

QoS Advanced Mode-Konfiguration für Managed Switches der Serie 300

Ziele

Im erweiterten QoS-Modus verwendet der Switch Richtlinien zur Unterstützung von QoS pro Datenfluss. Die Richtlinie und ihre Komponenten zeichnen sich durch folgende Merkmale aus:

- Eine Richtlinie kann eine oder mehrere Klassenzuordnungen enthalten.
- Eine Richtlinie enthält einen oder mehrere Datenflüsse mit jeweils benutzerdefinierter QoS.
- Ein einzelner Policer wendet die QoS auf eine einzelne Klassenzuordnung und damit auf einen einzigen Fluss an, der auf der QoS-Spezifikation der Richtlinie basiert.
- Eine Aggregat Policer wendet die QoS auf eine oder mehrere Klassenzuordnungen und damit auf einen oder mehrere Datenflüsse an.
- QoS pro Datenfluss wird auf Datenflüsse angewendet, indem die Richtlinien an die gewünschten Ports gebunden werden.

Anwendbare Geräte

- Managed Switches der Serie SF/SG 300

Softwareversion

- V1.2.7.76

Workflow zum Konfigurieren des erweiterten QoS-Modus

1. Wählen Sie Erweiterter Modus für das System aus.
2. Wenn sich die internen DSCP-Werte von den Werten für eingehende Pakete unterscheiden, konfigurieren Sie die Out-of-Profile-DSCP-Zuordnung auf der *Seite Out of Profile DSCP Mapping (Out-of-Profile-DSCP-Zuordnung)*, um die externen Werte internen Werten zuzuordnen.
3. Erstellen von ACLs. Informationen zum Workflow von ACLs finden Sie im Dokument *Creating ACLs (Erstellen von ACLs)*.
4. Erstellen Sie Klassenzuordnungen, und ordnen Sie ihnen die ACLs mithilfe der *Seite Klassenzuordnung* zu.
5. Erstellen Sie mithilfe der *Seite "Policy Table" (Richtlinientabelle)* eine Richtlinie, und ordnen Sie die Richtlinie mithilfe der *Seite "Policy Class Map"* einer oder mehreren Klassenzuordnungen zu. Die unten verwendeten Policer-Typen.

- Zentraler Policer
- Eine Richtlinie kann erstellt werden, um die Klassenzuordnung einem einzelnen Policer zuzuordnen.

- Aggregate-Policer:

Erstellen Sie eine QoS-Aktion für jeden Fluss, der alle übereinstimmenden Frames mithilfe der Seite für die *Aggregation Policer* an den Aggregations-Policer sendet.

6. Binden Sie die Richtlinie schließlich mithilfe der *Policy Binding Page* an eine Schnittstelle.

In diesem Dokument wird das Verfahren zum Konfigurieren der oben genannten Optionen veranschaulicht.

Erweiterter QoS-Modus

Aktivieren des erweiterten QoS-Modus

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Quality of Service > General > QoS Properties** aus. Die Seite *QoS-Eigenschaften* wird geöffnet:



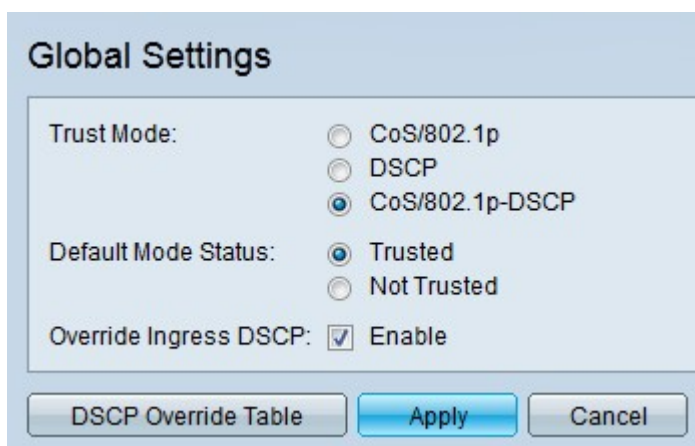
The screenshot shows a configuration window titled "QoS Properties". It contains three radio button options for "QoS Mode": "Disable", "Basic", and "Advanced". The "Advanced" option is selected. Below the options are two buttons: "Apply" and "Cancel".

