

300系列託管交換機上的QoS高級模式配置

目標

在QoS高級模式下，交換機使用策略來支援每流QoS。策略及其元件具有以下特性：

- 策略可能包含一個或多個類對映。
- 策略包含一個或多個流，每個流都有一個使用者定義的QoS。
- 基於策略器QoS規範，單個策略器將QoS應用於單個類對映，從而應用於單個流。
- 聚合策略器將QoS應用於一個或多個類對映，從而應用於一個或多個流。
- 通過將策略繫結到所需埠，將每個流的QoS應用到流。

適用裝置

- SF/SG 300系列託管交換器

軟體版本

- v1.2.7.76

配置QoS高級模式的工作流程

- 1.選擇系統的高級模式。
- 2.要將外部值對映到內部值，如果內部DSCP值與傳入資料包上使用的值不同，請在「[超出配置檔案DSCP對映](#)」頁上配置超出配置檔案DSCP對映。
- 3.建立ACL。有關建立ACL的工作流程，請參閱相關文檔。
- 4.使用「類對映」頁建立類對映並將ACL與其相關聯。
- 5.使用*Policy Table*頁建立策略，並使用*Policy Class Map*頁將該策略與一個或多個類對映相關聯。下面使用的策略器型別。

- 單個管制器
- 可以建立策略以將類對映關聯到單個監察器。
- 聚合監察器：

使用 *Aggregate Policer* 頁，為將所有匹配幀傳送到聚合管制器的每個流建立QoS操作

- 6.最後，使用*Policy Binding*頁將策略繫結到介面。

本檔案將說明設定上述指標的程式。

QoS進階模式

啟用QoS高級模式

步驟1.登入到Web配置實用程式，然後選擇Quality of Service > General > QoS Properties。
將開啟QoS屬性頁：



QoS Properties

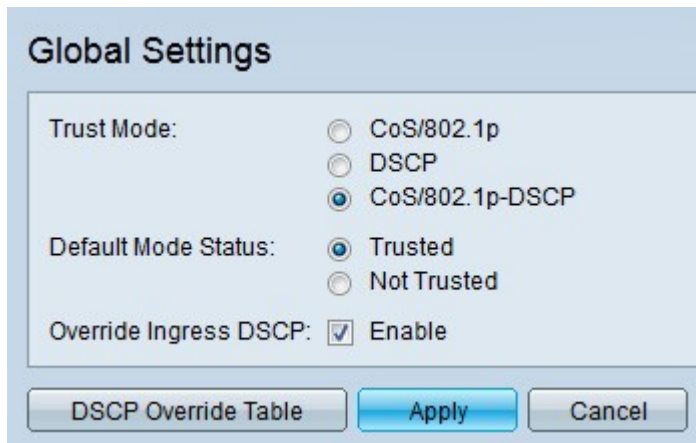
QoS Mode: Disable
 Basic
 Advanced

步驟2.按一下QoS模式欄位中的**Advanced**單選按鈕。

步驟3.按一下**Apply**。

全域性設定

步驟1.登入到Web配置實用程式並選擇**服務品質 > QoS高級模式 > 全域性設定**。將開啟「*超出配置檔案DSCP對映*」頁：



Global Settings

Trust Mode: CoS/802.1p
 DSCP
 CoS/802.1p-DSCP

Default Mode Status: Trusted
 Not Trusted

Override Ingress DSCP: Enable

DSCP Override Table							
DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out
0	0 ▼	16	16 ▼	32	32 ▼	48	48 ▼
1	1 ▼	17	17 ▼	33	33 ▼	49	49 ▼
2	2 ▼	18	18 ▼	34	34 ▼	50	50 ▼
3	3 ▼	19	19 ▼	35	35 ▼	51	51 ▼
4	4 ▼	20	20 ▼	36	36 ▼	52	52 ▼
5	5 ▼	21	21 ▼	37	37 ▼	53	53 ▼
6	6 ▼	22	22 ▼	38	38 ▼	54	54 ▼
7	7 ▼	23	23 ▼	39	39 ▼	55	55 ▼
8	8 ▼	24	24 ▼	40	40 ▼	56	56 ▼
9	9 ▼	25	25 ▼	41	41 ▼	57	57 ▼
10	10 ▼	26	26 ▼	42	42 ▼	58	58 ▼
11	11 ▼	27	27 ▼	43	43 ▼	59	59 ▼
12	12 ▼	28	28 ▼	44	44 ▼	60	60 ▼
13	13 ▼	29	29 ▼	45	45 ▼	61	61 ▼
14	14 ▼	30	30 ▼	46	46 ▼	62	62 ▼
15	15 ▼	31	31 ▼	47	47 ▼	63	63 ▼

超出配置檔案DSCP重新標籤

步驟1. 登入到Web配置實用程式並選擇服務品質> QoS高級模式>不在配置檔案DSCP對映。將開啟「超出配置檔案DSCP對映」頁：

Out of Profile DSCP Mapping

DSCP Remarking Table							
DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out
0	0 ▼	16	16 ▼	32	32 ▼	48	48 ▼
1	1 ▼	17	17 ▼	33	33 ▼	49	49 ▼
2	2 ▼	18	18 ▼	34	34 ▼	50	50 ▼
3	3 ▼	19	19 ▼	35	35 ▼	51	51 ▼
4	4 ▼	20	20 ▼	36	36 ▼	52	52 ▼
5	5 ▼	21	21 ▼	37	37 ▼	53	53 ▼
6	6 ▼	22	22 ▼	38	38 ▼	54	54 ▼
7	7 ▼	23	23 ▼	39	39 ▼	55	55 ▼
8	8 ▼	24	24 ▼	40	40 ▼	56	56 ▼
9	9 ▼	25	25 ▼	41	41 ▼	57	57 ▼
10	10 ▼	26	26 ▼	42	42 ▼	58	58 ▼
11	11 ▼	27	27 ▼	43	43 ▼	59	59 ▼
12	12 ▼	28	28 ▼	44	44 ▼	60	60 ▼
13	13 ▼	29	29 ▼	45	45 ▼	61	61 ▼
14	14 ▼	30	30 ▼	46	46 ▼	62	62 ▼
15	15 ▼	31	31 ▼	47	47 ▼	63	63 ▼

步驟2.配置DSCP重新標籤表。

- DSCP In — 顯示需要重新對映到替代值的傳入資料包的值。
- DSCP Out — 從DSCP Out下拉選單中選擇與DSCP In值對應的所需DSCP Out值。

附註：按一下「恢復預設值」將DSCP重新標籤表恢復為預設值。預設值是DSCP Out值與相應的DSCP In值的值匹配。

步驟3.按一下Apply。

類對映

步驟1.登入到Web配置實用程式並選擇**服務品質 > QoS高級模式 > 類對映**。此時將開啟「類對映」頁：

Class Mapping

Class Mapping Table						
<input type="checkbox"/>	Class Map Name	ACL 1	Match	ACL 2	Match	ACL 3
0 results found.						
<input type="button" value="Add..."/>		<input type="button" value="Delete"/>				

步驟2.按一下Add。系統將顯示Add Class Mapping視窗。

Class Map Name: (11/32 Characters Used)

Match ACL Type:
 IP
 MAC
 IP and MAC
 IP or MAC

IP:
 IPv4 or
 IPv6

MAC:

Preferred ACL:
 IP
 MAC

步驟3.在「類對映名稱」欄位中輸入類對映的名稱。

步驟4.點選與Match ACL Type欄位中所需的ACL對應的單選按鈕。

步驟5.如果定義的Match ACL欄位包含IP，請選中IP欄位中所需IP型別的覈取方塊。

- IPv4 — 從IPv4下拉選單中，選擇要應用於類對映的IPv4 ACL。
- IPv6 — 從IPv6下拉選單中選擇要應用於類對映的IPv6 ACL。

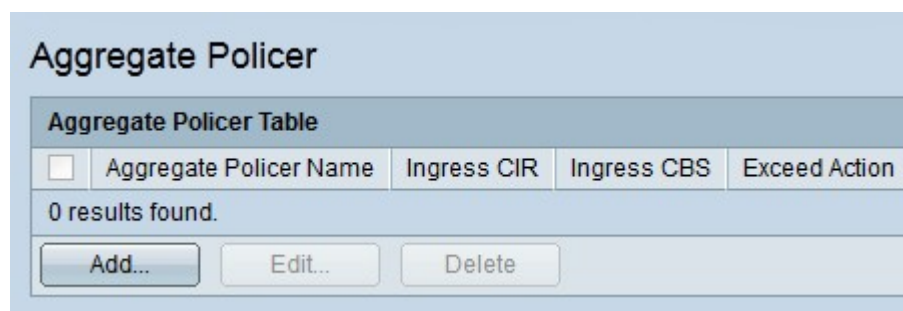
步驟6.如果定義的匹配ACL欄位包含MAC，則在MAC欄位中選擇要應用於類對映的MAC ACL。

步驟7.點選首選ACL欄位中與首選ACL型別對應的單選按鈕。此欄位確定是否應首先根據IP ACL或MAC ACL匹配資料。

步驟8.按一下Apply。

聚合管制器

步驟1.登入到Web配置實用程式並選擇**服務品質> QoS高級模式>聚合管制器**。將開啟 *Aggregate Policer*頁：



Aggregate Policer Table				
<input type="checkbox"/>	Aggregate Policer Name	Ingress CIR	Ingress CBS	Exceed Action
0 results found.				
Add...		Edit...		Delete

步驟2.按一下**Add**。系統將顯示 *Add Aggregate Policer*頁面。

步驟3.在Aggregate Policer Name欄位中輸入聚合監察器的名稱。

步驟4.在Ingress Committed Information Rate(CIR)欄位中輸入入口隊列允許的最大頻寬 (以千位每秒為單位)。

步驟5.在Ingress Committed Burst Size(CBS)欄位中輸入入口隊列的最大突發大小 (以位元組為單位)。這是允許以臨時突發量通過的流量，即使它高於定義的CIR。

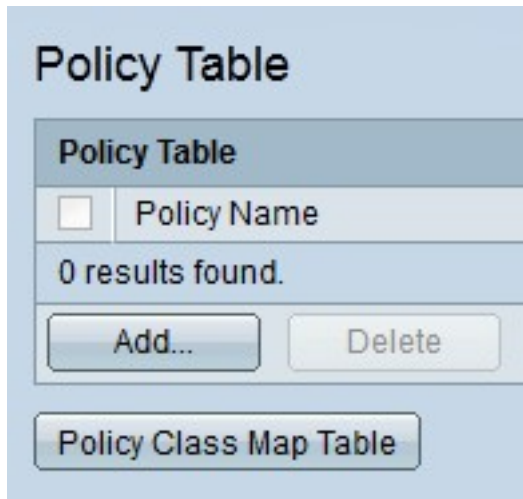
步驟6.點選與「超出操作」欄位中所需操作對應的單選按鈕。當傳入資料包超過CIR時，會發生此動作。

- 轉送 — 封包會被轉送。
- Drop — 封包遭捨棄。
- 超出配置檔案DSCP — 根據超出配置檔案DSCP對映表重新對映資料包的DSCP值。

步驟7.按一下**Apply**。

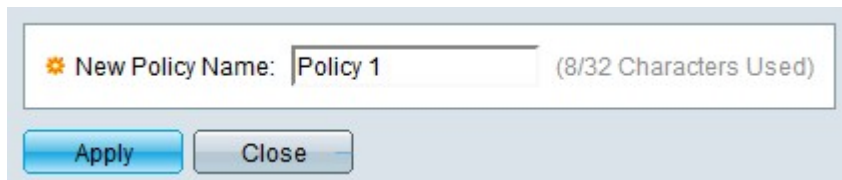
策略表

步驟1.登入到Web配置實用程式並選擇**服務品質> QoS高級模式>策略表**。將開啟 *策略表*頁：



步驟2.按一下**Add**。系統將顯示*Add Policy*視窗。

附註：按一下**Policy Class Map Table**以開啟*Policy Class Maps*頁。



步驟3.在New Policy Name欄位中輸入策略的名稱。

步驟4.按一下**Apply**。

策略類對映

步驟1.登入到Web配置實用程式並選擇**服務品質 > QoS高級模式 > 策略類對映**。將開啟*Policy Class Maps*頁：

步驟2.從Policy Name Equals to下拉選單中選擇一個策略。

步驟3.按一下**Go**顯示對映到指定策略的類對映。

步驟4.按一下**Add**將類對映對映到指定的策略。系統將顯示*Add Policy Class Map*視窗。

//image

策略名稱顯示在「策略名稱」欄位中。

步驟5.從Class Map Name下拉選單中選擇要對映到策略的類對映。

步驟6.點選與「操作型別」欄位中所需操作對應的單選按鈕。

- 使用預設信任模式 — 交換機忽略輸入CoS或DSCP值。與策略匹配的資料包將作為盡力而為傳送。
- Always Trust — 交換機信任與策略匹配的資料包的CoS或DSCP值。如果資料包是IP資料包，則基於資料包的DSCP值，將該資料包放入出口隊列中。否則，根據CoS值，封包會被置入輸出佇列中。
- Set — 從下拉選單中，選擇與策略匹配時將分配資料包的方法。
 - DSCP — 在New Value欄位中輸入將分配給資料包的DSCP值。
 - 隊列 — 在「新值」欄位中輸入資料包將傳送到的出口隊列。
 - CoS — 在New Value欄位中輸入要分配給資料包的CoS值。

步驟7.在Police Type欄位中點選與所需監察器型別對應的單選按鈕。

- 無 — 不使用任何策略。
- Single — 使用單個監察器。
- Aggregate — 使用聚合監察器。

步驟8.如果監察器型別為aggregate，請從Aggregate Policer下拉選單中選擇聚合監察器。

步驟9.如果監察器型別為單一，請填寫以下欄位。

- 輸入承諾資訊速率(CIR) — 在「輸入承諾資訊速率(CIR)」欄位中輸入輸入隊列允許的最大頻寬 (以千位每秒為單位)。
- 輸入承諾突發大小(CBS) — 在「輸入承諾突發大小(CBS)」欄位中輸入輸入隊列的最大突發大小 (以位元組為單位)。這是允許以臨時突發量通過的流量，即使它高於定義的CIR。
- 超出操作 — 點選與「超出操作」欄位中所需操作對應的單選按鈕。當傳入資料包超過CIR時，會發生此動作。
 - 無 — 不採取任何操作。
 - Drop — 丟棄資料包。
 - 超出配置檔案DSCP — 根據超出配置檔案DSCP對映表重新對映資料包的DSCP值。

步驟10.按一下Apply。

策略繫結

*Policy Binding*頁用於將策略繫結到埠。一旦策略繫結到埠，該策略就被視為在該埠上處於活動狀態。一次只能將一個策略繫結到埠，但是可以將單個策略繫結到多個埠。當策略繫結到埠時，它會過濾與定義的策略相匹配的輸入流量並應用QoS。

附註：要編輯策略，必須解除所有埠的繫結。

步驟1.登入到Web配置實用程式並選擇**服務品質 > QoS高級模式 > 策略繫結**。將開啟*Policy Binding*頁：

Policy Binding

Filter: Policy Name equals to

AND Interface Type equals to

g1 g2 g3 g4 g5 g6 g7 g8 g9 g10 g11 g12 g13 g14 g15 g16 g17 g18 g19 g20

步驟2.從Policy Name equals to下拉選單中選擇要繫結到介面的策略。

步驟3.從Interface Type下拉選單中選擇要將策略繫結到的介面型別。

步驟4.按一下「Go」。將顯示介面。

步驟5.選中Binding欄位中所需的覈取方塊，將策略繫結到埠。所有不符合策略規則的資料包將被丟棄。

步驟6.選中Permit Any欄位中所需的覈取方塊，以覆蓋策略並轉發所有資料包。

步驟7.按一下Apply。