

300シリーズマネージドスイッチのQoS拡張モード設定

目的

QoS拡張モードでは、スイッチはポリシーを使用してフローごとのQoSをサポートします。ポリシーとそのコンポーネントには、次の特性があります。

- ポリシーには、1つ以上のクラスマップが含まれる場合があります。
- ポリシーには、ユーザ定義のQoSを持つ1つ以上のフローが含まれます。
- 1つのポリサーは、ポリサーQoS仕様に基づいて、QoSを単一のクラスマップに適用し、したがって単一のフローに適用します。
- 集約ポリサーは、QoSを1つ以上のクラスマップ、つまり1つ以上のフローに適用します。
- フロー単位のQoSは、ポリシーを目的のポートにバインドすることによって、フローに適用されます。

該当するデバイス

- SF/SG 300シリーズマネージドスイッチ

[Software Version]

- v1.2.7.76

QoS詳細モードを設定するためのワークフロー

1. システムの詳細モードを選択します。
2. 外部値を内部値にマッピングするには、内部DSCP値が着信パケットで使用されるものと異なる場合は、「プロファイル外DSCPマッピング」ページで「プロファイル外DSCPマッピング」を設定します。
3. ACLの作成ACLのワークフローについては、『ACLの作成』を参照してください。
4. クラスマップを作成し、「クラスマッピング」ページを使用してACLを関連付けます。
5. 「Policy Table」ページを使用してポリシーを作成し、「Policy Class Map」ページを使用して、ポリシーを1つ以上のクラスマップに関連付けます。以下で使用するポリサーのタイプ。

- 単一ポリサー
- ポリシーを作成して、クラスマップを1つのポリサーに関連付けることができます。
- 集約ポリサー：

「集約ポリサー」ページを使用して、一致するすべてのフレームを集約ポリサーに送信するフローごとにQoSアクションを作成します

6. 最後に、ポリシー・バインディング・ページを使用して、ポリシーをインターフェイスにバインドします。

このドキュメントでは、上記を設定する手順について説明します。

QoS拡張モード

QoS拡張モードの有効化

ステップ1:Web設定ユーティリティにログインし、[Quality of Service] > [General] > [QoS Properties]を選択します。[QoSのプロパティ]ページが開きます。

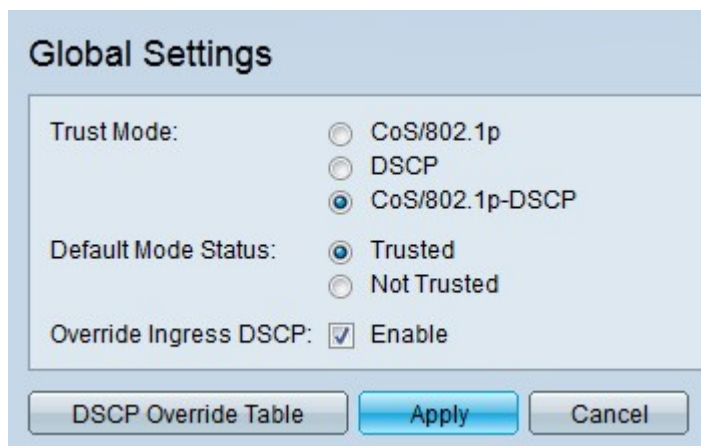
A screenshot of the 'QoS Properties' dialog box. It has a title bar 'QoS Properties'. Inside, there is a section 'QoS Mode:' with three radio button options: 'Disable', 'Basic', and 'Advanced'. The 'Advanced' option is selected. At the bottom, there are two buttons: 'Apply' and 'Cancel'.