Schritt 2: Klicken Sie im Feld "QoS-Modus" auf das Optionsfeld **Erweitert**.

Schritt 3: Klicken Sie auf **Übernehmen**.

Globale Einstellungen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Quality of Service > QoS Advanced Mode > Global Settings** aus. Die Seite *"Out of Profile DSCP Mapping"* wird geöffnet:



The screenshot shows a configuration window titled "Global Settings". It contains three sections of radio button options: "Trust Mode" with options "CoS/802.1p", "DSCP", and "CoS/802.1p-DSCP" (selected); "Default Mode Status" with options "Trusted" (selected) and "Not Trusted"; and "Override Ingress DSCP" with a checked checkbox and the label "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 ▼

Out-of-Profile-DSCP - Neukennzeichnung

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Quality of Service > QoS Advanced Mode > Out of Profile DSCP Mapping** aus. Die Seite "Out of Profile DSCP Mapping" wird geöffnet:

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 ▾

Schritt 2: Konfigurieren Sie die DSCP-Remarking-Tabelle.

- DSCP In - Zeigt den Wert der eingehenden Pakete an, die einem alternativen Wert neu zugeordnet werden müssen.
- DSCP Out (DSCP ausgehend): Wählen Sie in der Dropdown-Liste "DSCP Out" (DSCP ausgehend) den gewünschten DSCP Out-Wert aus, der dem DSCP In-Wert entspricht.

Hinweis: Klicken Sie auf Restore Defaults (Standardeinstellungen wiederherstellen), um die Tabelle mit der erneuten Kennzeichnung des DSCP auf die Standardwerte wiederherzustellen. In der Standardeinstellung stimmen die DSCP Out-Werte mit den Werten der entsprechenden DSCP In-Werte überein.

Schritt 3: Klicken Sie auf **Übernehmen**.

Klassenzuordnung

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Quality of Service > QoS Advanced Mode > Class Mapping** aus. Die Seite *Klassenzuordnung* wird geöffnet:

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"/>				

Schritt 2: Klicken Sie auf **Hinzufügen**. Das Fenster *Klassenzuordnung hinzufügen* wird angezeigt.

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

Schritt 3: Geben Sie im Feld Name der Klassenzuordnung einen Namen für die Klassenzuordnung ein.

Schritt 4: Klicken Sie im Feld "Match ACL Type" (ACL-Typ zuordnen) auf das Optionsfeld für die gewünschte ACL.

Schritt 5: Wenn das definierte Feld "Match ACL" (ACL zuordnen) IP enthält, aktivieren Sie das Kontrollkästchen des gewünschten IP-Typs im IP-Feld.

- IPv4 - Wählen Sie aus der IPv4-Dropdown-Liste die IPv4-ACL aus, die auf die Klassenzuordnung angewendet werden soll.
- IPv6 - Wählen Sie aus der IPv6-Dropdown-Liste die IPv6-ACL aus, die auf die Klassenzuordnung angewendet werden soll.

Schritt 6: Wenn das definierte Feld "Match ACL" (ACL zuordnen) MAC enthält, wählen Sie die MAC-ACL aus, die auf die Klassenzuordnung im MAC-Feld angewendet werden soll.

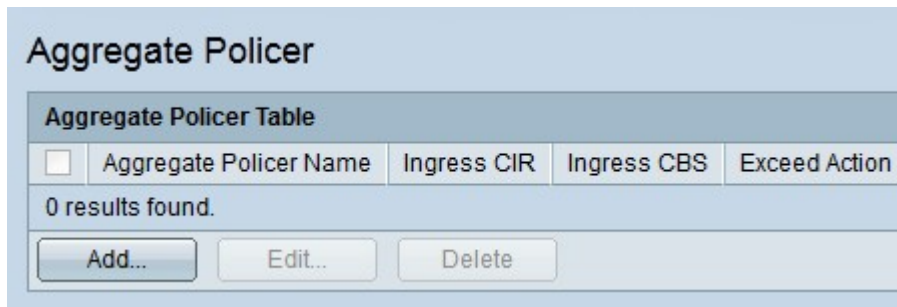
Schritt 7: Klicken Sie auf das Optionsfeld für den bevorzugten ACL-Typ im Feld Bevorzugte

ACL. Dieses Feld legt fest, ob die Daten zuerst anhand von IP-ACLs oder MAC-ACLs abgeglichen werden sollen.

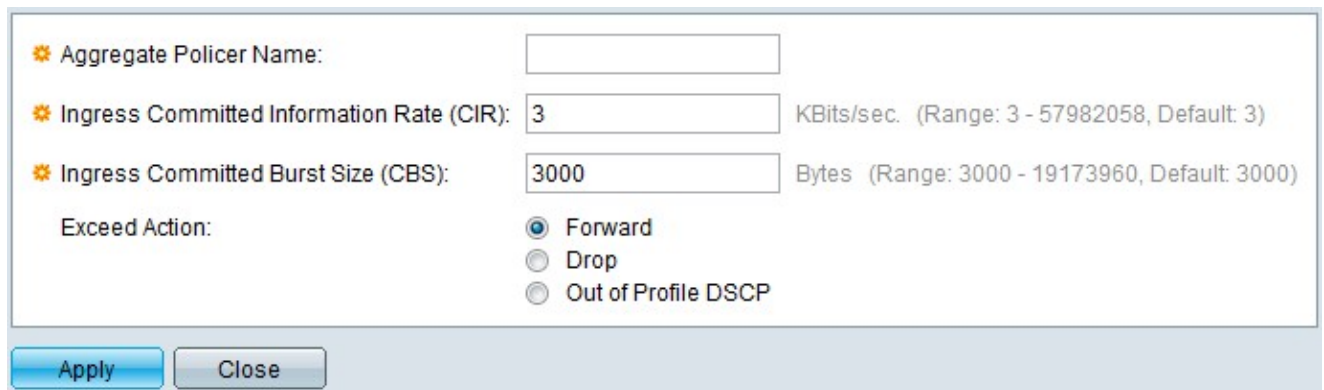
Schritt 8: Klicken Sie auf **Übernehmen**.

Aggregations-Policer

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Quality of Service > QoS Advanced Mode > Aggregate Policer** aus. Die Seite *Aggregate Policer* wird geöffnet:



Schritt 2: Klicken Sie auf **Hinzufügen**. Das Fenster *Seite "Aggregate Policer hinzufügen"* wird angezeigt.



Schritt 3: Geben Sie im Feld **Aggregate Policer Name** einen Namen für die Aggregate Policer ein.

Schritt 4: Geben Sie die maximal zulässige Bandbreite für die Eingangswarteschlange (in Kilobit pro Sekunde) im Feld **Ingress Committed Information Rate (CIR)** (Ingress Committed Information Rate (Eingangs-Committed-Informationsrate)) ein.

Schritt 5: Geben Sie im Feld **Ingress Committed Burst Size (CBS)** (Ingress Committed Burst Size) die maximale Burst-Größe für die Eingangswarteschlange (in Byte) ein. Dabei handelt es sich um die Datenverkehrsmenge, die als vorübergehender Burst weitergeleitet werden darf, selbst wenn sie über der festgelegten CIR liegt.

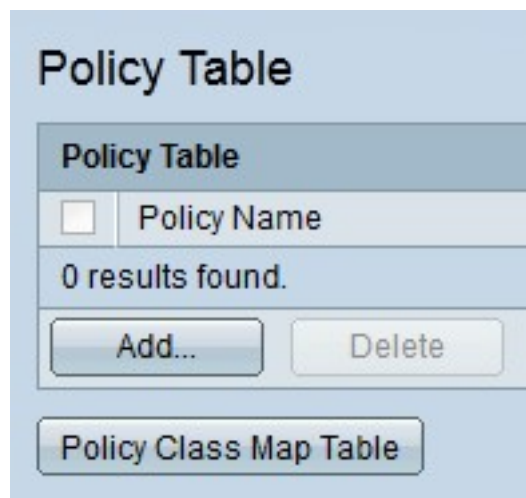
Schritt 6: Klicken Sie auf das Optionsfeld für die gewünschte Aktion im Feld **Aktion** überschritten. Diese Aktion tritt ein, wenn ein eingehendes Paket die CIR überschreitet.

- Forward (Weiterleiten): Das Paket wird weitergeleitet.
- Drop - Das Paket wird verworfen.
- Out-of-Profile-DSCP - Der DSCP-Wert des Pakets wird basierend auf der Out-of-Profile-DSCP-Zuordnungstabelle neu zugeordnet.

Schritt 7: Klicken Sie auf **Übernehmen**.

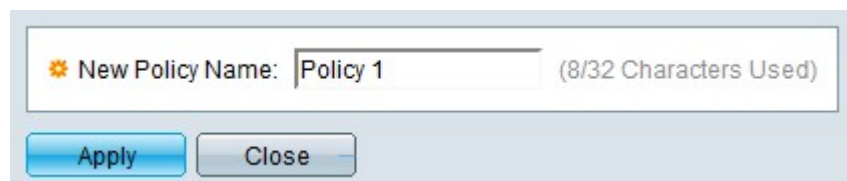
Richtlinien-Tabelle

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Quality of Service > QoS Advanced Mode > Policy Table** aus. Die Seite "*Policy Table*" wird geöffnet:



Schritt 2: Klicken Sie auf **Hinzufügen**. Das Fenster Seite "*Richtlinie hinzufügen*" wird angezeigt.

Hinweis: Klicken Sie auf **Policy Class Map Table**, um die Seite *Policy Class Maps* zu öffnen.



Schritt 3: Geben Sie einen Namen für die Richtlinie im Feld "Name der neuen Richtlinie" ein.

Schritt 4: Klicken Sie auf **Übernehmen**.

Richtlinien-Klassenzuordnungen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Quality of Service > QoS Advanced Mode > Policy Class Maps** aus. Die Seite *Policy Class Maps* wird geöffnet:

Schritt 2: Wählen Sie in der Dropdownliste Policy Name Equals to eine Richtlinie aus.

Schritt 3: Klicken Sie auf **Go**, um die der angegebenen Richtlinie zugeordneten Klassenzuordnungen anzuzeigen.

Schritt 4: Klicken Sie auf **Hinzufügen**, um der angegebenen Richtlinie eine Klassenzuordnung zuzuordnen. Das Fenster *Policy Class Map hinzufügen* wird angezeigt.

//image

Der Name der Richtlinie wird im Feld Policy Name (Richtlinienname) angezeigt.

Schritt 5: Wählen Sie in der Dropdownliste Name der Klassenzuordnung eine Klassenzuordnung aus, die der Richtlinie zugeordnet werden soll.

Schritt 6: Klicken Sie auf das Optionsfeld für die gewünschte Aktion im Feld Aktionstyp.

- Default Trust Mode (Standard-Vertrauensmodus verwenden): Der Switch ignoriert den eingehenden CoS- oder DSCP-Wert. Die Pakete, die mit der Richtlinie übereinstimmen, werden bestmöglich gesendet.
- Always Trust (Immer vertrauen): Der Switch vertraut dem CoS- oder DSCP-Wert von Paketen, die der Richtlinie entsprechen. Wenn es sich bei einem Paket um ein IP-Paket handelt, wird das Paket in einer Ausgangswarteschlange platziert, basierend auf dem DSCP-Wert des Pakets. Andernfalls wird das Paket basierend auf dem CoS-Wert in eine Ausgangswarteschlange gestellt.
- Set (Satz): Wählen Sie aus der Dropdown-Liste die Methode aus, in der Pakete zugewiesen werden, wenn sie der Richtlinie entsprechen.
 - DSCP - Geben Sie den DSCP-Wert ein, der den Paketen im Feld Neuer Wert zugewiesen wird.
 - Queue (Warteschlange) - Geben Sie die Ausgangswarteschlange ein, an die die Pakete im Feld New Value (Neuer Wert) gesendet werden.
 - CoS - Geben Sie den CoS-Wert ein, der den Paketen im Feld Neuer Wert zugewiesen wird.

Schritt 7: Klicken Sie auf das Optionsfeld für den gewünschten Policer-Typ im Feld Polzeichyp.

- Keine - Es wird keine Richtlinie verwendet.
- Single (Einzel) - Es wird eine einzige Policer verwendet.
- Aggregate (Aggregat) - Es wird eine aggregierte Policer verwendet.

Schritt 8: Wenn der Policer-Typ aggregiert ist, wählen Sie in der Dropdown-Liste Aggregate Policer (Aggregierter Policer) einen aggregierten Policer aus.

Schritt 9: Wenn der Policer-Typ Single ist, füllen Sie die folgenden Felder aus.

- Eingangs-Committed Information Rate (CIR) - Geben Sie die maximal zulässige Bandbreite für die Eingangs-Warteschlange (in Kilobit pro Sekunde) im Feld Ingress Committed Information Rate (CIR) ein.
- Ingress Committed Burst Size (CBS) (Eingesendete Burst-Größe) - Geben Sie die maximale Burst-Größe für die Eingangswarteschlange (in Byte) im Feld Ingress Committed Burst Size (CBS) ein. Dabei handelt es sich um die Datenverkehrsmenge, die als vorübergehender Burst

weitergeleitet werden darf, selbst wenn sie über der festgelegten CIR liegt.

- Exceed Action (Aktion überschritten) - Klicken Sie auf das Optionsfeld für die gewünschte Aktion im Feld Exceed Action (Aktion überschritten). Diese Aktion tritt ein, wenn ein eingehendes Paket die CIR überschreitet.
 - Keine — Es werden keine Maßnahmen ergriffen.
 - Drop - Das Paket wird verworfen.
 - Out-of-Profile-DSCP - Der DSCP-Wert des Pakets wird basierend auf der Out-of-Profile-DSCP-Zuordnungstabelle neu zugeordnet.

Schritt 10: Klicken Sie auf **Übernehmen**.

Richtlinienbindung

Die Seite *Richtlinienbindung* wird verwendet, um eine Richtlinie an Ports zu binden. Eine Richtlinie gilt als auf dem Port aktiv, sobald sie an den Port gebunden ist. Es kann jeweils nur eine Richtlinie an einen Port gebunden werden, jedoch kann eine einzelne Richtlinie an mehrere Ports gebunden werden. Wenn eine Richtlinie an einen Port gebunden ist, filtert sie und wendet QoS auf eingehenden Datenverkehr an, der der definierten Richtlinie entspricht.

Hinweis: Um eine Richtlinie zu bearbeiten, muss sie von allen Ports ungebunden sein.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Quality of Service > QoS Advanced Mode > Policy Binding** aus. Die Seite *Richtlinienbindung* wird geöffnet:

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

Schritt 2: Wählen Sie in der Dropdownliste Policy Name equals to die Richtlinie aus, die Sie an Schnittstellen binden möchten.

Schritt 3: Wählen Sie aus der Dropdown-Liste Interface Type (Schnittstellentyp) den Schnittstellentyp aus, an den Sie die Richtlinie binden möchten.

Schritt 4: Klicken Sie auf **Los**. Die Schnittstellen werden angezeigt.

Schritt 5: Aktivieren Sie die gewünschten Kontrollkästchen im Feld Bindung, um die Richtlinie an den Port zu binden. Alle Pakete, die nicht den Regeln der Richtlinie entsprechen, werden verworfen.

Schritt 6: Aktivieren Sie die gewünschten Kontrollkästchen im Feld "Zulassen beliebig", um die Richtlinie zu überschreiben und alle Pakete weiterzuleiten.

Schritt 7: Klicken Sie auf **Übernehmen**.