglia. Questa funzionalità consente ai frame con priorità più alta di rimanere nel buffer più a lungo in caso di congestione.



Come illustrato nel diagramma precedente, i frame arrivano e vengono inseriti nella coda. Quando la coda inizia a riempirsi, le soglie vengono controllate dall'ASIC della porta. Quando viene superata una soglia, i frame con valori CO identificati dall'amministratore vengono eliminati casualmente dalla coda. I mapping di soglia predefiniti per una coda 1q4t (trovati sulle schede di linea WS-X6248-RJ45 e WS-X6348-RJ45) sono i seguenti:

- la soglia 1 è impostata sul 50% e i valori 0 e 1 dei CO sono mappati a questa soglia
- la soglia 2 è impostata sul 60% e i valori 2 e 3 dei CO sono mappati su questa soglia
- la soglia 3 è impostata sull'80% e i valori 4 e 5 dei CO sono mappati su questa soglia
- la soglia 4 è impostata su 100% e i valori di CO 6 e 7 sono mappati su questa soglia

Per una coda 1P1q4t (disponibile sulle porte GE), i mapping predefiniti sono i seguenti:

- la soglia 1 è impostata sul 50% e i valori 0 e 1 dei CO sono mappati a questa soglia
- la soglia 2 è impostata sul 60% e i valori 2 e 3 dei CO sono mappati su questa soglia
- la soglia 3 è impostata sull'80% e i valori di CO 4 sono mappati su questa soglia
- la soglia 4 è impostata su 100% e i valori di CO 6 e 7 sono mappati su questa soglia
- Il valore 5 di CO è mappato alla coda di priorità rigida

Per un 1p1q0t (rilevato sulle porte 10/100 della scheda di linea WS-X6548-RJ45), i mapping

predefiniti sono i seguenti:

- I frame con CO5 vengono inviati alla coda Rx SP (coda 2), dove lo switch scarta i frame in ingresso solo quando il buffer della coda di ricezione SP è pieno al 100%.
- I frame con CO 0, 1, 2, 3, 4, 6 o 7 vanno alla coda Rx standard. Lo switch scarta i frame in ingresso quando il buffer della coda Rx è pieno al 100%.

L'amministratore può modificare queste soglie di rilascio. È inoltre possibile modificare i valori predefiniti dei CO mappati a ogni soglia. Schede di linea diverse implementano diverse implementazioni di code Rx. Di seguito è riportato un riepilogo dei tipi di coda.

CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

Questo comando imposta le soglie di rilascio della ricezione per tutte le porte di input con una coda e quattro soglie (denota 1q4t) su 20%, 40%, 75% e 100%.

Di seguito è riportato il comando emesso in modalità integrata Cisco IOS (modalità nativa).

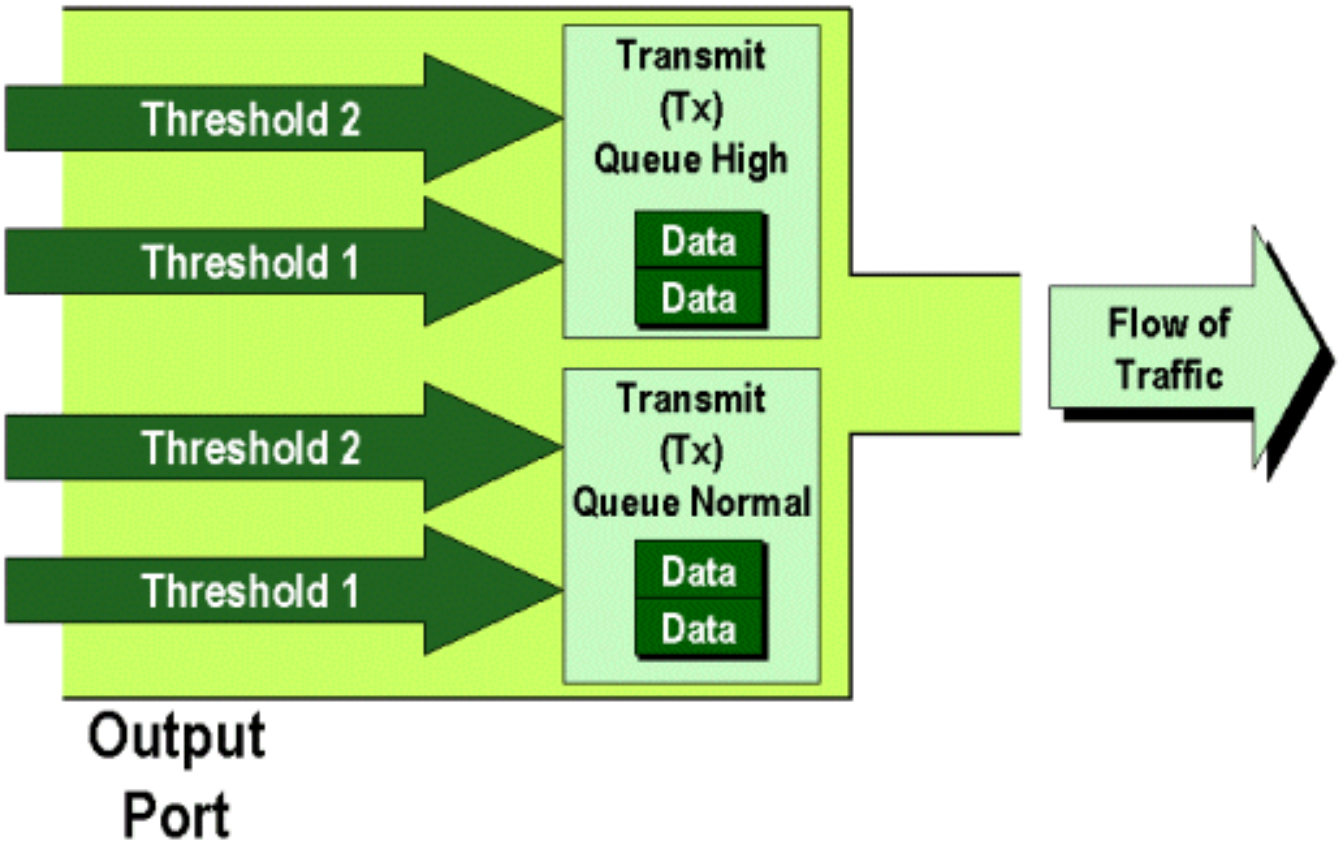
Cisco IOS integrato (modalità nativa)

```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100

!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line
card.
```

Le soglie di rilascio Rx devono essere abilitate dall'amministratore. Al momento, il comando **set port qos x/y trust-COs** deve essere usato per attivare le soglie di rilascio Rx (dove *x* è il numero del modulo e *y* è la porta del modulo).

Configurazione delle soglie di rilascio TX

Su una porta in uscita, la porta avrà due soglie TX utilizzate come parte del meccanismo di prevenzione della congestione, la coda 1 e la coda 2. La coda 1 è indicata come coda standard a bassa priorità e la coda 2 come coda standard ad alta priorità. A seconda delle schede di linea utilizzate, queste utilizzeranno un algoritmo di gestione delle code drop o delle soglie WRED. Entrambi gli algoritmi utilizzano due soglie per ciascuna coda TX.



L'amministratore può impostare manualmente queste soglie nel modo seguente:

CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

Questo comando imposta le soglie di rilascio TX per la coda 1 per tutte le porte di output con due code e due soglie (indica 2q2t) su 40% e 100%.

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

Questo comando imposta le soglie di rilascio WRED per la coda 1 per tutte le porte di output con una coda SP, due code normali e due soglie (denota 1p2q2t) su 60% e 100%. La coda 1 è definita come coda normale a bassa priorità e ha la priorità più bassa. La coda 2 è la coda normale ad alta priorità e ha una priorità più alta rispetto alla coda 1. La coda 3 è la coda SP ed è servita prima di tutte le altre code su quella porta.

Di seguito è riportato il comando equivalente eseguito in modalità integrata Cisco IOS (modalità nativa).

