Classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS

Sommario

Introduzione
Operazioni preliminari
Convenzioni
Prerequisiti
Componenti usati
Terminologia
Abilitazione di QoS
Gestione porta di input
Switching Engine (PFC)
Quattro possibili origini per DSCP interno
Quale delle quattro possibili origini di DSCP interno verrà utilizzata?
Riepilogo: Come viene scelto il DSCP interno?
Gestione porta di output
Note e limitazioni
ACL predefinito
trust-cos in limitazioni di voci ACL
Limitazioni delle schede di linea WS-X6248-xx, WS-X6224-xx e WS-X6348-xx
Riepilogo classificazione
Monitoraggio e verifica di una configurazione
Controllo della configurazione della porta
Controllo dell'ACL
Esempi di case study
Caso 1: Contrassegno sul bordo
Caso 2: Fiducia nel core solo con un'interfaccia Gigabit
Caso 3: Attendibilità nel core con una porta 62xx o 63xx nello chassis
Informazioni correlate

Introduzione

In questo documento viene esaminato ciò che accade durante il viaggio di un pacchetto all'interno dello chassis Catalyst 6000 relativamente alla marcatura e alla classificazione in diversi punti. Cita casi speciali, restrizioni e fornisce brevi casi di studio.

Questo documento non deve essere un elenco esaustivo dei comandi di Catalyst OS (CatOS) relativi alla qualità del servizio (QoS) o al contrassegno. Per ulteriori informazioni sull'interfaccia della riga di comando (CLI) di CatOS, consultare il seguente documento:

- Configurazione di QoS

Nota: questo documento considera solo il traffico IP.

Operazioni preliminari

Convenzioni

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

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Questo documento è valido per gli switch Catalyst serie 6000 con software CatOS e con uno dei seguenti Supervisor Engine:

- SUP1A + PFC
- SUP1A + PFC + MSFC
- SUP1A + PFC + MSFC2
- SUP2 + PFC2
- SUP2 + PFC2 + MSFC2

Tutti i comandi di esempio, tuttavia, sono stati provati su un Catalyst 6506 con SUP1A/PFC con software versione 6.3.

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

Terminologia

Di seguito è riportato un elenco della terminologia utilizzata nel presente documento:

- DSCP (Differentiated Services Code Point): I primi sei bit del byte Type of Service (ToS) nell'intestazione IP. DSCP è presente solo nel pacchetto IP.**Nota:** se si assegna anche un DSCP interno a ciascun pacchetto (IP o non IP), questa assegnazione del DSCP interno verrà descritta più avanti in questo documento.
- Precedenza IP: I primi tre bit del byte del tipo ToS nell'intestazione IP.
- CoS (Class of Service): L'unico campo che può essere utilizzato per contrassegnare un pacchetto sul layer 2 (L2). È costituito da uno dei tre bit seguenti:I tre bit dot1p nel tag dot1q del pacchetto IEEE dot1q.I tre bit chiamati "User Field" nell'intestazione dell'ISL (Inter-Switch Link) di un pacchetto ISL incapsulato.Non è presente alcun CoS in un pacchetto non dot1q o ISL.
- Classificazione: Processo utilizzato per selezionare il traffico da contrassegnare.
- Marcatura: Processo di impostazione di un valore DSCP di livello 3 (L3) in un pacchetto. In

questo documento, la definizione di marcatura viene estesa per includere l'impostazione dei valori di CoS L2.

Gli switch della famiglia Catalyst 6000 possono effettuare classificazioni in base ai tre parametri seguenti:

- DSCP
- Precedenza IP
- CoS

Gli switch della famiglia Catalyst 6000 stanno effettuando la classificazione e il contrassegno in diverse posizioni. Di seguito viene illustrato ciò che accade in questi diversi luoghi:

- Porta di ingresso (ASIC (Application-Specific Integrated Circuit) in entrata
- Motore di commutazione (Policy Feature Card (PFC))
- Porta di uscita (ASIC in uscita)

Abilitazione di QoS

Per impostazione predefinita, QoS è disabilitato sugli switch Catalyst 6000. Per abilitare QoS, usare il comando CatOS **set qos enable**.

Quando QoS è disabilitato, lo switch non esegue alcuna classificazione o contrassegno e, di conseguenza, ogni pacchetto lascia lo switch con la precedenza DSCP/IP di cui disponeva quando entra nello switch.

Gestione porta di input

Il parametro di configurazione principale per la porta in entrata, relativo alla classificazione, è lo stato di attendibilità della porta. Ogni porta del sistema può avere uno dei seguenti stati di trust:

- trust-ip-precedence
- trust-dscp
- trust-cos
- non attendibile

Nella parte restante di questa sezione viene descritto in che modo gli stati di attendibilità della porta influiscono sulla classificazione finale del pacchetto. Lo stato di attendibilità della porta può essere impostato o modificato utilizzando il seguente comando CatOS:

set port qos *mod*/**trust** *porta* **{untrusted | trust-cos | trust-ipprec | trust-dscp }**

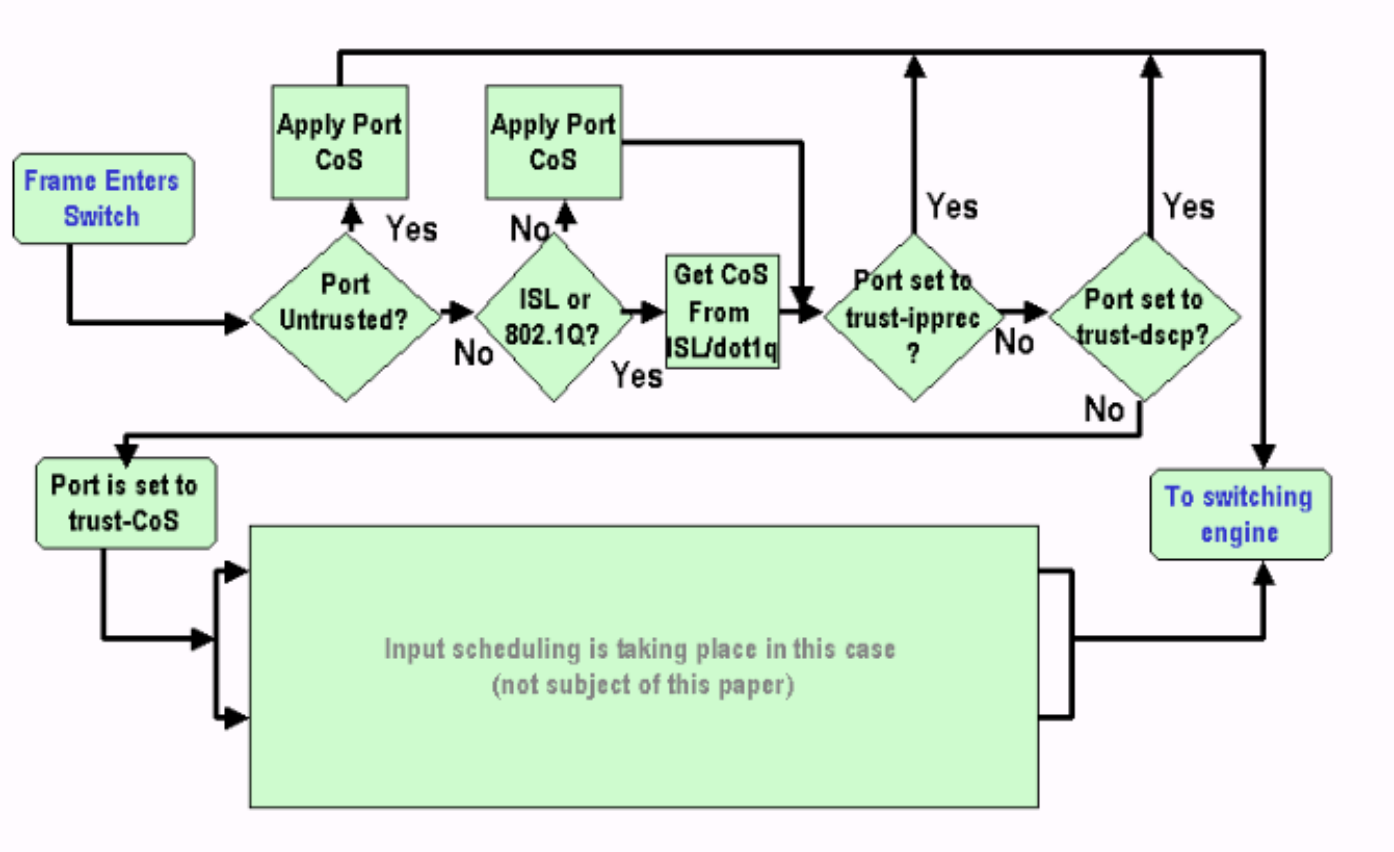
Nota: per impostazione predefinita, quando QoS è abilitato, tutte le porte sono in stato non attendibile.

A livello di porta di input è inoltre possibile applicare un CoS predefinito per porta, come nell'esempio seguente:

set port qos *mod/porta* **cos** *cos-value*

Se la porta è impostata su uno stato non attendibile, contrassegnare il frame con il CoS predefinito della porta e passare l'intestazione al motore di commutazione (PFC). Se la porta è impostata su

uno degli stati di attendibilità, applicare il CoS della porta predefinita (se il frame non dispone di un CoS ricevuto (dot1q o ISL)) o mantenere il CoS così com'è (per i frame dot1q e ISL) e passare il frame al motore di commutazione. La classificazione dell'input è illustrata nel seguente diagramma di flusso:



Nota: come mostrato nel diagramma di flusso sopra riportato, a ciascun frame viene assegnato un CoS interno (il CoS ricevuto o la porta predefinita), inclusi i frame senza tag che non hanno un CoS reale. Questo CoS interno e il DSCP ricevuto vengono scritti in un'intestazione speciale del pacchetto (chiamata intestazione del bus di dati) e inviati al motore di commutazione tramite il bus di dati. Ciò accade sulla scheda in entrata e a questo punto non è ancora noto se questo CoS interno sarà trasportato all'ASIC in uscita e inserito nel frame in uscita. Tutto questo dipende da ciò che il PFC fa e viene ulteriormente descritto nella sezione successiva.

Switching Engine (PFC)

Una volta che l'intestazione ha raggiunto il motore di commutazione, il motore di commutazione Encoded Address Recognition Logic (EARL) assegnerà a ciascun frame un DSCP interno. Questo DSCP interno è una priorità interna assegnata al frame dal PFC durante il transito sullo switch. Questo non è il DSCP nell'intestazione IPv4. Deriva da un'impostazione CoS o ToS esistente e viene utilizzata per reimpostare il CoS o il ToS quando il frame esce dallo switch. Questo DSCP interno viene assegnato a tutti i frame commutati (o instradati) dal PFC, anche ai frame non IP.

Quattro possibili origini per DSCP interno

Il DSCP interno deriva 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 ha configurato le mappe, verranno attivate le associazioni predefinite.

3. I bit CoS ricevuti sono già stati impostati prima che il frame entrasse nello switch o dal CoS predefinito della porta in ingresso se il frame in ingresso non contiene CoS. Come per la precedenza IP, esistono al massimo 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 già presente.
4. Il DSCP può essere impostato per il frame utilizzando un valore predefinito DSCP generalmente assegnato tramite una voce dell'elenco di controllo di accesso (ACL, Access Control List).

Per i numeri 2 e 3 nell'elenco di cui sopra, la mappatura statica utilizzata è per default, come segue:

- Il DSCP derivato è otto volte il CoS, per il mapping da CoS a DSCP.
- DSCP derivato è uguale a otto volte la precedenza IP, per la precedenza IP al mapping DSCP.

Questo mapping statico può essere ignorato dall'utente tramite i comandi seguenti:

set qos ipprec-dscp-map <dscp1> <dscp2>...<dscp8>

set qos cos-dscp-map <dscp1> <dscp2>...<dscp8>

Il primo valore del DSCP corrispondente alla mappatura per il CoS (o IP precedence) è "0", il secondo per il CoS (o IP precedence) è "1" e continua in questo schema.

Quale delle quattro possibili origini di DSCP interno verrà utilizzata?

In questa sezione vengono descritte le regole che determinano quale delle quattro possibili origini descritte in precedenza verrà utilizzata per ciascun pacchetto. Dipende dai seguenti parametri:

1. Quale ACL QoS verrà applicato al pacchetto? Ciò è determinato dalle seguenti regole:**Nota:** ogni pacchetto passa attraverso una voce ACL.Se alla porta o alla VLAN in ingresso non è collegato alcun ACL, applicare l'ACL predefinito.Se alla porta o alla VLAN in entrata è collegato un ACL e il traffico corrisponde a una delle voci dell'ACL, usare questa voce.Se alla porta o alla VLAN in arrivo è collegato un ACL e il traffico *non* corrisponde a una delle voci dell'ACL, usare l'ACL predefinito.
2. Ogni voce contiene una parola chiave di classificazione. Di seguito è riportato un elenco delle possibili parole chiave con le relative descrizioni:trust-ipprec: Il DSCP interno verrà derivato dalla precedenza IP ricevuta in base al mapping statico, indipendentemente dallo stato di trust della porta.trust-dscp: Il DSCP interno verrà derivato dal DSCP ricevuto indipendentemente dallo stato di attendibilità della porta.trust-cos: Il DSCP interno verrà derivato dal CoS ricevuto in base al mapping statico, se lo stato di trust tra porte è trusted (trust-cos, trust-dscp, trust-ipprec). Se lo stato di attendibilità della porta è trust-xx, il DSCP verrà derivato dalla porta predefinita CoS in base allo stesso mapping statico.dscp *xx*: Il DSCP interno dipenderà dai seguenti stati di attendibilità delle porte in ingresso:Se la porta non è considerata attendibile, il DSCP interno verrà impostato su *xx*.Se la porta è trust-dscp, il DSCP interno sarà il DSCP ricevuto nel pacchetto in arrivo.Se la porta è trust-CoS, il DSCP interno viene derivato dal CoS del pacchetto ricevuto.Se la porta è trust-ipprec, il DSCP

interno verrà derivato dalla precedenza IP del pacchetto ricevuto.

3. Ciascun ACL QoS può essere applicato a una porta o a una VLAN, ma è necessario considerare un parametro di configurazione aggiuntivo; il tipo di porta ACL. Una porta può essere configurata per essere basata su VLAN o su porta. Di seguito è riportata una descrizione dei due tipi di configurazione:Se la porta è configurata per essere basata su VLAN, cerca solo l'ACL applicato alla VLAN a cui appartiene la porta. Se alla porta è collegato un ACL, l'ACL verrà ignorato per il pacchetto in entrata su quella porta.Se una porta appartenente a una VLAN è configurata come basata sulla porta, anche se alla VLAN è collegato un ACL, non verrà presa in considerazione per il traffico in entrata da quella porta.

Di seguito viene riportata la sintassi con cui creare un ACL QoS per contrassegnare il traffico IP:

set qos acl ip ***acl_name*** **[dscp xx | trust-cos | trust-dscp | trust-ipprec]** ***regola di voce acl***

Il seguente ACL contrassegnerà tutto il traffico IP diretto all'host 1.1.1.1 con un DSCP di "40" e considererà attendibile-dscp per tutto il resto del traffico IP:

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

set qos acl TEST_ACL trust-dscp ip any any

Dopo aver creato l'ACL, è necessario mapparlo a una porta o a una VLAN, a tal fine, è possibile usare il comando seguente:

set qos acl map ***nome_acl*** **[modulo/porta] | VLAN]**

Per impostazione predefinita, ciascuna porta è basata sulla porta dell'ACL, quindi se si desidera collegare un ACL a una VLAN, è necessario configurare le porte di questa VLAN come basate sulla vlan. A tale scopo, eseguire il comando seguente:

set port qos ***module/port*** **vlan-based**

Per ripristinare la modalità basata sulla porta, è possibile usare il comando seguente:

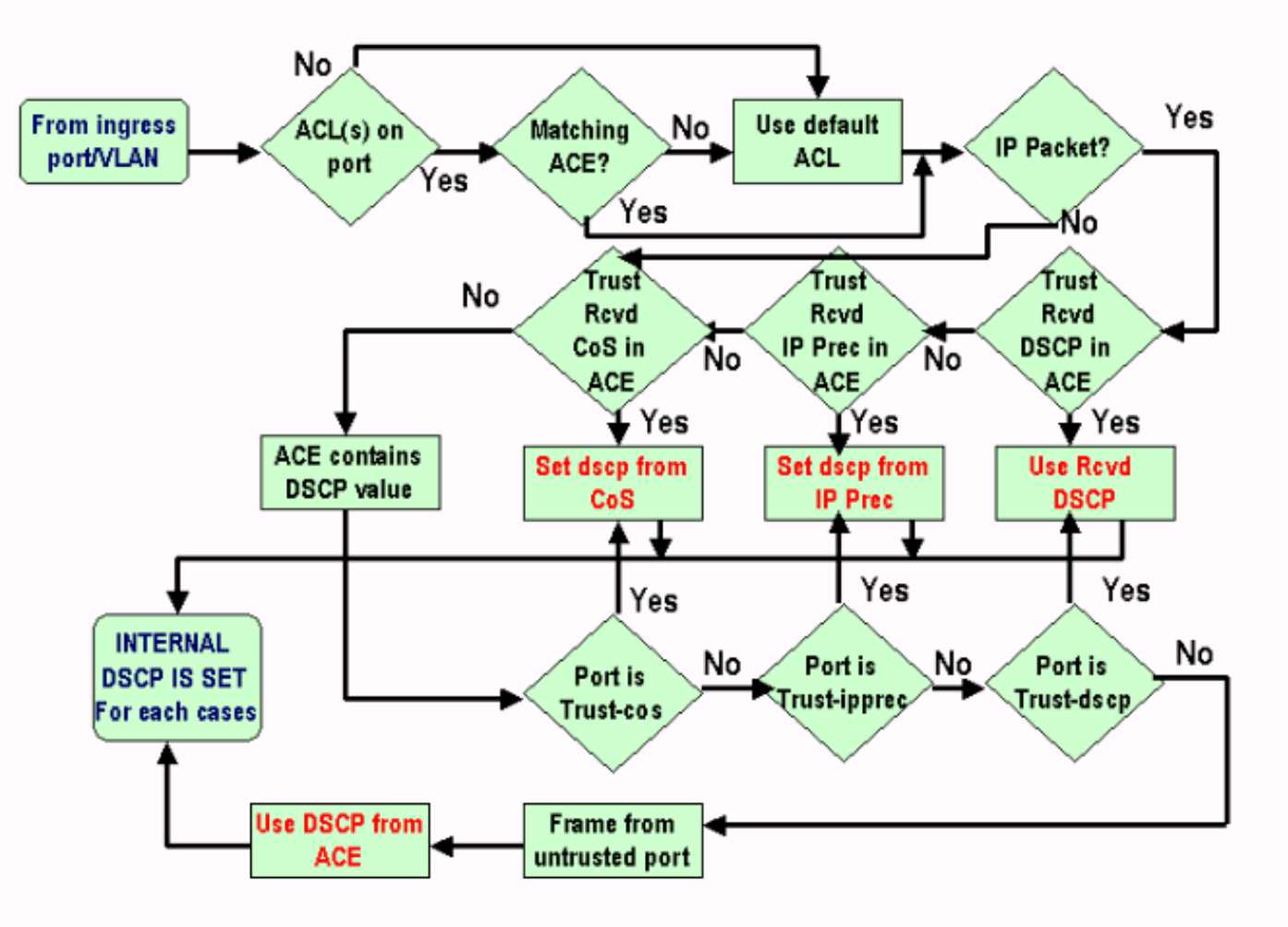
set port qos ***module/port*** **port-based**

Riepilogo: Come viene scelto il DSCP interno?

Il DSCP interno dipende dai seguenti fattori:

- stato trust porta
- ACL collegato alla porta
- ACL predefinito
- Basato su VLAN o su porta per quanto riguarda l'ACL

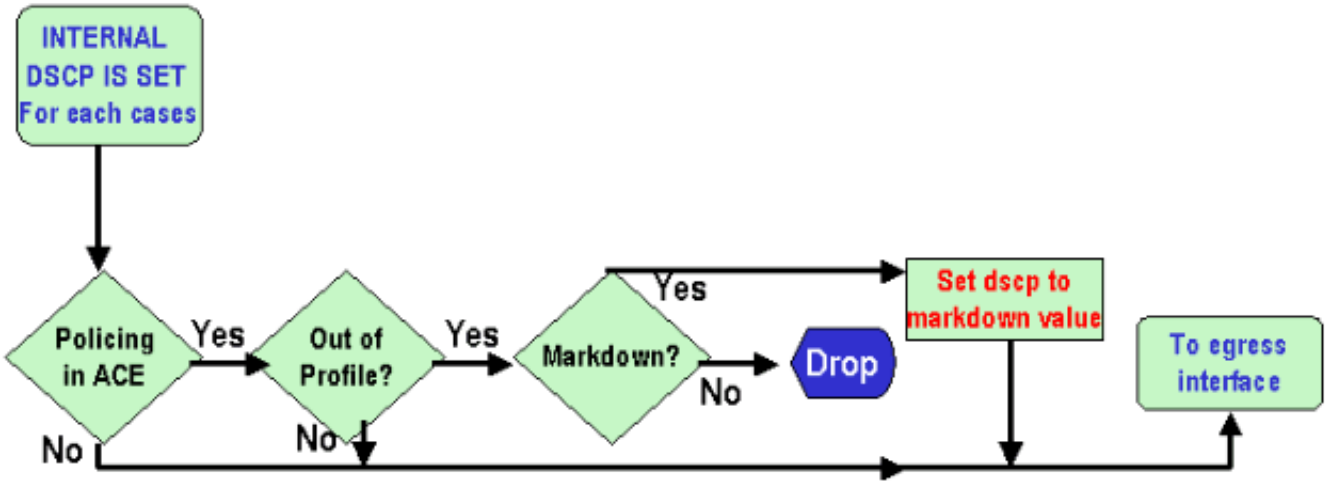
Il diagramma di flusso seguente riepiloga la modalità di scelta del DSCP interno in base alla configurazione:



Il PFC è anche in grado di eseguire il policing. Ciò potrebbe eventualmente determinare una riduzione del DSCP interno. Per ulteriori informazioni sul policing, consultare il seguente documento:

- Sorveglianza QoS su Catalyst 6000

Il seguente diagramma di flusso mostra come viene applicato il policer:



Gestione porta di output

Non è possibile modificare la classificazione a livello di porta di uscita, ma in questa sezione il pacchetto viene contrassegnato in base alle seguenti regole:

- Se il pacchetto è un pacchetto IPv4, copiare il DSCP interno assegnato dal motore di commutazione nel byte ToS dell'intestazione IPv4.
- Se la porta di output è configurata per un incapsulamento ISL o dot1q, utilizzare un CoS derivato dal DSCP interno e copiarlo nel frame ISL o dot1q.

Nota: il CoS deriva dal DSCP interno in base a un valore statico configurato dall'utente che esegue il comando seguente:

Nota: **set qos dscp-cos-map** ***dscp_list:cos_value***

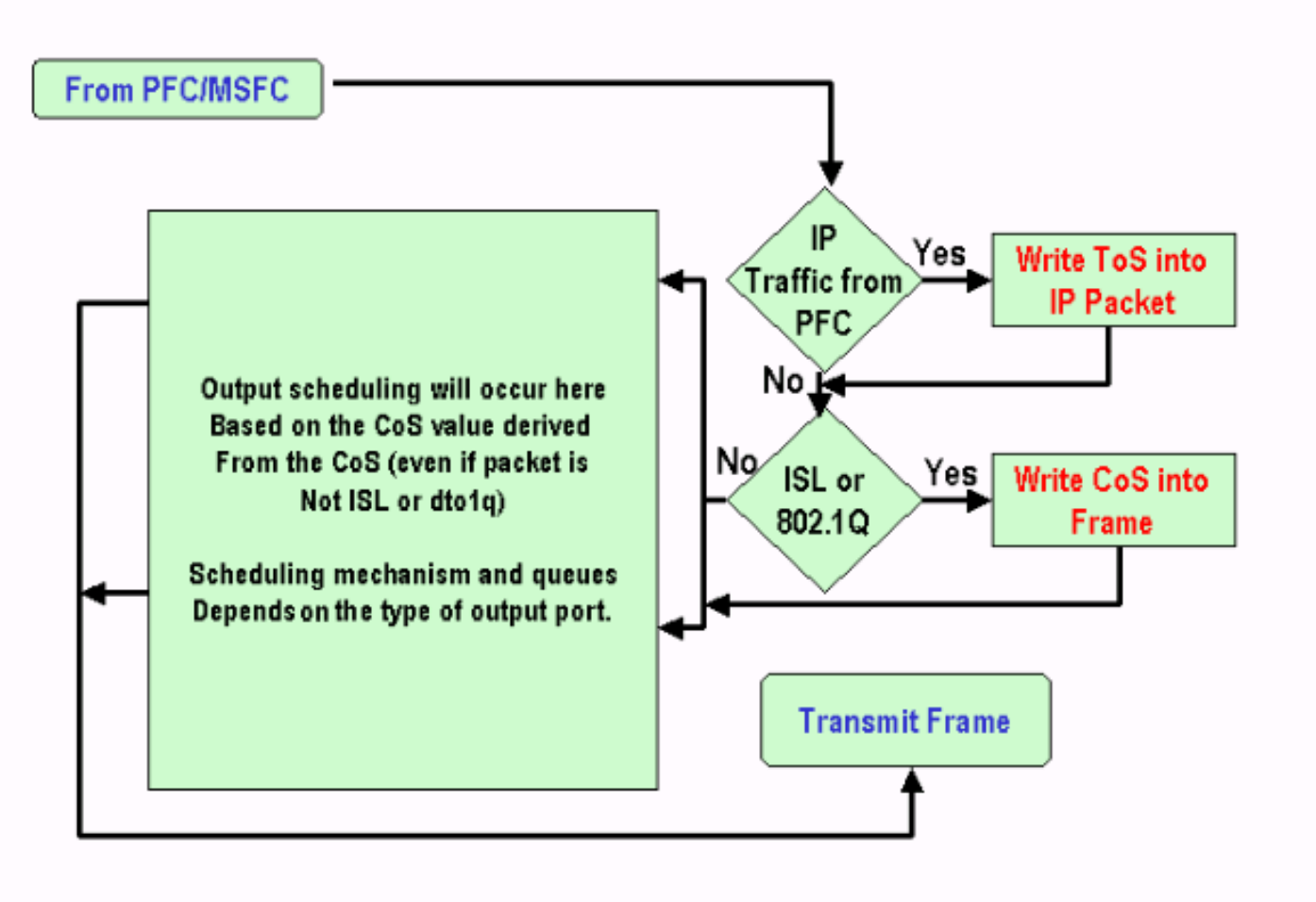
Nota: di seguito sono riportate le configurazioni predefinite. Per impostazione predefinita, il CoS è diviso per otto la parte intera del DSCP:

```
set qos dscp-cos-map 0-7:0
set qos dscp-cos-map 8-15:1
set qos dscp-cos-map 16-23:2
set qos dscp-cos-map 24-31:3
set qos dscp-cos-map 32-39:4
set qos dscp-cos-map 40-47:5
set qos dscp-cos-map 48-55:6
set qos dscp-cos-map 56-63:7
```

Una volta che il DSCP è scritto nell'intestazione IP e il CoS è derivato dal DSCP, il pacchetto viene inviato a una delle code di output per la pianificazione dell'output in base al CoS (anche se il pacchetto non è un dot1q o un ISL). Per ulteriori informazioni sulla pianificazione delle code di output, consultare il documento seguente:

- QoS sugli switch Catalyst serie 6000: Programmazione dell'output su Catalyst 6000 con PFC o PFC 2 con software CatOS

Il seguente diagramma di flusso riepiloga l'elaborazione del pacchetto riguardante il contrassegno nella porta di output:



Note e limitazioni

ACL predefinito

Per impostazione predefinita, l'ACL predefinito usa "dscp 0" come parola chiave di classificazione. Ciò significa che tutto il traffico che entra nello switch tramite una porta non attendibile verrà contrassegnato con un DSCP di "0" se QoS è abilitato. Per verificare l'ACL predefinito per l'IP, usare il comando seguente:

```
Boris-1> (enable) show qos acl  info default-action  ip
set qos acl default-action
-------------------------
ip dscp 0
```

Per modificare l'ACL predefinito, usare il comando seguente:

set qos acl default-action ip [dscp xx] | trust-CoS | trust-dscp | trust-ipprec]

trust-cos in limitazioni di voci ACL

Quando si utilizza la parola chiave trust-CoS all'interno di una voce, è presente un limite aggiuntivo. È possibile considerare attendibili i CoS in una voce solo se lo stato di attendibilità della ricezione non è non attendibile. Se si tenta di configurare una voce con trust-CoS, verrà visualizzato il seguente avviso:

```
Telix  (enable) set qos acl ip test_2 trust-CoS ip any any
Warning: ACL trust-CoS should only be used with ports that are also configured with port
trust=trust-CoS
test_2 editbuffer modified. Use 'commit' command to apply changes.
```

Questa limitazione è una conseguenza di quanto osservato in precedenza nella sezione Gestione porte di input. Come mostrato nel diagramma di flusso della sezione, se la porta non è attendibile, al frame viene immediatamente assegnata la porta predefinita CoS. Di conseguenza, il CoS in arrivo non viene mantenuto e non viene inviato al motore di commutazione, quindi non può essere considerato attendibile neanche con un ACL specifico.

Limitazioni delle schede di linea WS-X6248-xx, WS-X6224-xx e WS-X6348-xx

Questa sezione riguarda solo le seguenti schede di linea:

- WS-X624-100FX-MT: CATALYST 6000 100 FX MULTIMODE A 24 PORTE
- WS-X6248-RJ-45 : CATALYST 6000 10/100 RJ-45 MODULE A 48 PORTE
- WS-X6248-TEL: CATALYST 6000 10/100 TELCO MODULE A 48 PORTE
- WS-X6248A-RJ-45 : CATALYST 6000 10/100 A 48 PORTE, QOS MIGLIORATO
- WS-X6248A-TEL: CATALYST 6000 10/100 A 48 PORTE, QOS MIGLIORATO
- WS-X6324-100FX-MM: CATALYST 6000 100FX, ENH QOS, MT A 24 PORTE
- WS-X6324-100FX-SM: CATALYST 6000 100FX, ENH QOS, MT A 24 PORTE
- WS-X6348-RJ-45 : CATALYST 6000 10/100 A 48 PORTE, QO MIGLIORATO
- WS-X6348-RJ21V : CATALYST 6000 10/100 A 48 PORTE, ALIMENTAZIONE
- WS-X6348-RJ45V : CATALYST 6000 10/100 A 48 PORTE, ENH QOS, INLI NE POWER

Queste schede di linea, tuttavia, presentano alcune limitazioni aggiuntive:

- A livello di porta, non è possibile impostare trust-dscp o trust-ipprec.
- A livello di porta, se lo stato di attendibilità della porta è trust-CoS, si applicano le istruzioni seguenti:La soglia di ricezione per la programmazione dell'input è abilitata. Inoltre, il CoS nel pacchetto ricevuto viene usato per assegnare la priorità ai pacchetti per accedere al bus.Il CoS non verrà considerato attendibile e non verrà utilizzato per derivare il DSCP interno, a meno che non sia stato configurato anche l'ACL per il traffico in questione su trust-cos. Inoltre, non è sufficiente che le schede di linea abbiano trust-cos sulla porta, è necessario avere anche un ACL con trust-cos per quel traffico.
- Se lo stato di trust della porta non è attendibile, verrà eseguito il contrassegno normale (come nel caso standard). Dipende dall'ACL applicato al traffico.

Qualsiasi tentativo di configurare uno stato di attendibilità su una di queste porte visualizza uno dei seguenti messaggi di avviso:

```
telix (enable) set port qos 3/24 trust trust-ipprec
Trust type trust-ipprec not supported on this port.

telix (enable) set port qos 8/4 trust trust-dscp
Trust type trust-dscp not supported on this port.

telix (enable) set port qos 3/24 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/24.
Port  3/24 qos set to untrusted.
```

Riepilogo classificazione

Le tabelle che seguono mostrano il DSCP risultante classificato in base ai seguenti criteri:

- Stato di attendibilità della porta in ingresso.
- Parola chiave classification nell'ACL applicato.

Riepilogo della tabella generica per tutte le porte ad eccezione di WS-X62*xx* e WS-X63*xx*

Parola chiave ACL / Stato trust porta	dscp xx	trust-dscp	trust-ipprec	trust-CoS
Non attendibile	xx (1)	DSCP RX	derivato da Rx ipprec	0
trust-dscp	Rx-dscp	DSCP RX	derivato da Rx ipprec	derivato da Rx CoS o port CoS
trust-ipprec	derivato da Rx ipprec	DSCP RX	derivato da Rx ipprec	derivato da Rx CoS o port CoS
trust-CoS	derivato da Cisco Rx o CoS porta	DSCP RX	derivato da Rx ipprec	derivato da Rx CoS o port CoS

(1) Questo è l'unico modo per effettuare una nuova marcatura di un telaio.

Riepilogo tabella per WS-X62*xx* o WS-X63*xx*

Parola chiave ACL / Stato trust porta	dscp xx	trust-dscp	trust-ipprec	trust-CoS
Non attendibile	xx	DSCP RX	derivato da Rx ipprec	0
trust-dscp	Non supportato	Non supportato	Non supportato	Non supportato
trust-ipprec	Non supportato	Non supportato	Non supportato	Non supportato
trust-CoS	xx	DSCP RX	derivato da Rx ipprec	derivato da Rx CoS o port CoS

				(2)

(2) Questo è l'unico modo per conservare il CoS in entrata per il traffico proveniente da una scheda di linea 62*xx* o 63*xx*.

Monitoraggio e verifica di una configurazione

Controllo della configurazione della porta

Le impostazioni e le configurazioni della porta possono essere verificate usando il seguente comando:

show port qos *modulo/porta*

Tramite questo comando è possibile verificare, tra gli altri parametri, i seguenti parametri di classificazione:

- basato su porta o su VLAN
- tipo di porta trust
- ACL collegato alla porta

Di seguito è riportato un esempio di questo output del comando con i campi importanti relativi alla classificazione evidenziati:

```
tamer (enable) show port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.


Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 1/1    port-based     port-based      COPS           local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 1/1     1p2q2t       1p1q4t     untrusted     untrusted      0       0

(*)Runtime trust type set to untrusted.

Config:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                           IP

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                            IP
```

Nota: per ogni campo sono disponibili il parametro configurato e il parametro di runtime. Quello che verrà applicato al pacchetto è il parametro di runtime.

Controllo dell'ACL

Per verificare l'ACL applicato e quello visualizzato nei comandi precedenti, usare il comando seguente:

show qos acl info runtime *nome_acl*

```
tamer (enable) show qos acl info run test_2
set qos acl IP test_2
---------------------------------------------
1. dscp 32 ip any host 1.1.1.1
2. trust-dscp any
```

Esempi di case study

Gli esempi seguenti sono configurazioni di casi comuni che possono essere visualizzate in una rete.

Caso 1: Contrassegno sul bordo

Si supponga di configurare un Catalyst 6000 utilizzato come switch di accesso con molti utenti collegati allo slot 2, che è una scheda di linea WS-X6348 (10/100M). Gli utenti possono inviare quanto segue:

- Traffico dati normale: Questa condizione si verifica sempre nella VLAN 100 e deve essere restituito un DSCP di "0".
- Traffico vocale da un telefono IP: Questa condizione si trova sempre nella VLAN ausiliaria 101 e deve avere un DSCP di "40".
- Traffico di applicazioni mission critical: Questa condizione viene anche usata nella VLAN 100 e viene indirizzata al server 10.10.10.20. Il traffico deve avere un DSCP di "32".

Poiché nessuno di questi traffici è contrassegnato dall'applicazione, la porta rimarrà non attendibile e verrà configurato un ACL specifico per classificare il traffico. Un ACL verrà applicato alla VLAN 100 e un ACL alla VLAN 101. È necessario configurare tutte le porte come basate su VLAN. Di seguito è riportato un esempio della configurazione risultante:

```
set qos enable
set port qos 2/1-48 vlan-based
!--- Not needed, as it is the default. set port qos 2/1-48 trust untrusted set qos acl ip
Data_vlan dscp 32 ip any host 10.10.10.20 !--- Not needed, because if it is not present you
would !--- use the default ACL which has the same effect. Set qos acl ip Data_vlan dscp 0 ip any
any set qos acl ip Voice_vlan dscp 40 ip any any commit qos acl all set qos acl map Data_vlan
100 set qos acl map Voice_vlan 101
```

Caso 2: Fiducia nel core solo con un'interfaccia Gigabit

Si supponga di configurare un core Catalyst 6000 con solo un'interfaccia Gigabit nello slot 1 e nello slot 2 (senza schede di linea 62xx o 63xx nello chassis). Poiché il traffico è stato contrassegnato correttamente in precedenza dagli switch di accesso, non è necessario effettuare alcuna segnalazione, ma è necessario verificare che il DSCP in ingresso sia attendibile. Questo è il caso più semplice, in quanto tutte le porte verranno contrassegnate come trust-dscp e ciò dovrebbe essere sufficiente:

```
set qos enable
```

```
set port qos 1/1-2 trust trust-dscp
set port qos 2/1-16 trust trust-dscp
...
```

Caso 3: Attendibilità nel core con una porta 62xx o 63xx nello chassis

Si supponga di configurare un dispositivo di core/distribuzione con un collegamento Gigabit su una scheda di linea WS-X6416-GBIC (nello slot 2) e un collegamento 10/100 su una scheda di linea WS-X6348 (nello slot 3). Inoltre, è necessario considerare attendibile tutto il traffico in arrivo poiché è stato contrassegnato in precedenza a livello di switch di accesso. Poiché non è possibile impostare trust-dscp sulla scheda di linea 6348, il metodo più semplice in questo caso consiste nel lasciare tutte le porte come non attendibili e nel modificare l'ACL predefinito in trust-dscp, come nell'esempio seguente:

```
set qos enable
set port qos 2/1-16 trust untrusted
set port qos 3/1-48 trust untrusted
set qos acl default-action ip trust-dscp
```

Informazioni correlate

- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN
- Supporto tecnico – Cisco Systems