ステップ2:[QoS Mode]フィールドで[Advanced]オプションボタンをクリックします。

ステップ3:[Apply]をクリックします。

グローバル設定

ステップ1:Web設定ユーティリティにログインし、[Quality of Service] > [QoS Advanced Mode] > [Global Settings]を選択します。「プロファイル外DSCPマッピング」ページが開きます。

A screenshot of the 'Global Settings' dialog box. It has a title bar 'Global Settings'. Inside, there are three sections: 'Trust Mode:' with three radio button options: 'CoS/802.1p', 'DSCP', and 'CoS/802.1p-DSCP'. The 'CoS/802.1p-DSCP' option is selected. 'Default Mode Status:' with two radio button options: 'Trusted' and 'Not Trusted'. The 'Trusted' option is selected. 'Override Ingress DSCP:' with a checked checkbox and the text 'Enable'. At the bottom, there are three buttons: 'DSCP Override Table', 'Apply', and 'Cancel'.

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 ▼

プロファイル外DSCP再マーキング

ステップ1: Web設定ユーティリティにログインし、[Quality of Service] > [QoS Advanced Mode] > [Out of Profile DSCP Mapping]を選択します。「プロファイル外DSCPマッピング」ページが開きます。

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 ▼

ステップ2:DSCP再マーキングテーブルを設定します。

- DSCP In : 代替値に再マッピングする必要がある着信パケットの値を表示します。
- [DSCP Out]:[DSCP Out]ドロップダウンリストから、DSCP In値に対応する必要なDSCP Out値を選択します。

注 : [Restore Defaults]をクリックして、DSCP再マーキングテーブルをデフォルト値に復元します。デフォルトでは、DSCP Out値が、対応するDSCP In値の値と一致します。

ステップ3:[Apply]をクリックします。

クラスマッピング

ステップ1:Web設定ユーティリティにログインし、[Quality of Service] > [QoS Advanced Mode] > [Class Mapping]を選択します。「クラスマッピング」ページが開きます。

Class Mapping

Class Mapping Table						
☐	Class Map Name	ACL 1	Match	ACL 2	Match	ACL 3

0 results found.

ステップ2:[Add]をクリックします。[Add Class Mapping]ウィンドウが表示されます。

✱ 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

ステップ3:[Class Map Name]フィールドにクラスマップの名前を入力します。

ステップ4:[Match ACL Type]フィールドで、目的のACLに対応するオプションボタンをクリックします。

ステップ5：定義された[Match ACL]フィールドにIPが含まれている場合は、[IP]フィールドで目的のIPタイプのボックスをオンにします。

- [IPv4]:[IPv4]ドロップダウンリストから、クラスマップに適用するIPv4 ACLを選択します。
- [IPv6]:[IPv6]ドロップダウンリストから、クラスマップに適用するIPv6 ACLを選択します。

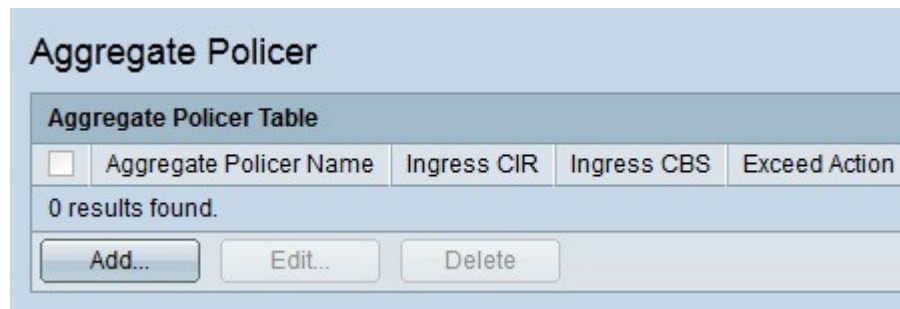
ステップ6：定義された[Match ACL]フィールドにMACが含まれている場合は、[MAC]フィールドでクラスマップに適用するMAC ACLを選択します。

ステップ7:[Preferred ACL]フィールドで、優先ACLタイプに対応するオプションボタンをクリックします。このフィールドは、IP ACLまたはMAC ACLに基づいて、データを最初に照合するかどうかを決定します。

ステップ8:[Apply]をクリックします。

集約ポリサー

ステップ1:Web設定ユーティリティにログインし、[Quality of Service] > [QoS Advanced Mode] > [Aggregate Policer]を選択します。「集約ポリサー」ページが開きます。



Aggregate Policer Table				
☐	Aggregate Policer Name	Ingress CIR	Ingress CBS	Exceed Action
0 results found.				

Add... Edit... Delete

ステップ2:[Add]をクリックします。[Add Aggregate Policer Page]ウィンドウが表示されます。

ステップ3:[Aggregate Policer Name]フィールドに集約ポリサーの名前を入力します。

ステップ4:[Ingress Committed Information Rate (CIR)]フィールドに、入力キューで許可される最大帯域幅 (キロビット/秒) を入力します。

ステップ5:[Ingress Committed Burst Size (CBS)]フィールドに、入力キューの最大バーストサイズ (バイト単位) を入力します。これは、定義されたCIRを超えている場合でも、一時的なバーストとして通過できるトラフィックの量です。

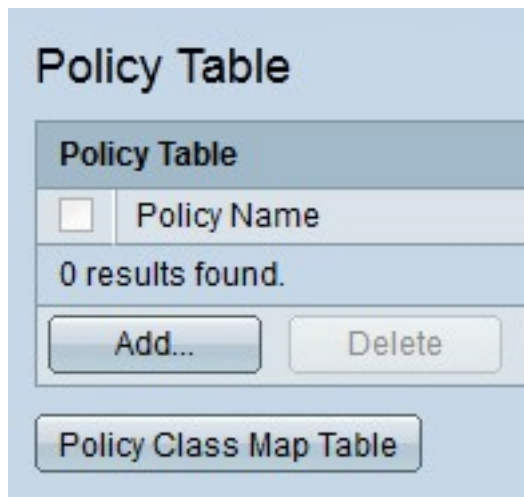
ステップ6:[Exceed Action]フィールドで、目的のアクションに対応するオプションボタンをクリックします。このアクションは、着信パケットがCIRを超えたときに実行されます。

- 転送：パケットが転送されます。
- ドロップ：パケットがドロップされます。
- プロファイル外DSCP：パケットのDSCP値は、プロファイル外DSCPマッピングテーブルに基づいて再マッピングされます。

ステップ7:[Apply]をクリックします。

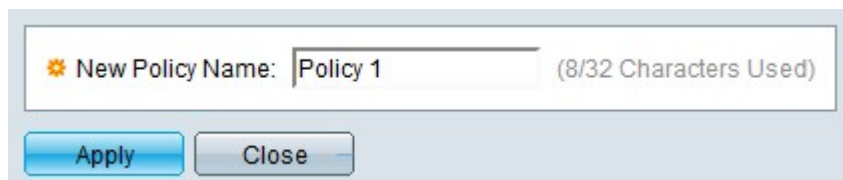
ポリシーテーブル

ステップ1:Web設定ユーティリティにログインし、[Quality of Service] > [QoS Advanced Mode] > [Policy Table]を選択します。「ポリシー・テーブル」ページが開きます。



ステップ2:[Add]をクリックします。[ポリシーの追加]ページウィンドウが表示されます。

注 : [ポリシークラスマップ表]をクリックして、[ポリシークラスマップ]ページを開きます。



ステップ3:[New Policy Name]フィールドにポリシーの名前を入力します。

ステップ4:[Apply]をクリックします。

ポリシークラスマップ

ステップ1:Web設定ユーティリティにログインし、[Quality of Service] > [QoS Advanced Mode] > [Policy Class Maps]を選択します。[ポリシークラスマップ]ページが開きます。

ステップ2:[Policy Name Equals to]ドロップダウンリストからポリシーを選択します。

ステップ3:[Go]をクリックして、指定したポリシーにマップされているクラスマップを表示します。

ステップ4:[Add]をクリックして、クラスマップを指定したポリシーにマップします。[Add Policy Class Map]ウィンドウが表示されます。

//image

ポリシーの名前が[Policy Name]フィールドに表示されます。

ステップ5:[Class Map Name]ドロップダウンリストから、ポリシーにマップするクラスマップを選択します。

ステップ6:[Action Type]フィールドで、目的のアクションに対応するオプションボタンをクリックします。

- Use Default Trust Mode : スイッチは入力CoSまたはDSCP値を無視します。ポリシーに一致するパケットは、ベストエフォートとして送信されます。
- Always Trust : スイッチは、ポリシーに一致するパケットのCoSまたはDSCP値を信頼します。パケットがIPパケットの場合、パケットはパケットのDSCP値に基づいて出力キューに配置されます。そうでない場合、パケットはCoS値に基づいて出力キューに配置されます。
- Set : ドロップダウンリストから、ポリシーに一致するパケットを割り当てる方法を選択します。

- DSCP:[New Value]フィールドに、パケットに割り当てられるDSCP値を入力します。

- [Queue] : パケットの送信先となる出力キューを[New Value]フィールドに入力します。

- CoS : パケットに割り当てられるCoS値を[New Value]フィールドに入力します。

ステップ7:[Police Type]フィールドで、目的のポリサータイプに対応するオプションボタンをクリックします。

- None : ポリシーは使用されません。
- Single : 単一のポリサーが使用されます。
- 集約 : 集約ポリサーが使用されます。

ステップ8 : ポリサータイプがaggregateの場合は、[Aggregate Policer]ドロップダウンリストから集約ポリサーを選択します。

ステップ9 : ポリサータイプが単一の場合は、次のフィールドに入力します。

- Ingress Committed Information Rate(CIR) : 入力キューで許可される最大帯域幅 (キロビット / 秒) を[Ingress Committed Information Rate(CIR)]フィールドに入力します。
- Ingress Committed Burst Size(CBS) : 入力キューの最大バーストサイズ (バイト単位) を[Ingress Committed Burst Size(CBS)]フィールドに入力します。これは、定義されたCIRを超えている場合でも、一時的なバーストとして通過できるトラフィックの量です。
- [超過アクション(Exceed Action)]:[超過アクション(Exceed Action)]フィールドで、目的のアクションに対応するオプションボタンをクリックします。このアクションは、着信パケットがCIRを超えたときに実行されます。

- None – アクションは実行されません。

- Drop : パケットがドロップされます。

- Out of Profile DSCP : パケットのDSCP値は、Out of Profile DSCP Mapping Tableに基づいて再マッピングされます。

ステップ10:[Apply]をクリックします。

ポリシーバインディング

ポリシーバインドページは、ポリシーをポートにバインドするために使用されます。ポートにバインドされたポリシーは、ポートでアクティブと見なされます。一度に1つのポートにバインドできるポリシーは1つだけですが、1つのポリシーを複数のポートにバインドすることはできます。ポリシーがポートにバインドされると、定義されたポリシーに一致する入カトラフィックにQoSがフィルタリングされて適用されます。

注：ポリシーを編集するには、すべてのポートからバインドを解除する必要があります。

ステップ1: Web設定ユーティリティにログインし、[Quality of Service] > [QoS Advanced Mode] > [Policy Binding]を選択します。「ポリシーバインド」ページが開きます。

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

ステップ2: [Policy Name equals to] ドロップダウンリストから、インターフェイスにバインドするポリシーを選択します。

ステップ3: [Interface Type] ドロップダウンリストから、ポリシーをバインドするインターフェイスのタイプを選択します。

ステップ4: [Go] をクリックします。インターフェイスが表示されます。

ステップ5: [Binding] フィールドで目的のチェックボックスをオンにして、ポリシーをポートにバインドします。ポリシーのルールを満たさないパケットはすべて廃棄されます。

ステップ6: [Permit Any] フィールドで必要なチェックボックスをオンにして、ポリシーを上書きしてすべてのパケットを転送します。

ステップ7: [Apply] をクリックします。