Cisco IOS integrato (modalità nativa)

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
```

```
Cat6500(config-if)#
```

In questo modo le soglie di rilascio WRED per una porta 1p2q2t vengono impostate su una coda compresa tra 1 e 40% per la soglia 1 (TX) e su 100% per la soglia 2 (TX).

Se necessario, è possibile disabilitare WRED anche in Cisco IOS integrato (modalità nativa). A tale scopo, utilizzare la forma **n"** del comando. Di seguito è riportato un esempio di disattivazione di WRED:

Cisco IOS integrato (modalità nativa)

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

Mapping dell'indirizzo MAC ai valori CO

Oltre a impostare i CO in base a una definizione di porta globale, lo switch consente all'amministratore di impostare i valori dei CO in base all'indirizzo MAC di destinazione e all'ID VLAN. In questo modo, i frame destinati a destinazioni specifiche possono essere contrassegnati con un valore CO predeterminato. Per eseguire questa configurazione, usare il comando seguente:

CatOS

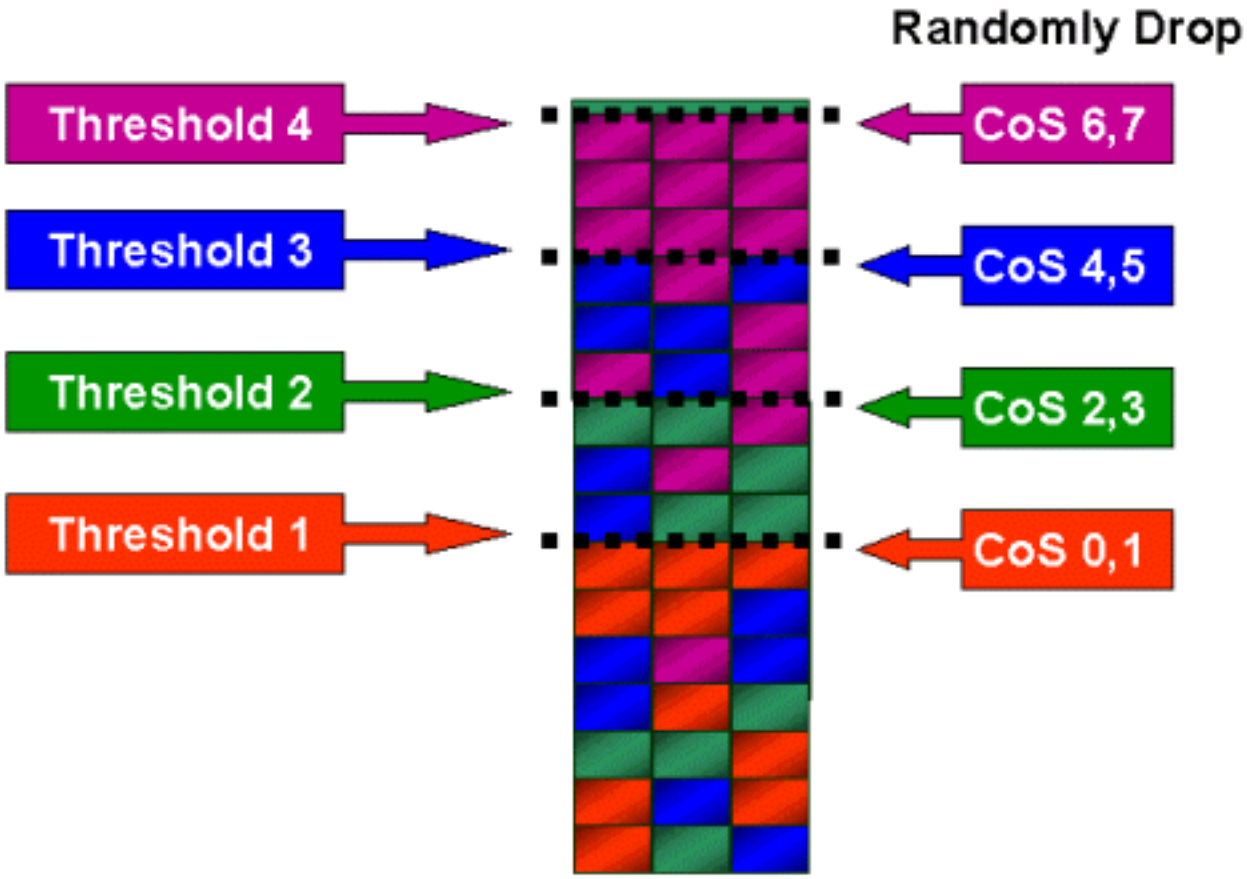
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

Questo comando imposta un CO di 5 per ogni frame il cui indirizzo MAC di destinazione è 00-00-0c-33-2a-4e proveniente dalla VLAN 200.

Non è disponibile alcun comando equivalente in Cisco IOS integrato (modalità nativa). Infatti questo comando è supportato solo quando non è presente alcun PFC e per il funzionamento di Cisco IOS integrato (modalità nativa) è necessario un PFC.

Mapping dei CO alle soglie

Dopo aver configurato le soglie, l'amministratore può assegnare i valori dei CO a tali soglie, in modo che, quando la soglia viene superata, i frame con valori di CO specifici possano essere eliminati. In genere, l'amministratore assegna i frame con priorità inferiore alle soglie inferiori, mantenendo quindi il traffico con priorità superiore nella coda in caso di congestione.



La figura precedente mostra una coda di input con quattro soglie e come i valori di CO sono stati assegnati a ciascuna soglia.

L'output seguente mostra come i valori dei CO possono essere mappati sulle soglie:

CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

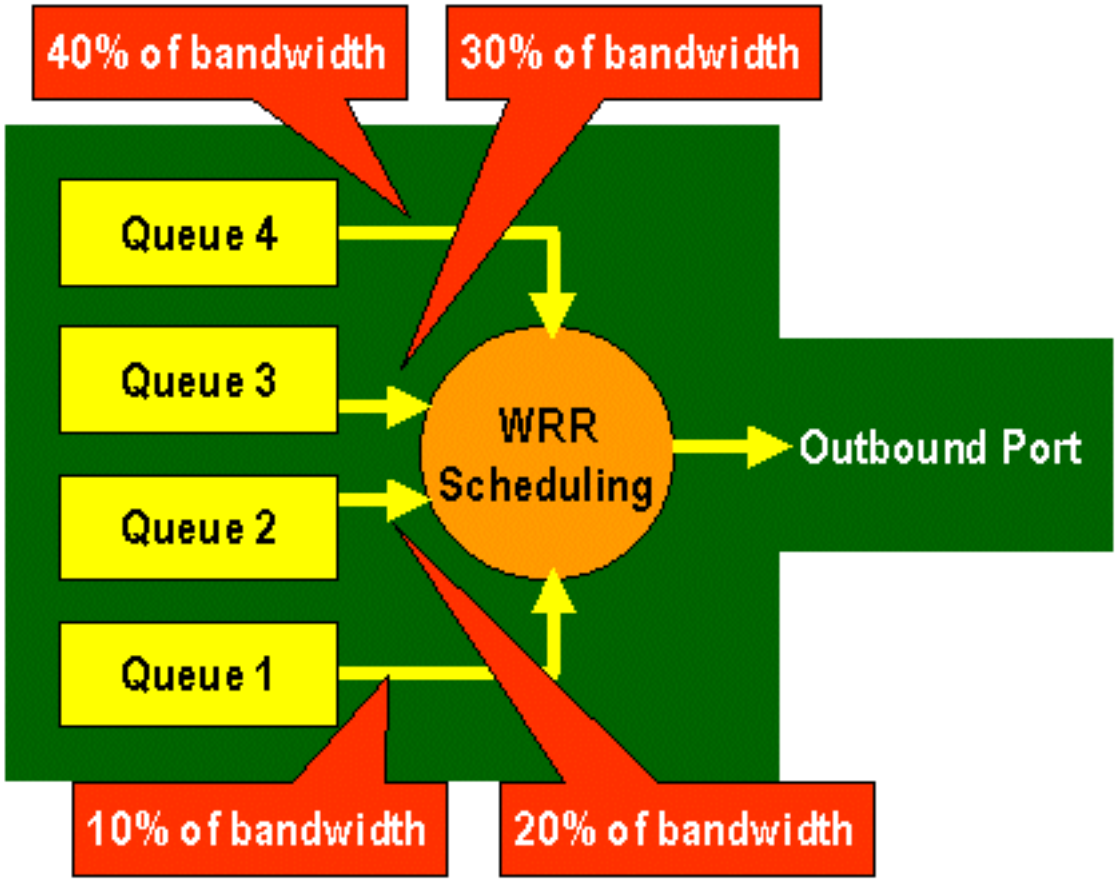
Questo comando assegna i valori 0 e 1 dei CO alla coda 1, soglia 1. Di seguito è riportato il comando equivalente in modalità integrata Cisco IOS (modalità nativa).

Cisco IOS integrato (modalità nativa)

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

Configurazione della larghezza di banda sulle code TX

Quando un frame viene inserito in una coda di output, viene trasmesso utilizzando un algoritmo di programmazione dell'output. Il processo di programmazione dell'output utilizza il WRR per trasmettere i frame dalle code di output. A seconda dell'hardware della scheda di linea in uso, vi sono due, tre o quattro code di trasmissione per porta.



Sulle schede di linea WS-X6248 e WS-X6348 (con strutture di coda 2q2t), il meccanismo WRR utilizza due code TX per la programmazione. Sulle schede di linea WS-X6548 (con una struttura di coda 1p3q1t) sono presenti quattro code TX. Di queste quattro code TX, tre sono servite dall'algoritmo WRR (l'ultima coda TX è una coda SP). Sulle schede di linea GE sono presenti tre code TX (utilizzando una struttura di coda 1p2q2t); una di queste code è una coda SP, quindi l'algoritmo WRR serve solo due code TX.

In genere, l'amministratore assegna un peso alla coda TX. Il comando WRR analizza la ponderazione assegnata alla coda di porte, utilizzata internamente dallo switch per determinare la quantità di traffico che verrà trasmessa prima di passare alla coda successiva. A ciascuna coda di porte può essere assegnato un valore di ponderazione compreso tra 1 e 255.

CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

Questo comando assegna un peso di 40 alla coda 1 e di 80 alla coda 2. Ciò significa in effetti un rapporto di due a uno (da 80 a 40 = da 2 a 1) della larghezza di banda assegnata tra le due code. Questo comando ha effetto su tutte le porte con due code e due soglie sulle porte.

Di seguito è riportato il comando equivalente eseguito in modalità integrata Cisco IOS (modalità nativa).

Cisco IOS integrato (modalità nativa)

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
Cat6500(config-if)#
```

Quanto sopra rappresenta un rapporto tre a uno tra le due code. Si noti che la versione Cat IOS di questo comando viene applicata solo a un'interfaccia specifica.

Mapping da DSCP a CO

Una volta posizionato il frame nella porta di uscita, l'ASIC della porta utilizzerà i CO assegnati per evitare la congestione (WRED) e i CO per determinare la pianificazione del frame (trasmissione del frame). A questo punto, lo switch utilizzerà una mappa predefinita per mappare il DSCP assegnato su un valore CO. Questa mappa predefinita viene visualizzata in questa tabella.

In alternativa, l'amministratore può creare una mappa che verrà utilizzata dallo switch per accettare il valore DSCP interno assegnato e creare un nuovo valore CO per il frame. Di seguito sono riportati alcuni esempi di come utilizzare CatOS e Cisco IOS (modalità nativa) integrato per ottenere questo risultato.

CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

Il comando precedente mappa i valori DSCP da 20 a 30 a un valore COs di 5, i valori DSCP da 10 a 15 a un valore CO di 3 e i valori DSCP da 45 a 52 a un valore COs di 7. Tutti gli altri valori DSCP utilizzano la mappa predefinita creata quando QoS è stato abilitato sullo switch.

Di seguito è riportato il comando equivalente eseguito in modalità integrata Cisco IOS (modalità nativa).

Cisco IOS integrato (modalità nativa)

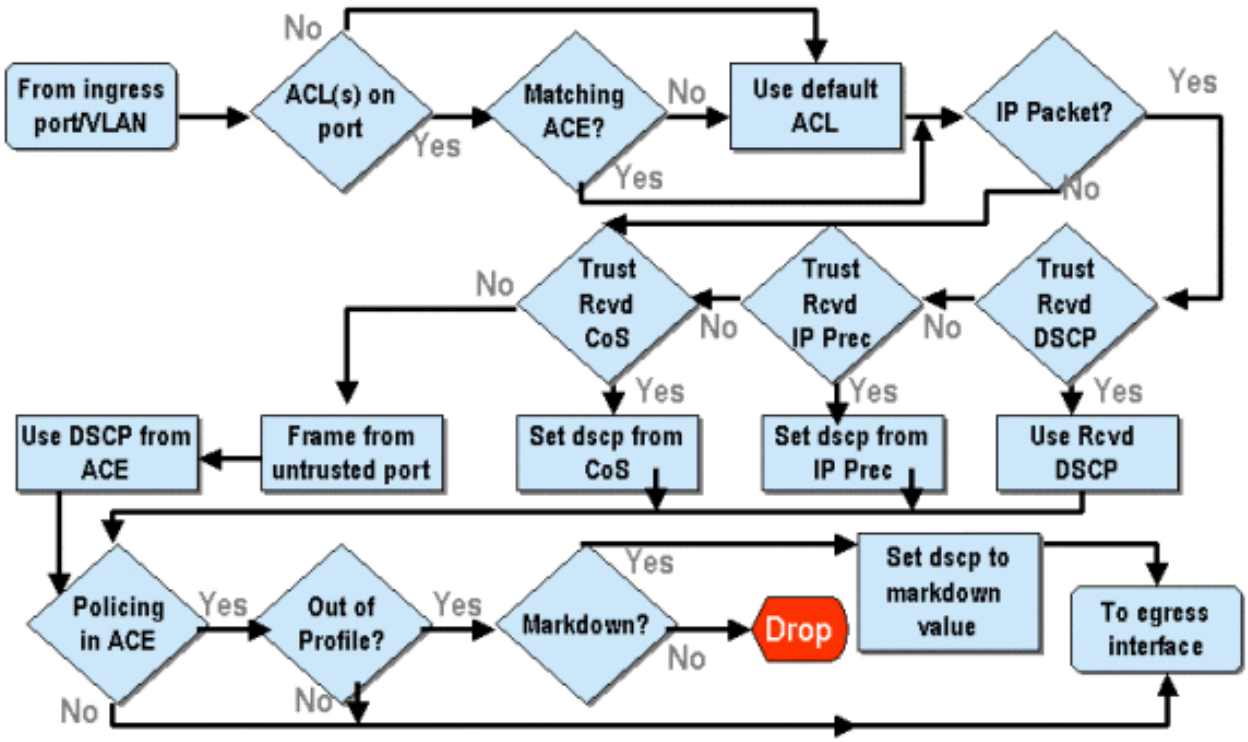
```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

In questo modo i valori DSCP di 20, 30, 40, 50, 52, 10 e 1 vengono impostati su un valore CO pari a 3.

Classificazione e policy con PFC

La PFC supporta la classificazione e il controllo dei frame. La classificazione può utilizzare un ACL per assegnare (contrassegnare) un frame in ingresso con una priorità (DSCP). Il policing consente di limitare un flusso di traffico a una determinata quantità di larghezza di banda.

Le sezioni seguenti descrivono queste funzionalità sul PFC dal punto di vista sia delle piattaforme CatOS che del sistema operativo Cisco IOS integrato (modalità nativa). I processi applicati dal PFC sono illustrati nel seguente diagramma:



Configurazione della policy sulla famiglia Catalyst 6000 con CatOS

La funzione di policing è suddivisa in due sezioni, una per CatOS e una per Cisco IOS (modalità nativa) integrato. Entrambi raggiungono lo stesso risultato finale, ma sono configurati e implementati in modi diversi.

Traffic policing

La PFC supporta la capacità di limitare la velocità (o controllare) del traffico in entrata verso lo switch e può ridurre il flusso del traffico a un limite predefinito. Il traffico che supera questo limite può essere scartato o lasciare il valore DSCP nel frame abbassato a un valore inferiore.

La limitazione della velocità di output (in uscita) non è attualmente supportata né nel PFC1 né nel PFC2. Verrà aggiunta una nuova revisione del PFC pianificata per la seconda metà del 2002 che supporterà la policy di output (o in uscita).

Il policing è supportato sia in CatOS che nel nuovo Cisco IOS integrato (modalità nativa), anche se la configurazione di queste funzionalità è molto diversa. Nelle sezioni seguenti verrà descritta la configurazione del policing in entrambe le piattaforme del sistema operativo.

Aggregati e microflussi (CatOS)

Aggregati e microflussi sono termini utilizzati per definire l'ambito di applicazione delle policy eseguito dal PFC.

Un microflusso definisce il controllo di un singolo flusso. Un flusso viene definito da una sessione con un indirizzo MAC SA/DA univoco, un indirizzo IP SA/DA e numeri di porta TCP/UDP. Per ogni nuovo flusso avviato tramite una porta di una VLAN, il microflusso può essere utilizzato per limitare la quantità di dati ricevuti per quel flusso dallo switch. Nella definizione di microflusso, i pacchetti che superano il limite di velocità prescritto possono essere scartati o avere il valore DSCP contrassegnato per difetto.

Analogamente a un microflusso, un aggregato può essere utilizzato per limitare il traffico. Tuttavia,

la velocità di aggregazione si applica a tutto il traffico in entrata su una porta o su una VLAN che corrisponde a un ACL QoS specificato. È possibile visualizzare l'aggregazione come il controllo del traffico cumulativo che corrisponde al profilo nella voce di controllo di accesso (ACE, Access Control Entry).

Sia l'aggregazione che il microflusso definiscono la quantità di traffico che può essere accettata nello switch. È possibile assegnare contemporaneamente un'aggregazione e un microflusso a una porta o a una VLAN.

Quando si definiscono i microflussi, è possibile definirne fino a 63 e definire fino a 1023 aggregati.

Voci di controllo dell'accesso e ACL QoS (CatOS)

Un ACL QoS è costituito da un elenco di ACE che definiscono un set di regole QoS utilizzate dalla PFC per elaborare i frame in ingresso. Gli ACL sono simili alle RACL (Router Access Control List). L'ACE definisce i criteri di classificazione, contrassegno e applicazione di policy per un frame in ingresso. Se un frame in ingresso corrisponde ai criteri impostati nell'ACE, il motore QoS elaborerà il frame (come ritenuto dall'ACE).

Tutta l'elaborazione QoS viene eseguita nell'hardware, quindi l'attivazione del controllo QoS non influisce sulle prestazioni dello switch.

Il PFC2 attualmente supporta fino a 500 ACL e questi ACL possono essere costituiti da un massimo di 32000 ACL (in totale). I numeri ACE effettivi dipendono dagli altri servizi definiti e dalla memoria disponibile nella PFC.

Èpossibile definire tre tipi di assi. IP, IPX e MAC. Sia gli access point IP che IPX ispezionano le informazioni dell'intestazione L3, mentre gli access point basati su MAC ispezionano solo le informazioni dell'intestazione L2. Si noti inoltre che gli ACL MAC possono essere applicati solo al traffico non IP e non IPX.

Creazione delle regole di controllo

Il processo di creazione di una regola di controllo implica la creazione di un'aggregazione (o microflusso), quindi il mapping di tale aggregazione (o microflusso) a una voce ACE.

Se, ad esempio, il requisito era quello di limitare tutto il traffico IP in entrata sulla porta 5/3 a un massimo di 20 MB, i due passaggi summenzionati devono essere configurati.

In primo luogo, l'esempio richiede che tutto il traffico IP in ingresso sia limitato. Ciò implica che è necessario definire un policer aggregato. Di seguito è riportato un esempio:

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

Abbiamo creato un aggregato chiamato flusso di test. Definisce una velocità di 20000 KBPS (20 MBPS) e una frammentazione di 13. La parola chiave policed-dscp indica che i dati che superano questo criterio avranno il valore DSCP contrassegnato come specificato in una mappa di markdown DSCP (ne esiste una predefinita o può essere modificata dall'amministratore). Un'alternativa all'uso della parola chiave policed-dscp è l'uso della parola chiave drop. La parola chiave drop elimina semplicemente tutto il traffico esterno al profilo (il traffico che rientra al di fuori del valore burst assegnato).

La funzione di controllo si basa su uno schema di bucket di token con perdita, in quanto l'utente definisce una frammentazione (ovvero la quantità di dati in bit al secondo che accetterà in un determinato intervallo di tempo (fisso)) e quindi la frequenza (definita come la quantità di dati che verrà svuotata in un singolo secondo). Tutti i dati che superano il flusso di questo bucket vengono eliminati o il relativo DSCP viene contrassegnato per difetto. Il periodo di tempo (o intervallo) specificato sopra è 0,00025 secondi (o 1/4000 di secondo) ed è fisso (ossia non è possibile utilizzare alcun comando di configurazione per modificare questo numero).

Il numero 13 dell'esempio precedente rappresenta un bucket in grado di accettare fino a 13.000 bit di dati ogni 1/4000 di secondo. Ciò si riferisce a 52 MB al secondo (13K * (1 / 0.00025) o 13K * 4000). È sempre necessario verificare che la velocità di frammentazione sia configurata in modo da essere uguale o superiore alla velocità di invio dei dati. In altre parole, la frammentazione deve essere maggiore o uguale alla quantità minima di dati che si desidera trasmettere per un determinato periodo. Se la frammentazione determina una cifra inferiore a quella specificata come velocità, il limite di velocità sarà uguale alla frammentazione. In altre parole, se si definisce una velocità di 20 MBPS e un burst che calcola fino a 15 MBPS, la velocità raggiungerà solo 15 MBPS. La domanda successiva da porsi è: perché 13? La frammentazione definisce la profondità del bucket di token, ovvero la profondità del bucket utilizzato per ricevere i dati in ingresso ogni 1/4000 di secondo. Pertanto, la frammentazione potrebbe essere un qualsiasi numero supportato su una velocità di trasferimento dati maggiore o uguale a 20 MB al secondo. Il minimo burst che si potrebbe utilizzare per un limite di velocità di 20MB è 2000/4000 = 5.

Quando elabora il policer, l'algoritmo di policing inizia riempiendo il bucket di token con una serie completa di token. Il numero di token è uguale al valore burst. Quindi, se il valore burst è 13, il numero di token nel bucket è uguale a 13.000. Per ogni 1/4000 di secondo, l'algoritmo di policing invierà una quantità di dati uguale al tasso definito diviso per 4000. Per ogni bit (cifra binaria) di dati inviati, consuma un token dal bucket. Al termine dell'intervallo, il bucket verrà rifornito con un nuovo set di token. Il numero di token che sostituisce è definito dalla velocità / 4000. Considerare l'esempio precedente per comprendere quanto segue:

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

Si supponga che si tratti di una porta a 100 MBPS e che venga inviato un flusso costante di 100 MBPS alla porta. Sappiamo che ciò equivale a una velocità in ingresso di 100.000.000 di bit al secondo. I parametri sono una velocità di 20000 e burst di 13. All'intervallo di tempo t0, c'è una serie completa di token nel bucket (che è 13.000). Nell'intervallo di tempo t0, verrà visualizzato il primo gruppo di dati da inviare alla porta. Per questo intervallo di tempo, la velocità di arrivo sarà di 100.000.000 / 4000 = 25.000 bit al secondo. Poiché il token bucket ha solo una profondità di 13.000 token, solo 13.000 bit dei 25.000 bit che arrivano alla porta in questo intervallo sono idonei per l'invio e 12.000 bit vengono scartati.

La velocità specificata definisce una velocità di inoltro di 20.000.000 bit al secondo, che equivale a 5.000 bit inviati per 1/4000 intervallo. Per ogni 5.000 bit inviati, vengono utilizzati 5.000 token. Nell'intervallo di tempo T1, arrivano altri 25.000 bit di dati, ma il bucket scende di 12.000 bit. Il bucket viene rifornito con token definiti come rate / 4000 (che equivale a 5.000 nuovi token). L'algoritmo invia quindi il successivo complemento di dati, che equivale ad altri 5.000 bit di dati (consumando altri 5.000 token) e così via per ogni intervallo.

In pratica, tutti i dati che superano la profondità del bucket (burst definito) vengono eliminati. Anche i dati rimanenti dopo l'invio (corrispondenti alla velocità indicata) vengono scartati, aprendo la strada alla successiva serie di dati in arrivo. Un pacchetto incompleto è un pacchetto che non è stato ricevuto completamente entro l'intervallo di tempo e che non viene quindi scartato finché non è stato ricevuto completamente nella porta.

Questo numero di burst presuppone un flusso costante del traffico. Tuttavia, nelle reti reali, i dati non sono costanti e il loro flusso è determinato dalle dimensioni della finestra TCP, che incorpora i riconoscimenti TCP nella sequenza di trasmissione. Per prendere in considerazione i problemi relativi alle dimensioni della finestra TCP, si consiglia di raddoppiare il valore di burst. Nell'esempio precedente, il valore suggerito di 13 sarebbe in realtà configurato come 26.

Un altro punto importante da sottolineare è che all'intervallo di tempo 0 (ossia, l'inizio di un ciclo di controllo), il token bucket è pieno di token.

Questo criterio aggregato deve ora essere incorporato in un ACE QoS. La voce di controllo di accesso è la posizione in cui la specifica viene creata per far corrispondere un set di criteri a un frame in ingresso. Si consideri l'esempio seguente. Si desidera applicare l'aggregazione definita in precedenza a tutto il traffico IP, ma in modo specifico al traffico proveniente dalla subnet 10.5.x.x e destinato alla subnet 203.100.45.x. L'ACE avrà il seguente aspetto:

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

Con il comando precedente viene creata una voce di controllo di accesso IP (indicata dall'uso del comando **set qos acl ip**), che è ora associata a un ACL QoS chiamato test-acl. Gli ACL successivi creati e associati all'ACL test-acl vengono aggiunti alla fine dell'elenco ACE. Alla voce ACE è associato il flusso di test aggregato. A tutti i flussi TCP con subnet di origine 10.5.0.0 e subnet di destinazione 203.100.45.0 verrà applicato questo criterio.

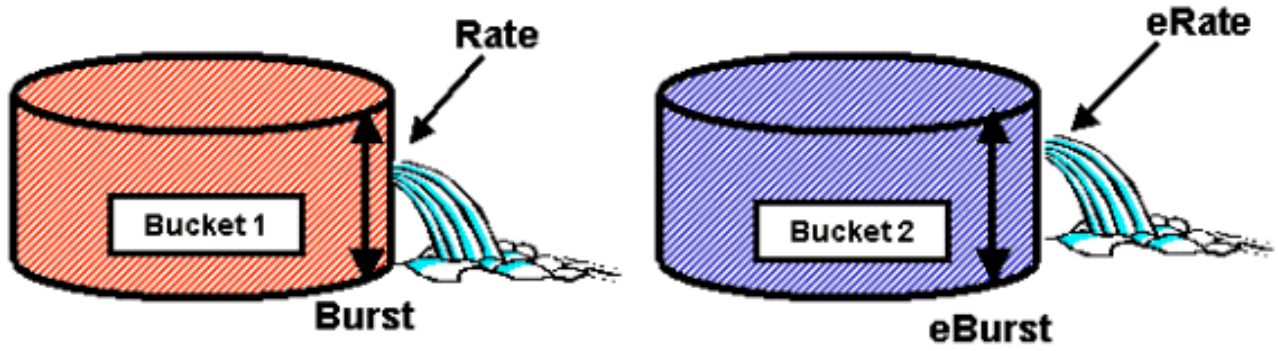
Gli ACL (e gli ACL associati) forniscono un livello molto granulare di flessibilità di configurazione che gli amministratori possono utilizzare. Un ACL può essere costituito da uno o più ACL. È possibile usare gli indirizzi di origine e/o di destinazione e i valori della porta L4 per identificare i flussi particolari di cui è necessario eseguire il policy.

Tuttavia, prima che si verifichi il controllo, l'ACL deve essere mappato su una porta fisica o su una VLAN.

Decisioni di policy PFC2

Per il PFC2, è stata apportata una modifica in CatOS 7.1 e CatOS 7.2, che ha introdotto un algoritmo a doppio bucket con perdita di dati per il policing. Con questo nuovo algoritmo vengono aggiunti i due nuovi livelli seguenti:

1. **Livello di Policing normale:** ciò equivale al primo periodo fisso e definisce i parametri che specificano la profondità del periodo fisso (burst) e la velocità di invio dei dati dal periodo fisso (rate).
2. **Livello di Policing in eccesso:** ciò equivale a un secondo periodo fisso e definisce i parametri che specificano la profondità del periodo fisso (eburst) e la velocità di invio dei dati dal periodo fisso (erate).



Questo processo funziona in modo che i dati inizino a riempire il primo bucket. Il PFC2 accetta un flusso di dati in ingresso inferiore o uguale alla profondità (valore burst) del primo bucket. I dati che fuoriescono dal primo periodo fisso possono essere contrassegnati e passati al secondo periodo fisso. Il secondo periodo fisso può accettare una velocità in entrata di dati provenienti dal primo periodo fisso a un valore inferiore o uguale al valore di rigenerazione. I dati del secondo periodo fisso vengono inviati a una velocità definita dal parametro relativo alla velocità meno il parametro relativo alla velocità. Anche i dati che fuoriescono dal secondo bucket possono essere contrassegnati per difetto o eliminati.

Di seguito è riportato un esempio di policer a bucket con doppia perdita:

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst
13 eburst 13
```

Questo esempio imposta in posizione un aggregato denominato AGG1 con una velocità di traffico superiore a 10 MBPS e verrà contrassegnato in base alla mappa DSCP controllata. Il traffico in eccesso rispetto alla velocità (impostata su 12 MBPS) verrà scartato in base alla parola chiave drop.

Applicazione di criteri di aggregazione ai moduli abilitati per DFC

Èopportuno notare che l'applicazione di policer aggregati su schede di linea non DFC può essere ottenuta grazie al modo in cui la 6000 utilizza un motore di inoltro centralizzato (PFC) per l'inoltro del traffico. L'implementazione di un motore di inoltro centrale consente di tenere traccia delle statistiche del traffico per una determinata VLAN. Questo processo può essere utilizzato per applicare un policer aggregato a una VLAN.

Su una scheda di linea abilitata DFC, tuttavia, le decisioni di inoltro vengono distribuite a tale scheda di linea. La DFC è a conoscenza solo delle porte presenti sulla scheda di linea immediata e non del traffico su altre schede di linea. Per questo motivo, se un policer aggregato viene applicato a una VLAN con porte membro su più moduli DFC, il policer potrebbe produrre risultati incoerenti. Il motivo è che la DFC può solo tenere traccia delle statistiche delle porte locali e non tiene conto delle statistiche delle porte sulle altre schede di linea. Per questo motivo, un policer aggregato applicato a una VLAN con porte membro su una scheda di linea DFC attivate causerà il superamento del limite classificato per le porte VLAN residenti solo sulla scheda di linea DFC.

CatOS (DSCP Markdown Maps)

Le mappe di markdown DSCP vengono utilizzate quando il policer è definito per marcare il traffico fuori profilo invece di eliminarlo. Il traffico esterno al profilo è definito come il traffico che supera l'impostazione di frammentazione definita.

Quando QoS è abilitato, viene impostata una mappa di markdown DSCP predefinita. Questa mappa di markdown predefinita è elencata in questa tabella nelle prime parti del documento.

L'interfaccia della riga di comando (CLI) consente agli amministratori di modificare la mappa di markdown predefinita tramite il comando **set qos policed-dscp-map**. Di seguito è riportato un esempio.

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

Questo esempio modifica la mappa DSCP controllata in modo che rifletta il fatto che i valori DSCP da 20 a 25 verranno contrassegnati con un valore DSCP di 7 e i valori DSCP da 33 a 38 verranno contrassegnati con un valore DSCP di 3.

Mappatura dei criteri su VLAN e porte (CatOS)

Dopo aver compilato l'ACL, occorre mapparlo a una porta o a una VLAN in modo che l'ACL abbia effetto.

Un comando interessante che rileva molti elementi inconsapevoli è l'impostazione QoS predefinita che rende tutte le porte QoS basate. L'applicazione di un'aggregazione (o microflusso) a una VLAN non avrà effetto su una porta a meno che questa non sia stata configurata per la QoS basata su VLAN.

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

Se si modifica la QoS basata sulla porta in QoS basata sulla VLAN, tutti gli ACL assegnati a quella porta vengono immediatamente scollegati e tutti gli ACL basati sulla VLAN vengono assegnati a quella porta.

Per mappare l'ACL a una porta (o VLAN), usare il comando seguente:

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

Anche dopo aver mappato l'ACL a una porta (o a una VLAN), l'effetto dell'ACL rimane attivo solo dopo il commit dell'ACL nell'hardware. Questa procedura è descritta nella sezione seguente. A questo punto, l'ACL risiede in un buffer di modifica temporaneo in memoria. In questo buffer, è possibile modificare l'ACL.

Per rimuovere gli ACL non salvati che risiedono nel buffer di modifica, usare il comando **rollback**. Questo comando essenzialmente elimina l'ACL dal buffer di modifica.

```
Console> (enable) rollback qos acl test-acl
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

Commit degli ACL (CatOS)

Per applicare l'ACL QoS definito (in precedenza), è necessario eseguire il commit dell'ACL nell'hardware. Processo di commit delle copie dell'ACL dal buffer temporaneo all'hardware PFC. Una volta residente nella memoria PFC, il criterio definito nell'ACL QoS può essere applicato a tutto il traffico che corrisponde all'ACL

Per semplificare la configurazione, la maggior parte degli amministratori utilizza il comando **commit all**. Tuttavia, è possibile eseguire il commit di un ACL specifico (uno dei tanti) che attualmente potrebbe risiedere nel buffer di modifica. Di seguito è riportato un esempio del comando commit.

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

Se si desidera rimuovere un ACL da una porta (o da una VLAN), è necessario cancellare la mappa che associa l'ACL a quella porta (o VLAN) usando il comando seguente:

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

Configurazione della policy sulla famiglia Catalyst 6000 con Cisco IOS integrato (modalità nativa)

Il Policing è supportato con Cisco IOS integrato (modalità nativa). Tuttavia, la configurazione e l'implementazione della funzione di policing sono ottenute utilizzando mappe delle politiche. Ogni mappa utilizza più classi di criteri per creare una mappa dei criteri che possono essere definite per diversi tipi di flussi di traffico.

Le classi della mappa dei criteri, quando si filtra, utilizzano ACL basati su IOS e istruzioni di corrispondenza delle classi per identificare il traffico da sottoporre a policy. Una volta identificato il traffico, le classi di criteri possono utilizzare i criteri di aggregazione e microflusso per applicare i criteri di controllo al traffico corrispondente.

Nelle sezioni seguenti viene illustrata in modo molto più dettagliato la configurazione del policing per la modalità integrata Cisco IOS (modalità nativa).

Aggregati e microflussi (Cisco IOS integrato (modalità nativa))

Aggregati e microflussi sono termini utilizzati per definire l'ambito di applicazione delle policy eseguito dal PFC. Analogamente a CatOS, gli aggregati e i microflussi sono utilizzati anche in Cisco IOS integrato (modalità nativa).

Un microflusso definisce il controllo di un singolo flusso. Un flusso viene definito da una sessione con un indirizzo MAC SA/DA univoco, un indirizzo IP SA/DA e numeri di porta TCP/UDP. Per ogni nuovo flusso avviato tramite una porta di una VLAN, il microflusso può essere utilizzato per limitare la quantità di dati ricevuti per quel flusso dallo switch. Nella definizione di microflusso, i pacchetti che superano il limite di velocità prescritto possono essere scartati o avere il valore DSCP contrassegnato per difetto. I microflussi vengono applicati utilizzando il comando Police flow che fa parte di una classe mappa dei criteri.

Per abilitare il controllo del microflusso in modalità integrata Cisco IOS (modalità nativa), è necessario abilitarlo a livello globale sullo switch. A tale scopo, eseguire il comando seguente:

```
Cat6500(config)# mls qos flow-policing
```

Il monitoraggio del microflusso può essere applicato anche al traffico con bridging, ovvero al traffico che non è commutato con L3. Per abilitare lo switch al supporto del monitoraggio del

microflusso sul traffico con bridging, eseguire il comando seguente:

```
Cat6500(config)# mls qos bridged
```

Questo comando abilita anche il controllo del microflusso per il traffico multicast. Se il traffico multicast deve avere un policer di microflusso applicato, questo comando (**mls qos bridged**) deve essere abilitato.

Analogamente a un microflusso, un aggregato può essere utilizzato per limitare il traffico. Tuttavia, la velocità di aggregazione si applica a tutto il traffico in entrata su una porta o su una VLAN che corrisponde a un ACL QoS specificato. È possibile visualizzare l'aggregazione come il policing del traffico cumulativo che corrisponde a un profilo di traffico definito.

In modalità integrata Cisco IOS (modalità nativa) è possibile definire due forme di aggregati, come illustrato di seguito:

- policy di aggregazione per interfaccia
- criteri aggregati denominati

Gli aggregati per interfaccia vengono applicati a una singola interfaccia eseguendo il comando **Police** all'interno di una classe mappa dei criteri. Queste classi di mappe possono essere applicate a più interfacce, ma il policer regola ogni interfaccia separatamente. Gli aggregati denominati vengono applicati a un gruppo di porte e al traffico di polizia in tutte le interfacce in modo cumulativo. Le aggregazioni denominate vengono applicate usando il comando **mls qos aggregate policer**.

Quando si definiscono i microflussi, è possibile definirne fino a 63 e definire fino a 1023 aggregati.

Creazione delle regole di policy (Cisco IOS integrato (modalità nativa))

Il processo di creazione di una regola di controllo implica la creazione di un'aggregazione (o microflusso) tramite una mappa dei criteri e quindi l'associazione di tale mappa a un'interfaccia.

Si consideri lo stesso esempio creato per CatOS. Il requisito era quello di limitare tutto il traffico IP in entrata sulla porta 5/3 a un massimo di 20 MBPS.

Innanzitutto, è necessario creare una mappa dei criteri. Creare una mappa dei criteri denominata limit-traffic. A tal fine:

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

Si noterà immediatamente che il prompt dello switch cambia per riflettere il fatto che l'utente si trova nella modalità di configurazione per la creazione di una classe mappa. Tenere presente che una mappa dei criteri può contenere più classi. Ogni classe contiene un set separato di azioni dei criteri che possono essere applicate a diversi flussi di traffico.

Creeremo una classe di traffico per limitare specificamente il traffico in entrata a 20 MBPS. Chiameremo questa classe limit-to-20, come mostrato di seguito.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
Cat6500(config-pmap-c)#
```

Il prompt cambia di nuovo per indicare che la configurazione corrente è quella della classe di mappa (mostrata con la lettera -c alla fine del prompt). Se si desidera applicare il limite di velocità in modo che corrisponda al traffico in entrata specifico, è possibile configurare un ACL e applicarlo al nome della classe. Per applicare il limite di 20 MBPS al traffico proveniente dalla rete 10.10.1.x, usare il seguente ACL:

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

Èpossibile aggiungere questo ACL al nome della classe nel modo seguente:

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

Una volta definita la mappa della classe, è possibile definire i singoli policer per tale classe. È possibile creare aggregati (utilizzando la parola chiave Police) o microflussi (utilizzando la parola chiave Police flow). Creare l'aggregazione come illustrato di seguito.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

L'istruzione class sopra riportata (comando **Police**) imposta un limite di velocità di 20000 k (20 MBPS) con una frammentazione di 52 MBPS (13000 x 4000 = 52 MB). Se il traffico corrisponde al profilo e rientra nel limite nominale, l'azione viene impostata dall'istruzione di conferma-azione per trasmettere il traffico nel profilo. Se il traffico è fuori profilo (ossia, nell'esempio riportato sopra il limite di 20 MB), l'istruzione di superamento viene impostata in modo da interrompere il traffico (ossia, nell'esempio riportato, tutto il traffico superiore a 20 MB viene interrotto).

Quando si configura un microflusso, viene eseguita un'azione simile. Se si desidera limitare a 200 K ciascuno tutti i flussi in una porta corrispondente a una determinata mappa di classe, la configurazione di tale flusso sarà simile alla seguente:

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

Mappe markdown DSCP

Le mappe di markdown DSCP vengono utilizzate quando il policer è definito per marcare il traffico

fuori profilo invece di eliminarlo. Il traffico esterno al profilo è definito come il traffico che supera l'impostazione di frammentazione definita.

Quando QoS è abilitato, viene stabilita una mappa di markdown DSCP predefinita. Questa mappa di markdown predefinita è elencata in questa tabella. La CLI consente agli amministratori di modificare la mappa di markdown predefinita usando il comando **set qos policed-dscp-map**. Di seguito è riportato un esempio.

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

Questo esempio definisce una modifica alla mappa DSCP predefinita sottoposta a policy in base alla quale il valore DSCP di 32 verrà contrassegnato con un valore DSCP pari a 16. Per una porta con questo policer definito, il valore DSCP di tutti i dati in arrivo con questo valore DSCP che fanno parte di un blocco di dati in eccesso rispetto alla frammentazione dichiarata verrà contrassegnato con un valore DSCP inferiore a 16.

Mappatura dei criteri su VLAN e porte (Cisco IOS integrato (modalità nativa))

Dopo la creazione, i criteri devono essere mappati a una porta o a una VLAN per renderli effettivi. A differenza del processo di commit in CatOS, non esiste un equivalente in Cisco IOS integrato (modalità nativa). Quando un criterio è mappato a un'interfaccia, il criterio è attivo. Per mappare il criterio sopra indicato a un'interfaccia, eseguire il comando seguente:

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

Se una policy è mappata a una VLAN, per ciascuna porta della VLAN a cui si desidera applicare la policy VLAN, è necessario informare l'interfaccia che QoS è basato su VLAN usando il comando **mls qos vlan-based**.

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

Supponendo che l'interfaccia 3/5 faccia parte della VLAN 100, la policy denominata limit-traffic applicata alla VLAN 100 si applicherà anche all'interfaccia 3/5.

Configurazione della classificazione sulla famiglia Catalyst 6000 con CatOS

Il PFC introduce il supporto per la classificazione dei dati tramite ACL in grado di visualizzare le informazioni delle intestazioni L2, L3 e L4. Per un SupI, o IA (senza PFC), la classificazione è limitata all'utilizzo delle parole chiave trust sulle porte.

Nella sezione seguente vengono descritti i componenti di configurazione QoS utilizzati dal PFC per la classificazione nel software CatOS.

Mapping da CO a DSCP (CatOS)

All'ingresso dello switch, un frame avrà un valore DSCP impostato dallo switch. Se la porta è in uno stato attendibile e l'amministratore ha utilizzato la parola chiave trust-COs, il valore CO impostato nel fotogramma verrà utilizzato per determinare il valore DSCP impostato per il fotogramma. Come accennato in precedenza, lo switch può assegnare i livelli di servizio al frame mentre attraversa lo switch in base al valore DSCP interno.

Questa parola chiave su alcuni dei moduli 10/100 precedenti (WS-X6248 e WS-X6348) non è supportata. Per questi moduli, si consiglia di utilizzare gli ACL per applicare le impostazioni dei CO ai dati in ingresso.

Quando QoS è abilitato, lo switch crea una mappa predefinita. Questa mappa viene utilizzata per identificare il valore DSCP che verrà impostato in base al valore CO. Queste mappe sono elencate in questa tabella più indietro nel documento. In alternativa, l'amministratore può impostare una mappa univoca. Di seguito è riportato un esempio.

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```

Il comando precedente imposta la mappa seguente:

CO	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Anche se è molto improbabile che la mappa sopra riportata venga utilizzata in una rete reale, serve per dare un'idea di quello che può essere raggiunto utilizzando questo comando.

Mappatura IP Precedence to DSCP (CatOS)

Analogamente alla mappa DSCP, un frame può avere un valore DSCP determinato dall'impostazione di precedenza IP dei pacchetti in ingresso. Questo problema si verifica solo se la porta è impostata come trusted dall'amministratore e se è stata utilizzata la parola chiave trust-ipprec.

Quando QoS è abilitato, lo switch crea una mappa predefinita. In questa tabella viene fatto riferimento in precedenza in questo documento. Questa mappa viene utilizzata per identificare il valore DSCP che verrà impostato in base al valore di precedenza IP. In alternativa, l'amministratore può impostare una mappa univoca. Di seguito è riportato un esempio:

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```

Il comando precedente imposta la mappa seguente:

Precedenza IP	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Anche se è molto improbabile che la mappa sopra riportata venga utilizzata in una rete reale, serve per dare un'idea di quello che può essere raggiunto utilizzando questo comando.

Classificazione (CatOS)

Quando un frame viene passato alla PFC per l'elaborazione, il processo di classificazione viene eseguito sul frame. Il PFC utilizzerà un ACL preconfigurato (o un ACL predefinito) per assegnare un DSCP al frame. Nell'ACE, per assegnare un valore DSCP viene utilizzata una delle quattro parole chiave disponibili. Essi sono i seguenti:

1. TRUST-DSCP (solo ACL IP)
2. TRUST-IPPREC (solo ACL IP)
3. TRUST-COS (tutti gli ACL tranne IPX e MAC su una PFC2)
4. DSCP

La parola chiave TRUST-DSCP presume che il frame in arrivo nel PFC abbia già un valore DSCP impostato prima di entrare nello switch. Lo switch conserva questo valore DSCP.

Con TRUST-IPPREC, il PFC deriva un valore DSCP dal valore di precedenza IP esistente residente nel campo ToS. Il PFC utilizzerà la precedenza IP per le mappe DSCP per assegnare il DSCP corretto. Quando QoS è abilitato sullo switch, viene creata una mappa predefinita. In alternativa, è possibile utilizzare una mappa creata dall'amministratore per derivare il valore DSCP.

Analogamente a TRUST-IPPREC, la parola chiave TRUS-COS indica al PFC di derivare un valore DSCP dai CO nell'intestazione del frame. Per assistere il PFC nella derivazione del DSCP, è inoltre disponibile una mappa dei CO per DSCP (di default assegnata a un amministratore).

La parola chiave DSCP viene usata quando un frame arriva da una porta non attendibile. Ciò presenta una situazione interessante per derivare il DSCP. A questo punto, il DSCP configurato nell'istruzione set qos acl viene utilizzato per derivare il DSCP. Tuttavia, è a questo punto che gli ACL possono essere utilizzati per derivare un DSCP per il traffico in base ai criteri di classificazione impostati nell'ACE. Ciò significa che in una ACE è possibile utilizzare criteri di classificazione quali l'indirizzo di origine e di destinazione IP, i numeri di porta TCP/UDP, i codici ICMP, il tipo IGMP, i numeri di rete e di protocollo IPX, gli indirizzi di origine e di destinazione MAC e gli Ethertype (solo per il traffico non IP e non IPX) per identificare il traffico. Ciò significa che una voce ACE può essere configurata per assegnare un valore DSCP specifico per indicare il traffico HTTP sul traffico FTP.

Si consideri l'esempio seguente:

```
Console> (enable) set port qos 3/5 trust untrusted
```

Se si imposta una porta come non attendibile, la PFC utilizzerà un ACE per derivare il DSCP per il frame. Se la voce ACE è configurata con criteri di classificazione, i singoli flussi da tale porta possono essere classificati con priorità diverse. Di seguito è riportata un'illustrazione degli assi:

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

In questo esempio sono presenti due istruzioni ACE. La prima identifica qualsiasi flusso TCP (la parola chiave any viene utilizzata per identificare il traffico di origine e di destinazione) il cui numero di porta è 80 (80 = HTTP) a cui assegnare un valore DSCP pari a 32. La seconda ACE identifica il traffico proveniente da qualsiasi host e destinato a qualsiasi host il cui numero di porta TCP è 21 (FTP) a cui assegnare un valore DSCP pari a 16.

Configurazione della classificazione sulla famiglia Catalyst 6000 con Cisco IOS integrato (modalità nativa)

Nella sezione seguente vengono descritti i componenti della configurazione QoS utilizzati per supportare la classificazione nel PFC con Cisco IOS integrato (modalità nativa).

Mappatura CO a DSCP (Cisco IOS integrato (modalità nativa))

All'ingresso dello switch, un frame avrà un valore DSCP impostato dallo switch. Se la porta è in uno stato attendibile e l'amministratore ha utilizzato la parola chiave mls qos trust-COs (sulle porte GE o sulle porte 10/100 sulle schede di linea WS-X6548), il valore CO impostato nel frame verrà utilizzato per determinare il valore DSCP impostato per il frame. Come accennato in precedenza, lo switch può assegnare i livelli di servizio al frame mentre attraversa lo switch in base al valore DSCP interno.

Quando QoS è abilitato, lo switch crea una mappa predefinita. Fare riferimento a questa tabella per le impostazioni predefinite. Questa mappa viene utilizzata per identificare il valore DSCP che verrà impostato in base al valore CO. In alternativa, l'amministratore può impostare una mappa univoca. Di seguito è riportato un esempio.

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

Il comando precedente imposta la mappa seguente:

CO	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Anche se è molto improbabile che la mappa sopra riportata venga utilizzata in una rete reale, serve per dare un'idea di quello che può essere raggiunto utilizzando questo comando.

Mappatura IP Precedence to DSCP (Cisco IOS integrato (modalità nativa))

Analogamente alla mappa DSCP, un frame può avere un valore DSCP determinato dall'impostazione di precedenza IP dei pacchetti in ingresso. Questo problema si verifica solo se la porta è impostata come trusted dall'amministratore e se è stata utilizzata la parola chiave mls qos trust-ipprec. Questa parola chiave è supportata solo sulle porte GE e sulle porte 10/100 sulle schede di linea WS-X6548. Per le porte 10/100 sulle schede di linea WS-X6348 e WS-X6248, è consigliabile utilizzare gli ACL per assegnare l'attendibilità della precedenza IP ai dati in arrivo.

Quando QoS è abilitato, lo switch crea una mappa predefinita. Fare riferimento a questa tabella per le impostazioni predefinite. Questa mappa viene utilizzata per identificare il valore DSCP che verrà impostato in base al valore di precedenza IP. In alternativa, l'amministratore può impostare una mappa univoca. Di seguito è riportato un esempio.

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

Il comando precedente imposta la mappa seguente:

Precedenza IP	0	1	2	3	4	5	6	7

DSCP	20	30	1	43	63	12	13	8

Anche se è molto improbabile che la mappa sopra riportata venga utilizzata in una rete reale, serve per dare un'idea di quello che può essere raggiunto utilizzando questo comando.

Classificazione (Cisco IOS integrato (modalità nativa))

Quando un frame viene passato alla PFC, è possibile eseguire il processo di classificazione per assegnare una nuova priorità a un frame in ingresso. Ciò è possibile solo se il frame proviene da una porta non attendibile o se il frame è stato classificato come non attendibile.

Un'azione di classe mappa dei criteri può essere utilizzata per:

1. TRUST CO
2. TRUST IP-PRECEDENCE
3. DSCP ATTENDIBILE
4. NESSUNA ATTENDIBILITÀ

La parola chiave TRUST DSCP presume che il frame in arrivo nel PFC abbia già un valore DSCP impostato prima di entrare nello switch. Lo switch conserva questo valore DSCP.

Con TRUST IP-PRECEDENCE, il PFC deriva un valore DSCP dal valore di precedenza IP esistente residente nel campo ToS. Il PFC utilizzerà una precedenza IP per la mappa DSCP per assegnare il DSCP corretto. Quando QoS è abilitato sullo switch, viene creata una mappa predefinita. In alternativa, è possibile utilizzare una mappa creata dall'amministratore per derivare il valore DSCP.

Analogamente a TRUST IP-PRECEDENCE, la parola chiave TRUST COs indica al PFC di derivare un valore DSCP dai CO nell'intestazione del frame. Per assistere il PFC nella derivazione del DSCP, è inoltre disponibile una mappa dei CO per DSCP (di default assegnata a un amministratore).

Di seguito è riportato un esempio di derivazione di DSCP da una priorità esistente (DSCP, IP precedence o CO).

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

La mappa di classe sopra riportata deriva il valore DSCP dai CO nell'intestazione Ethernet.

Il formato NO TRUST della parola chiave viene utilizzato quando un frame arriva da una porta non attendibile. Ciò consente al frame di avere un valore DSCP assegnato durante il processo di policing.

Considerare l'esempio seguente relativo alla modalità di assegnazione di una nuova priorità (DSCP) a flussi diversi in arrivo nel PFC utilizzando la definizione di criterio seguente.

```
Cat6500(config)# access-list 102 permit tcp any any eq http
```

```
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-
c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

L'esempio precedente mostra quanto segue:

1. Creazione di un ACL per identificare i flussi http in entrata nella porta.
2. Mappa dei criteri denominata new-dscp-for-flow.
3. Mappa di classe (test names) che utilizza l'elenco degli accessi 102 per identificare il traffico per il quale la mappa di classe eseguirà l'azione.
4. Il test della mappa di classe imposterà lo stato di attendibilità per il frame in ingresso su non attendibile e assegnerà un DSCP di 24 a tale flusso.
5. Questa mappa di classe limiterà inoltre l'aggregazione di tutti i flussi http a un massimo di 1 MB.

COPS (Common Open Policy Server)

COPS è un protocollo che consente alla famiglia Catalyst 6000 di configurare la funzionalità QoS da un host remoto. Al momento, il COPS è supportato solo tramite CatOS e fa parte dell'architettura intserv per QoS. Attualmente non è disponibile alcun supporto (alla data del presente documento) per COPS quando si utilizza Cisco IOS (modalità nativa) integrato. Il protocollo COPS trasferisce le informazioni di configurazione QoS allo switch, ma non è l'origine delle informazioni di configurazione QoS. L'uso del protocollo COPS richiede un gestore QoS esterno per ospitare le configurazioni QoS per lo switch. Il gestore QoS esterno avvierà il push verso il basso di tali configurazioni allo switch utilizzando il protocollo COPS. QoS Policy Manager (QPM) di Cisco è un esempio di QoS Manager esterno.

In questo documento non viene spiegato il funzionamento di QPM, bensì viene spiegato come configurare lo switch in modo da supportare le configurazioni QoS esterne usando QPM.

Configurazione COPS

Per impostazione predefinita, il supporto COPS è disabilitato. Per utilizzare COPS sullo switch, è necessario attivarlo. A tale scopo, eseguire il comando seguente:

```
Console> (enable) set qos policy-source cops
!-- QoS policy source for the switch set to COPS. Console> (enable)
```

Quando questo comando viene avviato, alcuni valori di configurazione QoS predefiniti verranno originati dal server COPS. Tra questi:

1. Mapping da CO a coda
2. Assegnazioni delle soglie delle code di input e output
3. Assegnazioni larghezza di banda WRR
4. Qualsiasi criterio di aggregazione e microflusso
5. Mappe da DSCP a CO per il traffico in uscita
6. ACL
7. Assegnazioni predefinite CO porte

Quando le configurazioni QoS vengono eseguite utilizzando COPS, è importante tenere presente che l'applicazione di tali configurazioni viene applicata in modo diverso. Anziché configurare direttamente le porte, il protocollo COPS viene utilizzato per configurare l'ASIC della porta. L'ASIC della porta in genere controlla un gruppo di porte, pertanto la configurazione COPS viene applicata contemporaneamente a più porte.

L'ASIC della porta configurato è l'ASIC GE. Sulle schede di linea GE, sono presenti quattro porte per GE (porte 1-4, 5-8, 9-12, 13-16). Su queste schede di linea, la configurazione COPS influisce su ciascun gruppo di porte. Sulle schede di linea 10/100 (come indicato in precedenza in questo documento), sono disponibili due gruppi di ASIC, GE e 10/100 ASIC. Un ASIC GE esiste per quattro ASIC 10/100. Ogni ASIC 10/100 supporta 12 porte 10/100. COPS configura l'ASIC GE. Pertanto, quando si applica la configurazione QoS alle schede di linea 10/100 tramite COPS, la configurazione si applica a tutte le 48 porte 10/100.

Quando si abilita il supporto COPS con il comando **set qos policy-source cops**, la configurazione QoS tramite COPS viene applicata a tutti gli ASIC dello chassis dello switch. È possibile applicare la configurazione COPS a ASIC specifici. A tale scopo, è possibile utilizzare il comando seguente:

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```

Come si evince dall'applicazione del comando sopra riportato, il comando è stato emesso su un modulo GE quando il comando ha avuto effetto su quattro porte.

Server dei punti di decisione e nomi di dominio

I server dei punti di decisione delle policy (PDPS) sono i responsabili delle policy esterne utilizzati per archiviare i dettagli di configurazione QoS spostati sullo switch. Se sullo switch è abilitato il COPS, lo switch deve essere configurato con l'indirizzo IP del gestore esterno che fornirà i dettagli di configurazione QoS allo switch. Analogamente, quando SNMP è abilitato e l'indirizzo IP del programma di gestione SNMP è definito.

Il comando per identificare i PDF esterni viene eseguito utilizzando quanto segue:

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```

Il comando precedente identifica il dispositivo 192.168.1.1 come server del punto di decisione principale.

Quando lo switch comunica con i PDP, deve far parte di un dominio definito nei PDP. Il PDPS comunica solo con gli switch che fanno parte del suo dominio definito, quindi lo switch deve essere configurato per identificare il dominio COPS a cui appartiene. A tale scopo, eseguire il comando seguente:

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```

Il comando precedente mostra lo switch configurato per far parte del dominio denominato remote-cat6k. Questo dominio deve essere definito in QPM e lo switch deve essere aggiunto a tale dominio.

Informazioni correlate

- Switch - Supporto dei prodotti
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems