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

Sommario

Introduzione

In questo documento viene esaminato cosa succede con il contrassegno e la classificazione di un pacchetto nelle varie fasi dello chassis Cisco Catalyst 6500/6000 con software Cisco IOS®. Questo documento descrive casi speciali e restrizioni e fornisce brevi casi di studio.

In questo documento non viene fornito un elenco esaustivo di tutti i comandi del software Cisco IOS relativi a QoS o al contrassegno. Per ulteriori informazioni sull'interfaccia della riga di

comando (CLI) del software Cisco IOS, consultare il documento sulla configurazione di QoS PFC.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware:

- Switch Catalyst serie 6500/6000 con software Cisco IOS e che usano uno dei seguenti Supervisor Engine:Un Supervisor Engine 1A con una Policy Feature Card (PFC) e un Multilayer Switch Feature Card (MSFC)Supervisor Engine 1A con PFC e MSFC2Un Supervisor Engine 2 con PFC2 e MSFC2

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.

Convenzioni

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

Terminologia

L'elenco fornisce la terminologia utilizzata nel presente documento:

- DSCP (Differentiated Services Code Point) - I primi sei bit del byte del tipo di servizio (ToS) nell'intestazione IP. DSCP è presente solo nel pacchetto IP.**Nota:** lo switch assegna anche un DSCP interno a ciascun pacchetto, IP o non IP. Nella sezione Quattro possibili origini per il DSCP interno di questo documento viene descritta in dettaglio l'assegnazione del DSCP interno.
- Precedenza IP: i primi tre bit del byte ToS nell'intestazione IP.
- CoS (Class of Service) - L'unico campo che può essere utilizzato per contrassegnare un pacchetto sul layer 2 (L2). Il CoS è costituito da uno dei tre bit seguenti:I tre bit IEEE 802.1p (dot1p) nel tag IEEE 802.1Q (dot1q) per il pacchetto dot1q.**Nota:** per impostazione predefinita, gli switch Cisco non etichettano i pacchetti VLAN nativi.I tre bit chiamati "User Field" nell'intestazione ISL (Inter-Switch Link) di un pacchetto incapsulato da ISL.**Nota:** CoS non è presente in un pacchetto non dot1q o ISL.
- Classificazione: il processo utilizzato per selezionare il traffico da contrassegnare.
- Contrassegno - Processo che imposta un valore DSCP di livello 3 (L3) in un pacchetto. Questo documento estende la definizione di marcatura per includere l'impostazione dei valori di CoS L2.

Gli switch Catalyst serie 6500/6000 possono effettuare le classificazioni sulla base di questi tre parametri:

- DSCP
- Precedenza IP
- CoS

Gli switch Catalyst serie 6500/6000 eseguono la classificazione e il contrassegno in diverse fasi. Questo è ciò che accade in luoghi diversi:

- Porta di ingresso (circuito integrato specifico per l'applicazione in entrata [ASIC])
- Motore di commutazione (PFC)
- Porta di uscita (ASIC in uscita)

Gestione porta di input

Il parametro di configurazione principale per la porta in entrata, in relazione 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`

Per impostare o modificare lo stato di `attendibilità` della porta, usare questo comando del software Cisco IOS in modalità `interfaccia`:

```
6k(config-if)#mls qos trust ?
  cos            cos keyword
  dscp          dscp keyword
  ip-precedence  ip-precedence keyword
  <cr>
```

Nota: per impostazione predefinita, tutte le porte sono in stato `non attendibile` quando QoS è abilitato. Per abilitare la funzionalità QoS sugli switch Catalyst 6500 con software Cisco IOS, usare il comando **mls qos** nella modalità di configurazione principale.

A livello di porta di input, è possibile applicare anche un CoS predefinito per porta. Di seguito è riportato un esempio:

```
6k(config-if)#mls qos cos cos-value
```

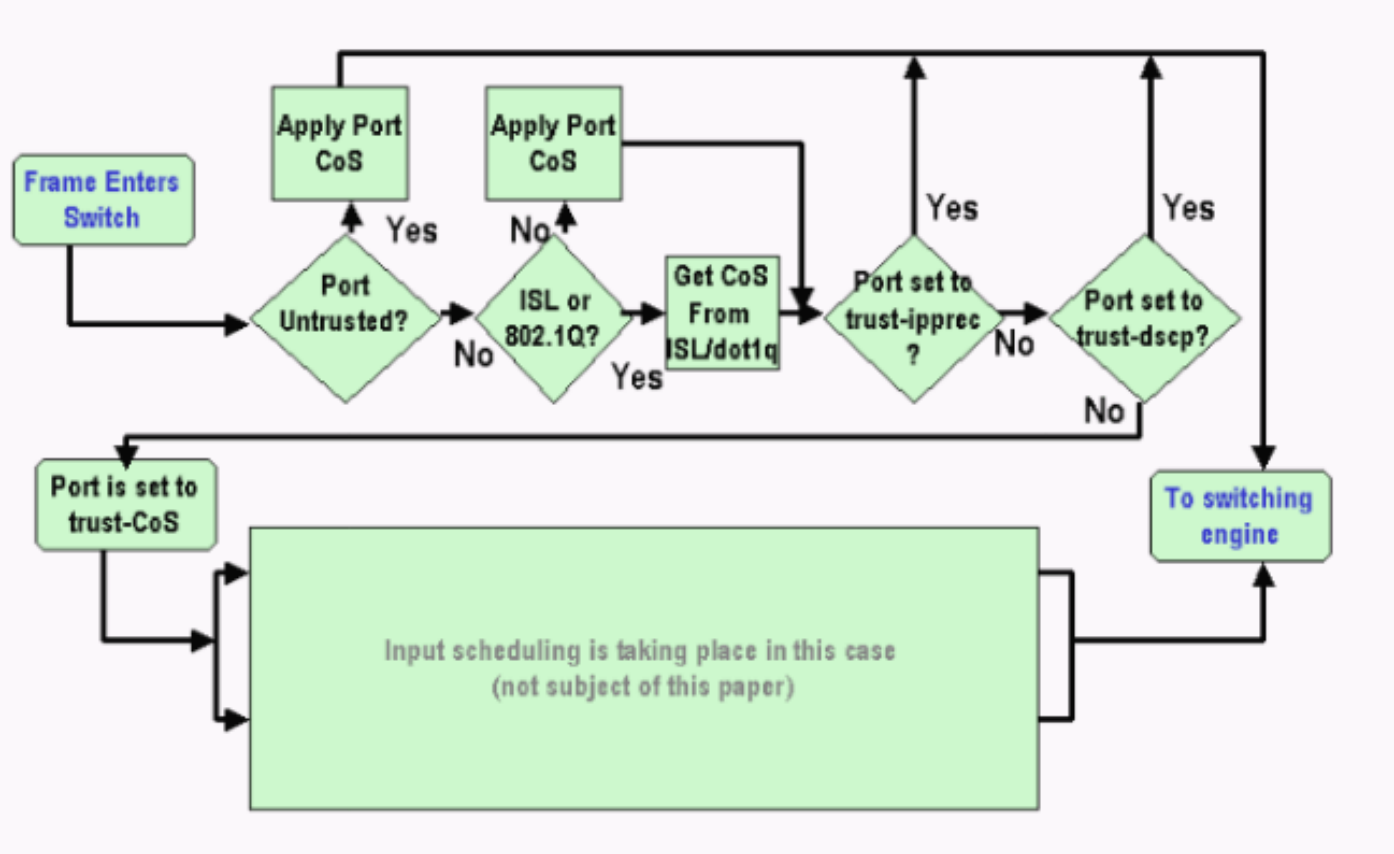
Il servizio CoS predefinito viene applicato a tutti i pacchetti, ad esempio IP e IPX (Internetwork Packet Exchange). Il servizio CoS predefinito può essere applicato a qualsiasi porta fisica.

Se la porta è in 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`, eseguire una delle due opzioni seguenti:

- Se il frame non ha un CoS ricevuto (dot1q o ISL), applicare il CoS della porta predefinita.
- Per i frame dot1q e ISL, lasciare il CoS inalterato.

Passare quindi il frame al motore di commutazione.

In questo esempio vengono illustrati la classificazione e il contrassegno di input. Nell'esempio viene mostrato come assegnare un CoS interno a ciascun frame:



Nota: come mostrato nell'esempio, a ciascun frame viene assegnato un CoS interno. L'assegnazione si basa sul CoS ricevuto o sulla porta predefinita. Il CoS interno include frame senza tag che non trasportano alcun CoS reale. Il CoS interno è scritto in una speciale intestazione di pacchetto, chiamata intestazione del bus di dati, e inviato tramite il bus di dati al motore di commutazione.

Switching Engine (PFC)

Quando l'intestazione raggiunge il motore di commutazione, la logica di riconoscimento degli indirizzi avanzata (EARL, Enhanced Address Recognition Logic) assegna a ciascun frame un DSCP interno. Questo DSCP interno è una priorità interna assegnata al frame dal PFC mentre il frame passa attraverso lo switch. Questo non è il DSCP nell'intestazione IP versione 4 (IPv4). Il DSCP interno deriva da un'impostazione CoS o ToS esistente e viene utilizzato 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.

In questa sezione viene descritto come assegnare un criterio servizio all'interfaccia per creare un contrassegno. Nella sezione viene inoltre illustrata l'impostazione finale del DSCP interno, che dipende dallo stato di `attendibilità` della porta e dai criteri del servizio applicati.

Configurare la policy sui servizi per classificare o contrassegnare un pacchetto nel software Cisco IOS versione 12.1(12c)E e successive

Completare questa procedura per configurare i criteri del servizio:

1. Configurare un elenco di controllo di accesso (ACL) per definire il traffico da prendere in considerazione.È possibile assegnare un numero o un nome all'ACL e Catalyst 6500/6000 supporta un ACL esteso. Utilizzare il comando **access-list *xxx*** Software Cisco IOS, come

mostrato nell'esempio:

```
(config)#access-list 101 permit ip any host 10.1.1.1
```

2. Configurare una classe di traffico (mappa di classe) in modo che corrisponda al traffico sulla base dell'ACL definito o del DSCP ricevuto.Eseguire il comando **class-map** Cisco IOS Software. QoS PFC non supporta più di un'istruzione match per mappa di classe. Inoltre, QoS PFC supporta solo queste istruzioni di corrispondenza:**match ip access-groupcorrispondenza ip dscpcorrispondenza ip precedenceprotocollo di corrispondenzaNota:** il comando **match protocol** consente di utilizzare Network Based Application Recognition (NBAR) per associare il traffico.**Nota:** di queste opzioni, sono supportate solo le istruzioni **match ip dscp** e **match ip precedence**. Tali indicazioni non sono tuttavia utili per contrassegnare o classificare i pacchetti. È possibile utilizzare queste istruzioni, ad esempio, per eseguire il policy su tutti i pacchetti che corrispondono a un determinato DSCP. Tuttavia, questa azione esula dall'ambito del presente documento.

```
(config)#class-map class-name
(config-cmap)#match {access-group | input-interface | ip dscp}
```

Nota: in questo esempio vengono visualizzate solo tre opzioni per il comando **match**. Al prompt dei comandi è tuttavia possibile configurare molte altre opzioni.**Nota:** una delle opzioni in questo comando **match** viene accettata come criterio di corrispondenza e le altre opzioni vengono tralasciate, a seconda dei pacchetti in arrivo.Di seguito è riportato un esempio:

```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```

3. Configurare una mappa dei criteri per applicare un criterio a una classe definita in precedenza.La mappa dei criteri contiene:Un nomeSet di istruzioni classPer ogni istruzione di classe, l'azione da eseguire per la classeLe azioni supportate in PFC1 e PFC2 QoS sono:**trust dscptrust ip precedencecc trustset ip dscp** nel software Cisco IOS versione 12.1(12c)E1 e successive**impostare la precedenza ip** nel software Cisco IOS versione 12.1(12c)E1 e successive**poliziaNota:** questa azione esula dall'ambito del presente documento.

```
(config)#policy-map policy-name
(config-pmap)#class class-name
(config-pmap-c)#{police | set ip dscp}
```

Nota: in questo esempio vengono mostrate solo due opzioni, ma è possibile configurare molte altre opzioni al prompt dei comandi `(config-map-c)#`.Di seguito è riportato un esempio:

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   set ip dscp 16
```

4. Configurare un input dei criteri del servizio per applicare una mappa dei criteri definita in precedenza per una o più interfacce.**Nota:** è possibile associare una policy sul servizio all'interfaccia fisica o all'interfaccia SVI (Virtual Interface) o VLAN commutata. Se si collega un criterio dei servizi a un'interfaccia VLAN, le uniche porte che utilizzano questo criterio dei

servizi sono le porte che appartengono alla VLAN e sono configurate per la funzionalità QoS basata su VLAN. Se la porta non è impostata per la funzionalità QoS basata su VLAN, utilizzerà comunque la funzionalità QoS basata sulla porta predefinita e verificherà solo i criteri del servizio collegati all'interfaccia fisica.Nell'esempio seguente viene applicato il criterio `test_policy` del servizio alla porta Gigabit Ethernet 1/1:

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

Nell'esempio, il criterio `test_policy` del servizio viene applicato a tutte le porte della VLAN 10 che hanno una configurazione basata su VLAN dal punto di vista QoS:

```
(config) interface gigabitethernet 1/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Nota: è possibile combinare i passi 2 e 3 di questa procedura se si ignora la definizione specifica della classe e si collega l'ACL direttamente nella definizione della mappa dei criteri. In questo esempio, se la classe `TEST Police` non è stata definita prima della configurazione della mappa dei criteri, la classe viene definita all'interno della mappa dei criteri:

```
(config)#policy-map policy-name
(config-pmap)#class class_name {access-group acl_index_or_name | dscp dscp_1 [dscp_2
[dscp_N]] | precedence ipp_1 [ipp_2 [ipp_N]]}
!--- Note: This command should be on one line.

policy-map TEST
class TEST police access-group 101
```

Configurare la policy sui servizi per classificare o contrassegnare un pacchetto nel software Cisco IOS con versioni precedenti al software Cisco IOS versione 12.1(12c)E

Nel software Cisco IOS con versioni precedenti al software Cisco IOS versione 12.1(12c)E1, non è possibile usare l'azione **set ip dscp** o **set ip precedence** in una mappa dei criteri. Pertanto, l'unico modo per contrassegnare il traffico specifico definito da una classe è configurare un policer con una frequenza molto alta. Questa velocità dovrebbe essere, per esempio, almeno la velocità della linea della porta o qualcosa di abbastanza alto da consentire a tutto il traffico di raggiungere il policer. Quindi, utilizzare **set-dscp-transmission *xx*** come azione di conformità. Per impostare questa configurazione, attenersi alla procedura seguente:

1. Configurare un ACL per definire il traffico da prendere in considerazione.È possibile assegnare un numero o un nome all'ACL e Catalyst 6500/6000 supporta un ACL esteso. Utilizzare il comando **access-list *xxx*** Software Cisco IOS, come mostrato nell'esempio:
   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Configurare una classe di traffico (mappa di classe) in modo che corrisponda al traffico sulla base dell'ACL definito o del DSCP ricevuto.Eseguire il comando **class-map** Cisco IOS Software. QoS PFC non supporta più di un'istruzione match per mappa di classe. Inoltre, QoS PFC supporta solo queste istruzioni di corrispondenza:**match ip access-**

groupcorrispondenza ip dscpcorrispondenza ip precedenceprotocollo di corrispondenzaNota: il comando **match protocol** consente di utilizzare NBAR per associare il traffico.**Nota:** di queste istruzioni, solo le istruzioni **match ip dscp** e **match ip precedence** sono supportate e funzionano. Queste indicazioni, tuttavia, non sono utili per marcare o classificare i pacchetti. È possibile utilizzare queste istruzioni, ad esempio, per eseguire il policy su tutti i pacchetti che corrispondono a un determinato DSCP. Tuttavia, questa azione esula dall'ambito del presente documento.

```
(config)#class-map  class-name
(config-cmap)#match {access-group | input-interface | ip dscp}
```

Nota: in questo esempio vengono visualizzate solo tre opzioni per il comando **match**. Al prompt dei comandi è tuttavia possibile configurare molte altre opzioni.Di seguito è riportato un esempio:

```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```

3. Configurare una mappa dei criteri per applicare un criterio a una classe definita in precedenza.La mappa dei criteri contiene:Un nomeSet di istruzioni classPer ogni istruzione di classe, l'azione da eseguire per la classeLe azioni supportate in QoS PFC1 o PFC2 sono:**trust dscptrust ip precedencecc trustpoliziaÈ**necessario utilizzare l'istruzione **Police** perché le azioni **set ip dscp** e **set ip precedence** non sono supportate. Poiché non si vuole controllare il traffico, ma solo contrassegnarlo, utilizzare un policer definito per consentire tutto il traffico. Pertanto, configurare il policer con una velocità elevata e una frammentazione. Ad esempio, è possibile configurare il policer con la velocità e la frammentazione massime consentite. Di seguito è riportato un esempio:

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   police  4000000000 31250000 conform-action
   set-dscp-transmit 16 exceed-action policed-dscp-transmit
```

4. Configurare un input dei criteri del servizio per applicare una mappa dei criteri definita in precedenza a una o più interfacce.**Nota:** la policy del servizio può essere collegata a un'interfaccia fisica o all'interfaccia SVI o VLAN. Se a un'interfaccia VLAN è collegato un criterio del servizio, solo le porte che appartengono alla VLAN e sono configurate per le funzionalità QoS basate su VLAN utilizzano questo criterio del servizio. Se la porta non è impostata per la funzionalità QoS basata su VLAN, utilizzerà comunque la funzionalità QoS basata sulla porta predefinita e verificherà solo i criteri dei servizi collegati all'interfaccia fisica.Nell'esempio seguente viene applicato il criterio `test_policy` del servizio alla porta Gigabit Ethernet 1/1:

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

Nell'esempio, il criterio `test_policy` del servizio viene applicato a tutte le porte della VLAN 10 che hanno una configurazione basata su VLAN dal punto di vista QoS:

```
(config) interface gigabitethernet 1/2
```

```
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Quattro possibili origini per DSCP interno

Il DSCP interno deriva da uno dei seguenti elementi:

1. Valore DSCP ricevuto esistente, impostato prima che il frame entri nello switchUn esempio è il **trust dscp**.
2. Bit di precedenza IP ricevuti già impostati nell'intestazione IPv4Poiché sono presenti 64 valori DSCP e solo otto valori di precedenza IP, l'amministratore configura un mapping utilizzato dallo switch per derivare il DSCP. Sono presenti mapping predefiniti, nel caso in cui l'amministratore non configuri i mapping. Un esempio è **trust ip precedence**.
3. I bit CoS ricevuti che sono già impostati prima che il frame entri nello switch e che sono archiviati nell'intestazione del bus dati, o se il frame in arrivo non contiene CoS, dal CoS predefinito della porta in arrivoCome per la precedenza IP, esistono al massimo otto valori CoS, ognuno dei quali deve essere mappato a uno dei 64 valori DSCP. L'amministratore può configurare questa mappa oppure lo switch può utilizzare la mappa predefinita già presente.
4. I criteri del servizio possono impostare il DSCP interno su un valore specifico.

Per i numeri 2 e 3 di questo elenco, il mapping statico è per impostazione predefinita, nel modo seguente:

- Per il mapping da CoS a DSCP, il DSCP derivato è otto volte superiore al CoS.
- Per il mapping IP precedence-to-DSCP, il DSCP derivato è otto volte superiore alla precedenza IP.

Èpossibile utilizzare questi comandi per ignorare e verificare questa mappatura statica:

- **mls qos map ip-prec-dscp** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*
- **mappa mls qos cos-dscp** *dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*

Il primo valore del DSCP che corrisponde al mapping per il CoS (o IP precedence) è 0. Il secondo valore per il CoS (o IP precedence) è 1 e il modello continua in questo modo. Ad esempio, questo comando modifica il mapping in modo che CoS 0 sia mappato al DSCP 0 e CoS 1 al DSCP 8 e così via:

```
Cat65(config)#mls qos map cos-dscp 0 8 16 26 32 46 48 54
Cat65#show mls qos maps
CoS-dscp map:
 cos:     0 1  2   3   4   5   6   7
  ---------------------------------
 dscp:    0 8 16  26  32  46  48  54
```

Come viene scelto il DSCP interno?

Il DSCP interno è scelto sulla base dei seguenti parametri:

- Mappa dei criteri QoS applicata al pacchettoLa mappa dei criteri QoS è determinata dalle

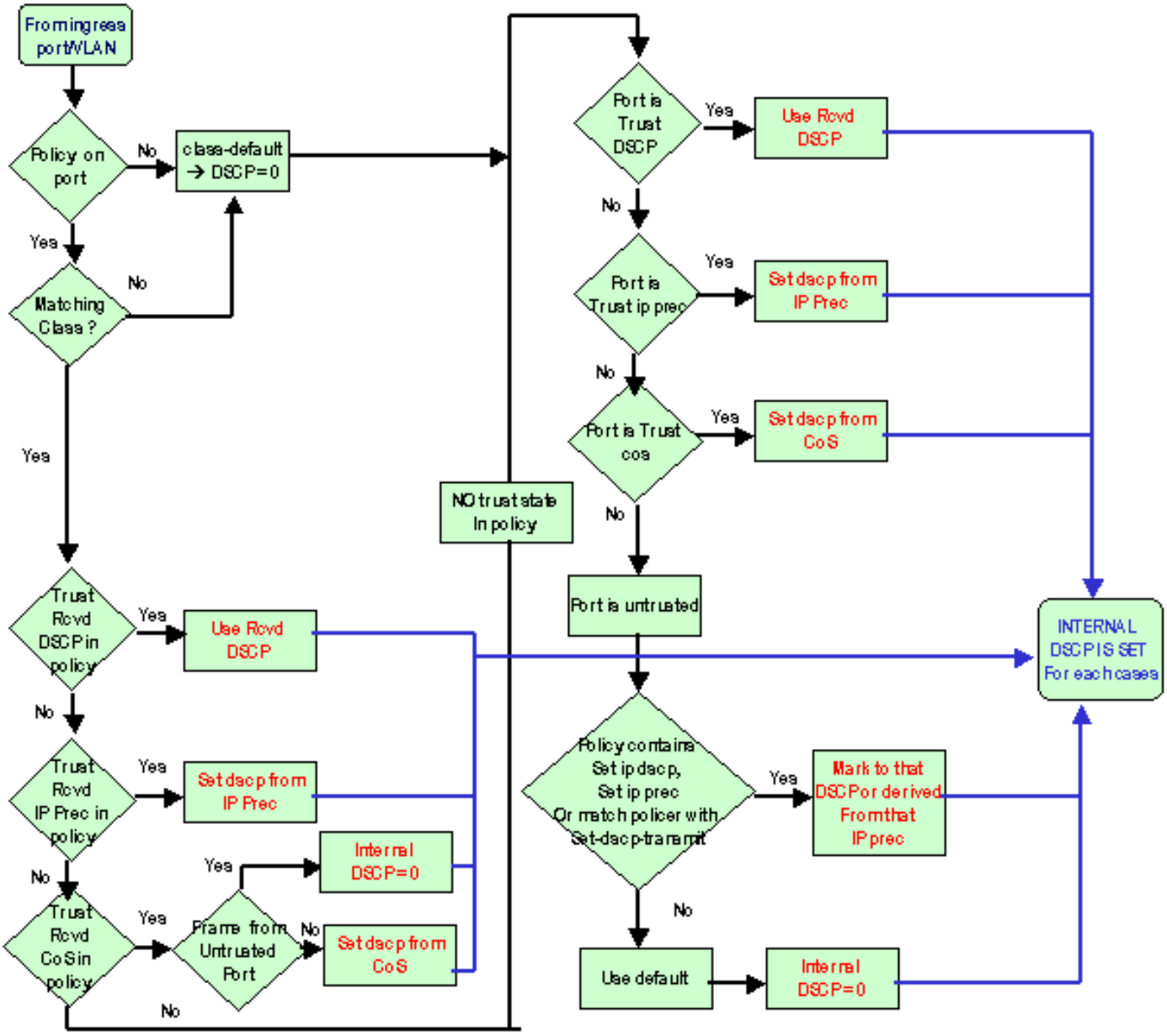
seguenti regole:Se alla porta o alla VLAN in ingresso non è collegato alcun criterio del servizio, utilizzare il criterio predefinito.**Nota:** per impostazione predefinita, il DSCP interno viene impostato su 0.Utilizzare questa voce se alla porta o alla VLAN in ingresso è associato un criterio del servizio e se il traffico corrisponde a una delle classi definite dal criterio.Se alla porta o alla VLAN in ingresso è associato un criterio del servizio e il traffico non corrisponde a una delle classi definite dal criterio, utilizzare il valore predefinito.

- Stato di `attendibilità` della porta e azione della mappa dei criteriQuando la porta ha uno specifico stato di `attendibilità` e un criterio con un determinato contrassegno (azione di attendibilità simultanea), si applicano le seguenti regole:Il comando **set ip dscp** o il DSCP definito per policer in una mappa dei criteri viene applicato solo se la porta viene lasciata in stato `non attendibile`.Se la porta ha uno stato di `attendibilità`, questo stato di `attendibilità` viene utilizzato per derivare il DSCP interno. Lo stato di `attendibilità` della porta ha sempre la precedenza sul comando **set ip dscp**.Il comando **trust *xx*** in una mappa dei criteri ha la precedenza sullo stato di `attendibilità` della porta.Se la porta e il criterio contengono uno stato di `attendibilità` diverso, viene preso in considerazione lo stato di `attendibilità` che deriva dal mapping dei criteri.

Pertanto, il DSCP interno dipende da questi fattori:

- Stato di `attendibilità` della porta
- I criteri del servizio (con l'uso di ACL) collegati alla porta
- Mappa criteri predefinita**Nota:** il valore predefinito reimposta il DSCP su 0.
- Basato su VLAN o su porta per quanto riguarda l'ACL

Il diagramma riepiloga come viene scelto il DSCP interno in base alla configurazione:



Il PFC è anche in grado di eseguire il policing. Ciò può eventualmente determinare un markdown del DSCP interno. Per ulteriori informazioni sul monitoraggio, consultare il documento sul monitoraggio QoS sugli switch Catalyst serie 6500/6000.

Gestione porta di output

Non è possibile eseguire alcuna operazione a livello di porta di uscita per modificare la classificazione. Tuttavia, contrassegnare il pacchetto in base a queste 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. Copiare il CoS nel frame ISL o dot1q.

Nota: il CoS è derivato dal DSCP interno in base a un valore statico. Utilizzare questo comando per configurare l'interfaccia statica:

```
Router(config)#mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7
```

```
[dscp8]]]]]]] to cos_value
!--- Note: This command should be on one line.
```

In questa sezione vengono visualizzate le configurazioni predefinite. Per impostazione predefinita, CoS è la parte intera del DSCP divisa per otto. Utilizzare questo comando per visualizzare e verificare il mapping:

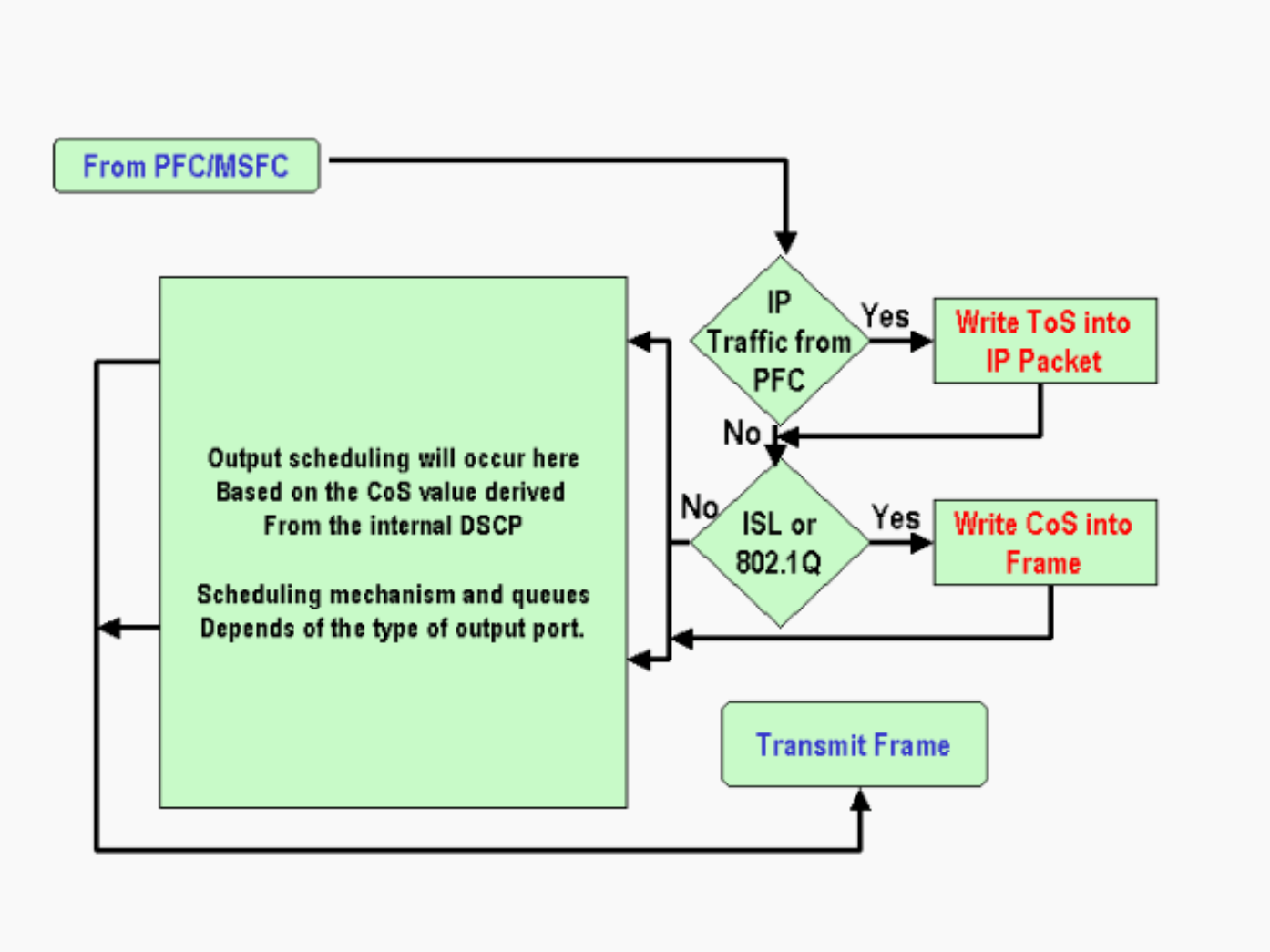
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

Per modificare questa mappatura, usare questo comando di configurazione nella modalità di configurazione normale:

```
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 8 9 10 11 12 13 14 15 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
...
```

Dopo aver scritto il DSCP nell'intestazione IP e aver derivato il CoS dal DSCP, il pacchetto viene inviato a una delle code di output per la pianificazione dell'output sulla base del CoS. Questo si verifica anche se il pacchetto non è un dot1q o un ISL. Per ulteriori informazioni sulla pianificazione delle code di output, consultare il documento sulla pianificazione dell'output QoS sugli switch Catalyst serie 6500/6000 con software di sistema Cisco IOS.

Il diagramma mostra l'elaborazione del pacchetto in relazione al contrassegno nella porta di uscita:



Note e limitazioni

ACL predefinito

L'ACL predefinito usa "dscp 0" come parola chiave di classificazione. Tutto il traffico che entra nello switch tramite una porta non attendibile e non raggiunge una voce dei criteri del servizio è contrassegnato con un DSCP pari a 0 se QoS è abilitato. Al momento, non è possibile modificare l'ACL predefinito nel software Cisco IOS.

Nota: nel software Catalyst OS (CatOS), è possibile configurare e modificare questo comportamento predefinito. Per ulteriori informazioni, fare riferimento alla sezione *ACL predefinito* di classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS.

Limitazioni delle schede di linea WS-X61xx, 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 Multimode 100 FX 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 100 FX a 24 porte, QoS migliorato, MT
- WS-X6324-100FX-SM: Catalyst 6000 100 FX a 24 porte, QoS migliorato, MT
- WS-X6348-RJ-45: Catalyst 6000 10/100 a 48 porte, QoS migliorato
- WS-X6348-RJ21V: Catalyst 6000 10/100, alimentazione in linea a 48 porte
- WS-X6348-RJ45V: Catalyst 6000 10/100 a 48 porte, QoS migliorato, alimentazione in linea
- WS-X6148-RJ21V: Catalyst 6500 10/100 Inline Power a 48 porte
- WS-X6148-RJ45V: Catalyst 6500 10/100 Inline Power a 48 porte

Queste schede di linea hanno un limite. A livello di porta, non è possibile configurare lo stato di `attendibilità` con l'uso di una delle seguenti parole chiave:

- `trust-dscp`
- `trust-ipprec`
- `trust-cos`

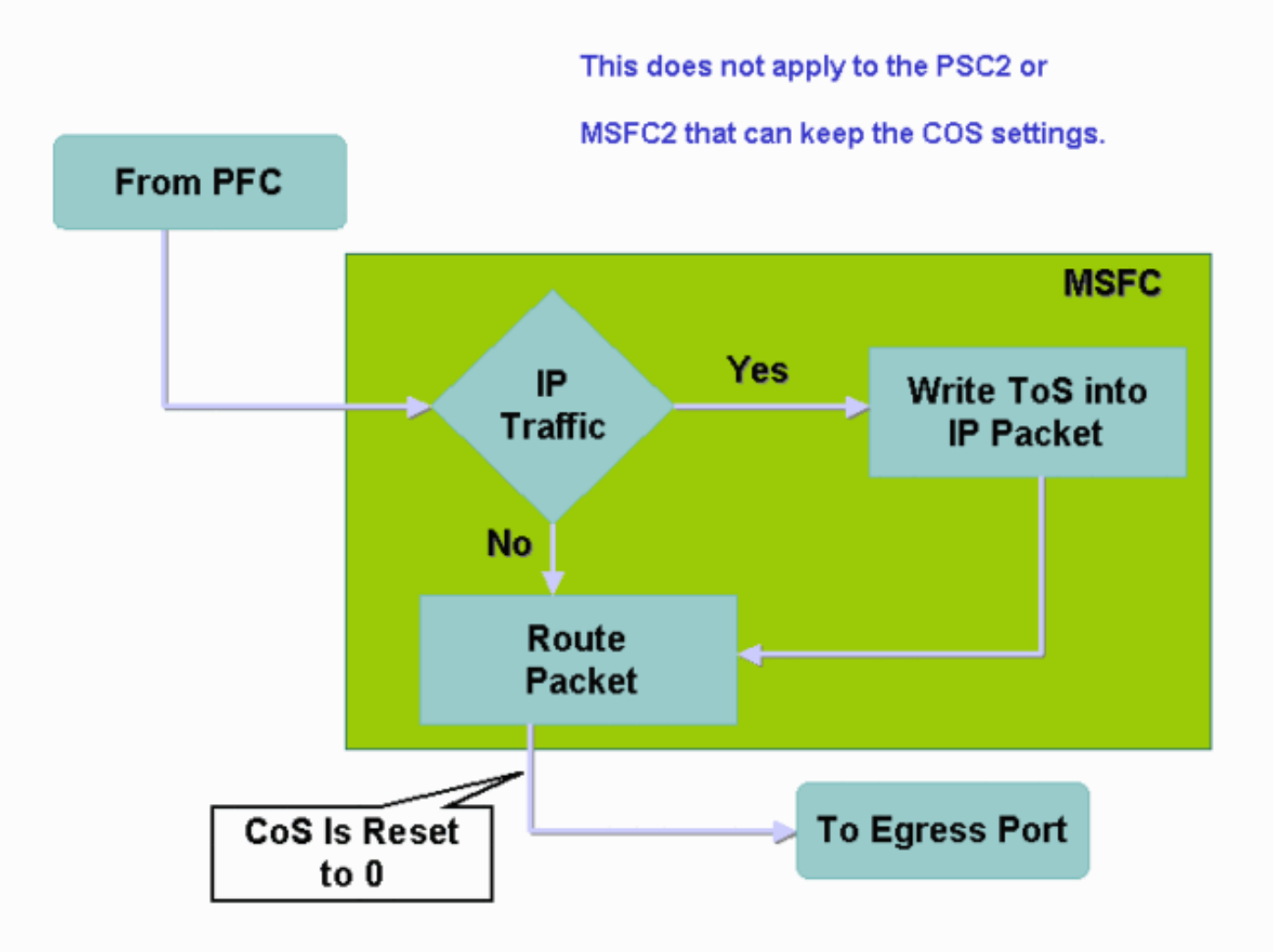
Èpossibile utilizzare solo lo stato `non attendibile`. Qualsiasi tentativo di configurare uno stato di `attendibilità` su una di queste porte visualizza uno dei seguenti messaggi di avviso:

```
Tank(config-if)#mls qos trust ?
  extend  extend keyword
Tank(config-if)#mls qos trust
% Incomplete command.
Tank(config-if)#mls qos trust cos
                              ^
% Invalid input detected at '^' marker.
Tank(config-if)#mls qos trust ip-pre
                              ^
% Invalid input detected at '^' marker.
```

Ènecessario collegare una policy sui servizi alla porta o alla VLAN se si desidera che un frame affidabile si trovi su una scheda di linea di questo tipo. Utilizzare il metodo nel caso 1: Contrassegno nella sezione Edge di questo documento.

Pacchetti provenienti da MSFC1 o MSFC2 su Supervisor Engine 1A/PFC

Il valore CoS di tutti i pacchetti provenienti dall'MSFC1 o dall'MSFC2 è 0. Il pacchetto può essere un pacchetto con routing software o un pacchetto emesso dall'MSFC. Si tratta di una limitazione del PFC in quanto reimposta il CoS di tutti i pacchetti provenienti dall'MSFC. La precedenza DSCP e IP viene mantenuta. Il PFC2 non presenta questa limitazione. Il CoS esistente del PFC2 equivale alla precedenza IP del pacchetto.



Riepilogo classificazione

Le tabelle di questa sezione mostrano il DSCP risultante in base a queste classificazioni:

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

Questa tabella fornisce un riepilogo generico per tutte le porte ad eccezione di WS-X62xx e WS-X63xx:

Parola chiave mappa criteri Stato trust porta	set-ip-dscp xx o set-dscp-broadcast xx	trust-dscp	trust-ipprec	trust-cos
non attendibile	xx[1]	Rx[2] DSCP	Derivato da Rx ipprec	0
trust-dscp	DSCP Rx	DSCP Rx	Derivato da Rx ipprec	Derivato da Rx CoS o port CoS
trust-	Derivato da Rx	DSCP	Derivato	Derivato da

ipprec	ipprec	Rx	da Rx ipprec	Rx CoS o port CoS
trust-cos	Derivato da Rx CoS o port CoS	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 frame.

[2] Rx = ricezione

Nella tabella seguente viene fornito un riepilogo delle porte WS-X61xx, WS-X62xx e WS-X63xx:

Parola chiave mappa criteri **Stato trust porta**	**set-ip-dscp xx o set-dscp-broadcast 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	Non supportato	Non supportato	Non supportato	Non supportato

Monitoraggio e verifica di una configurazione

Controllo della configurazione della porta

Per verificare le impostazioni e le configurazioni della porta, usare il comando **show queuing interface** *id-interfaccia*.

Quando si esegue questo comando, è possibile verificare i seguenti parametri di classificazione, tra cui:

- Basato su porta o su VLAN
- Tipo di porta `trust`
- L'ACL collegato alla porta

Di seguito è riportato un esempio di questo output del comando. I campi importanti relativi alla classificazione vengono visualizzati in grassetto:

```
6500#show queuing interface gigabitethernet 3/2
Interface GigabitEthernet3/2 queuing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust COS
  Default COS is 0
  Transmit queues [type = 1p2q2t]:
```

L'output mostra che la configurazione della porta specifica è con `trust cos` a livello di porta. Inoltre, il valore predefinito del parametro Port CoS è 0.

Controlla classi definite

Usare il comando **show class-map** per controllare le classi definite. Di seguito è riportato un esempio:

```
Boris#show class-map
 Class Map match-all test (id 3)
   Match access-group  112

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all voice (id 4)
```

Controllare la mappa dei criteri applicata a un'interfaccia

Utilizzare questi comandi per controllare la mappa dei criteri applicata e rilevata nei comandi precedenti:

- **show mls qos ip interface** *id*
- **show policy-map interface** *id-interfaccia*

Di seguito sono riportati alcuni esempi dell'output del comando:

```
Boris#show mls qos ip gigabitethernet 1/1
   [In] Default.   [Out] Default.
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

 Int  Mod Dir  Class-map  DSCP AgId Trust FlId AgForward-Pk AgPoliced-k
 -----------------------------------------------------------------------
 Gi1/1 1  In   TEST       0    0*   No    0    1242120099             0
```

Nota: è possibile esaminare i seguenti campi relativi alla classificazione:

- `Class-map`: indica la classe collegata al criterio del servizio associato all'interfaccia.
- `Trust` - Indica se l'azione di polizia in quella classe contiene un comando **trust** e gli elementi attendibili nella classe.
- `DSCP` - Indica il DSCP trasmesso per i pacchetti che hanno raggiunto quella classe.

```
Tank#show policy-map interface fastethernet 4/4

 FastEthernet4/4

  service-policy input: TEST_aggre2

    class-map: Test_marking (match-all)
      27315332 packets
      5 minute offered rate 25726 pps
```

```
match: access-group 101
police :
  10000000 bps 10000 limit 10000 extended limit
  aggregate-forwarded 20155529 packets action: transmit
  exceeded 7159803 packets action: drop
  aggregate-forward 19498 pps exceed 6926 pps
```

Esempi di case study

In questa sezione vengono fornite configurazioni di esempio di casi comuni che possono essere visualizzati in una rete.

Caso 1: Contrassegno sul bordo

Si supponga di configurare un Catalyst 6000 che viene utilizzato come switch di accesso. Molti utenti si connettono allo slot 2 dello switch, una scheda di linea WS-X6348 (10/100 Mbps). Gli utenti possono inviare:

- Traffico dati normale: questo traffico si trova sempre nella VLAN 100 e deve avere un DSCP di 0.
- Traffico vocale da un telefono IP: questo traffico è sempre presente nella VLAN ausiliaria voce 101 e deve avere un DSCP di 46.
- Traffico applicazioni mission-critical: questo traffico viene inoltrato anche nella VLAN 100 e viene indirizzato al server 10.10.10.20. Questo traffico deve avere un DSCP di 32.

L'applicazione non contrassegna nessuno di questo traffico. Pertanto, lasciare la porta `non attendibile` e configurare un ACL specifico per classificare il traffico. Alla VLAN 100 viene applicato un ACL e alla VLAN 101 un ACL. È necessario configurare tutte le porte come basate sulla VLAN. Di seguito è riportato un esempio della configurazione risultante:

```
Boris(config)#mls qos
Boris(config)#interface range fastethernet 2/1-48
Boris(config-if)#mls qos vlan-based
Boris(config-if)#exit
Boris(config)#ip access-list extended Mission_critical
Boris(config-ext-nacl)#permit ip any host 10.10.10.20
Boris(config)#ip access-list extended Voice_traffic
Boris(config-ext-nacl)#permit ip any any
Boris(config)#class-map voice

Boris(config-cmap)#match access-group Voice_traffic
Boris(config)#class-map Critical

Boris(config-cmap)#match access-group Mission_critical
Boris(config)#policy-map Voice_vlan
Boris(config-pmap)#class voice
Boris(config-pmap-c)#set ip dscp 46
Boris(config)#policy-map Data_vlan
Boris(config-pmap)#class Critical
Boris(config-pmap-c)#set ip dscp 32
Boris(config)#interface vlan 100
Boris(config-if)#service-policy input Data_vlan
Boris(config)#interface vlan 101
Boris(config-if)#service-policy input Voice_vlan
```

Caso 2: Fiducia nel core solo con interfacce Gigabit Ethernet

Si supponga di configurare un core Catalyst 6000 con solo un'interfaccia Gigabit Ethernet nello slot 1 e nello slot 2. Gli switch di accesso hanno precedentemente contrassegnato il traffico correttamente. Pertanto, non è necessario effettuare alcuna osservazione. Tuttavia, è necessario verificare che lo switch di base consideri attendibile il DSCP in ingresso. Questo caso è il più semplice perché tutte le porte sono contrassegnate come `trust-dscp`, che dovrebbe essere sufficiente:

```
6k(config)#mls qos
6k(config)#interface range gigabitethernet 1/1-2 , gigabitethernet 2/1-2
6k(config-if)#mls qos trust dscp
```

Informazioni correlate

- Qualità del servizio sugli switch Catalyst serie 6000
- Classificazione e contrassegno QoS sugli switch Catalyst serie 6500/6000 con software CatOS
- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems