# Content

# Chapter 1 QoS Configuration

## 1.1 Introduction to QoS

QoS (Quality of Service) is a set of capabilities that allow you to create differentiated services for network traffic, thereby providing better service for selected network traffic. QoS is a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate extra bandwidth but provides more effective bandwidth management according to the application requirement and network management policy.

## 1.1.1 QoS Terms

**QoS:** Quality of Service, provides a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate new bandwidth but provides more effective bandwidth management according to the application requirement and network management.

**QoS Domain:** QoS Domain supports QoS devices to form a net-topology that provides Quality of Service, so this topology is defined as QoS Domain.

**CoS:** Class of Service, the classification information carried by Layer 2 802.1Q frames, taking 3 bits of the Tag field in frame header, is called user priority level in the range of 0 to 7.

Layer 2 802.1Q/P Frame

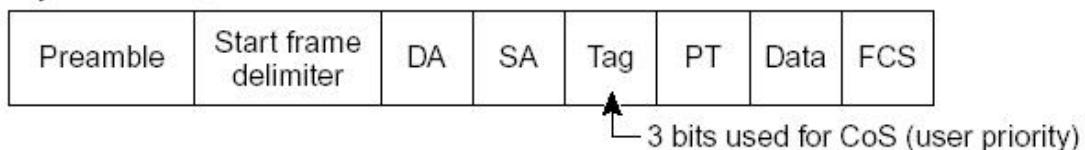| Preamble | Start frame delimiter | DA | SA | Tag | PT | Data | FCS |

— 3 bits used for CoS (user priority)

Fig 1- 1 CoS priority

**ToS:** Type of Service, a one-byte field carried in Layer 3 IPv4 packet header to symbolize the service type of IP packets. Among ToS field can be IP Precedence value or DSCP value.

Layer 3 IPv4 Packet

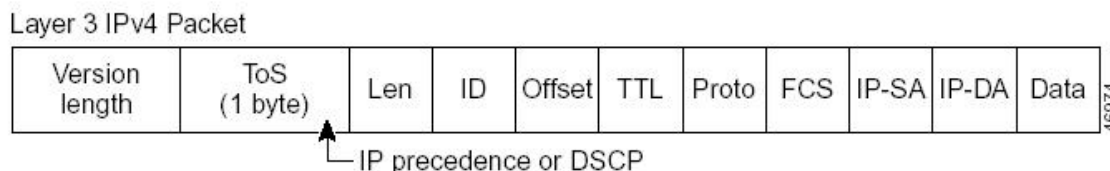| Version length | ToS (1 byte) | Len | ID | Offset | TTL | Proto | FCS | IP-SA | IP-DA | Data |
|---|---|---|---|---|---|---|---|---|---|---|

└─ IP precedence or DSCP

Fig 1- 2 ToS priority

**IP Precedence:** IP priority. Classification information carried in Layer 3 IP packet header, occupying 3 bits, in the range of 0 to 7.

**DSCP:** Differentiated Services Code Point, classification information carried in Layer 3 IP packet header, occupying 6 bits, in the range of 0 to 63, and is downward compatible with IP Precedence.

**Internal Priority:** The internal priority setting of the switch chip, it's valid range relates with the chip, it's shortening is Int-Prio or IntP.

**Drop Precedence:** When processing the packets, firstly drop the packets with the bigger drop precedence, the ranging is 0-1. It's shortening is Drop-Prec or DP.

**Classification:** The entry action of QoS, classifying packet traffic according to the classification information carried in the packet and ACLs.

**Policing:** Ingress action of QoS that lays down the policing policy and manages the classified packets.

**Remark:** Ingress action of QoS, perform allowing, degrading or discarding operations to packets according to the policing policies.

Scheduling**: QoS** *egress* action. Add the packets to the corresponding egress queue according to the internal priority. And then decide sending and dropping according to Drop Precedence, sending algorithm and queue weight of egress queue.

## 1.1.2 QoS Implementation

To implement the switch software QoS, a general, mature reference model should be given. QoS can not create new bandwidth, but can maximize the adjustment and configuration for the current bandwidth resource. Fully implemented QoS can achieve complete management over the network traffic. The following is as accurate as possible a description of QoS.

The data transfer specifications of IP cover only addresses and services of source and destination, and ensure correct packet transmission using OSI layer 4 or above protocols such as TCP. However, rather than provide a mechanism for providing and protecting packet transmission bandwidth, IP provide bandwidth service by the best effort. This is acceptable for services like Mail and FTP, but for increasing multimedia business data and e-business data transmission, this best effort method cannot satisfy the bandwidth and low-lag requirement.

Based on differentiated service, QoS specifies a priority for each packet at the ingress. The classification information is carried in Layer 3 IP packet header or Layer 2 802.1Q frame header. QoS provides same service to packets of the same priority, while offers different operations for packets of different priority.  QoS-enabled switch or router can provide different bandwidth according to the packet classification information, and can remark on the classification information according to the policing policies configured, and may discard some low priority packets in case of bandwidth shortage.

If devices of each hop in a network support differentiated service, an end-to-end QoS solution can be created. QoS configuration is flexible, the complexity or simplicity depends on the network topology and devices and analysis to incoming/outgoing traffic.

## 1.1.3  Basic QoS Model

The basic QoS consists of four parts: Classification, Policing, Remark and Scheduling, where classification, policing and remark are sequential ingress actions, and Queuing and Scheduling are QoS egress actions.
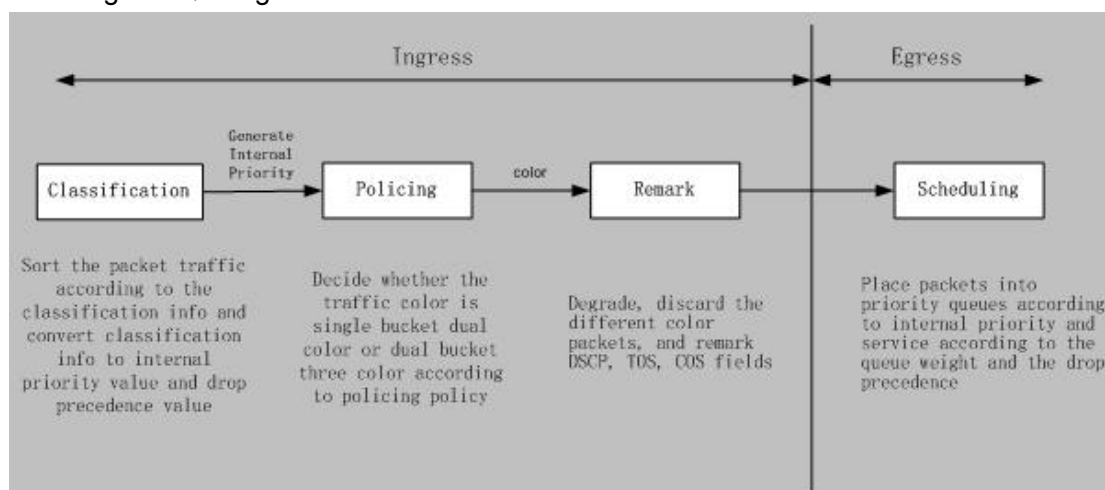


Fig 1-  3 Basic QoS Model

**Classification:** Classify traffic according to packet classification information and generate internal priority based the classification information. For different packet types, classification is performed differently; the flowchart below explains this in detail.
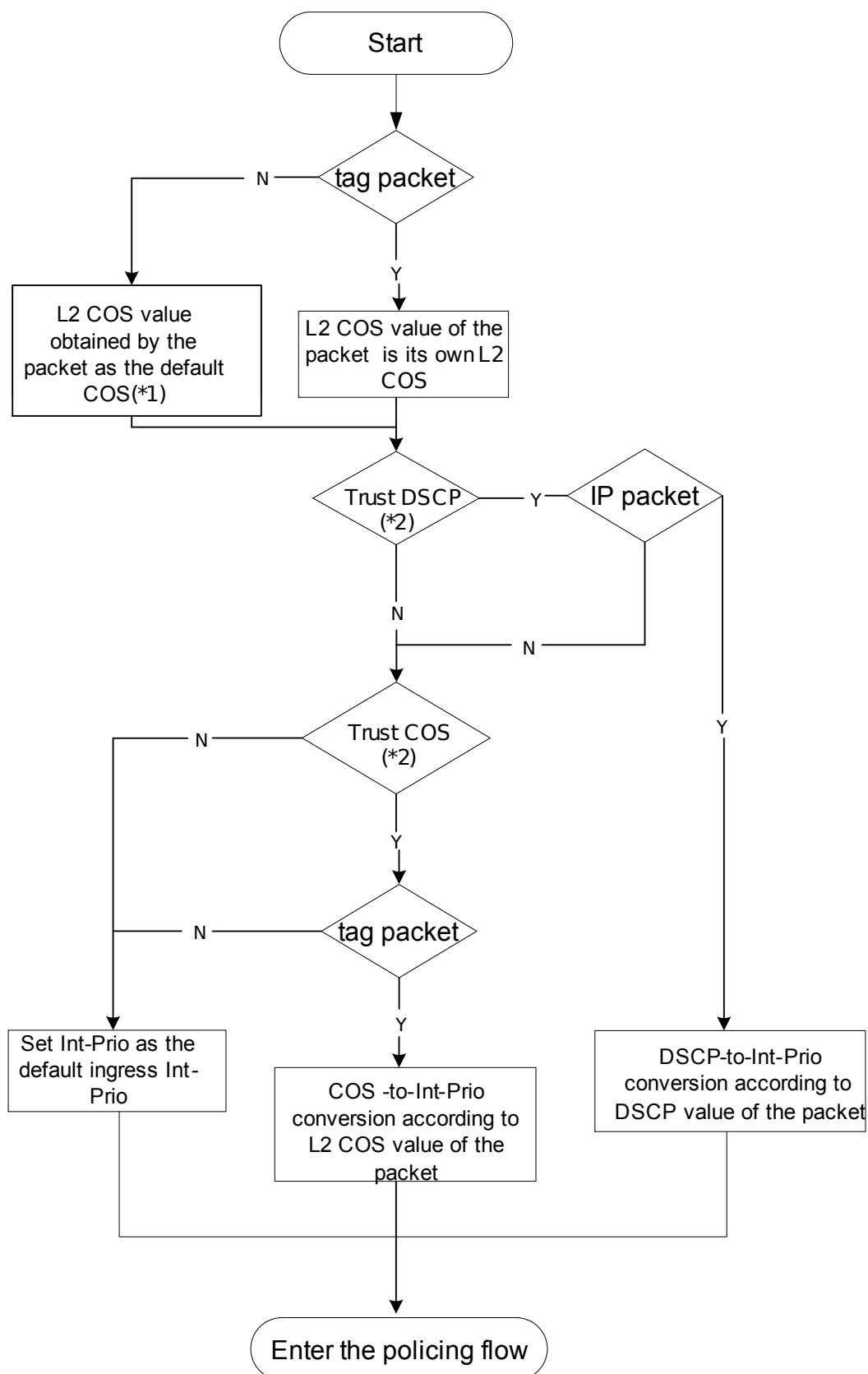
Fig 1- 4 Classification process

Note 1: L2 CoS value is considered a property of the packets, there is no relation with the internal priority obtained of the following flow.

Note 2: Allow Trust DSCP and Trust COS to be configured at the same time, the priority is as follows: DSCP>COS.

**Policing and remark:** Each packet in classified ingress traffic is assigned an internal priority value, and can be policed and remarked.

Policing can be performed based on the flow to configure different policies that allocate bandwidth to classified traffic, the assigned bandwidth policy may be single bucket dual color or dual bucket three color. The traffic, will be assigned with different color, can be discarded or passed, for the passed packets, add the remarking action. Remarking uses a new Int-Prio value of lower priority to replace the original higher level Int-Prio value in the packet. COS and DSCP fields will be modifed according to the new Int-Prio at the egress. The following flowchart describes the operations.

```
                          ╭────────────────╮
                          │      Start      │
                          ╰────────────────╯
                                   │
                                   ▼
                          ╱◇◇◇◇◇◇◇◇◇◇◇╲
                  No ─────╱ Whether configure ╲
                          ╲   the policy    ╱
                           ╲◇◇◇◇◇◇◇◇◇◇◇╱
                                   │
                                  Yes
                                   │
                                   ▼
                          ╱◇◇◇◇◇◇◇◇◇◇◇╲
                          ╱ Unrelated action ╲──── Drop ────┐
                          ╲  with the color ╱               │
                           ╲◇◇◇◇◇◇◇◇◇◇◇╱                    │
                                   │                        │
                                  Pass                      │
                                   │                        │
                                   ▼                        │
                  ┌─────────────────────────────┐          │
                  │ The option is as follows:    │          │
                  │ Set Int-Prio: Set the internal priority of │
                  │ the packets                  │          │
                  └─────────────────────────────┘          │
                                   │                        │
                                   ▼                        │
                  ┌─────────────────────────────┐          │
                  │ Decide the packet color      │          │
                  │ and action according to      │          │
                  │ the policing policy          │          │
                  └─────────────────────────────┘          │
                                   │                        │
                                   ▼                        │
                          ╱◇◇◇◇◇◇◇◇◇◇◇╲                    │
                          ╱  The specific   ╲──── Drop ─────┤
                          ╲  color action  ╱                │
                           ╲◇◇◇◇◇◇◇◇◇◇◇╱                    │
                                   │                        │
                                  Pass                      │
                                   │                        │
                                   ▼                        │
                  ┌─────────────────────────────────────┐  │
                  │ Select one option of the following： │  │
                  │ Set Int-Prio: Set the internal priority of the │
                  │ packets( *1)                         │  │
                  │ Policied-IntP-Transmit: Drop the internal priority of │
                  │ the packets( *2)                     │  │
                  └─────────────────────────────────────┘  │
                                   │                        │
                                   ▼                        ▼
                          ╭────────────────╮      ╭────────────────╮
                          │ Enter scheduling │      │   Drop the     │
                          ╰────────────────╯      │    packets     │
                                                   ╰────────────────╯
```
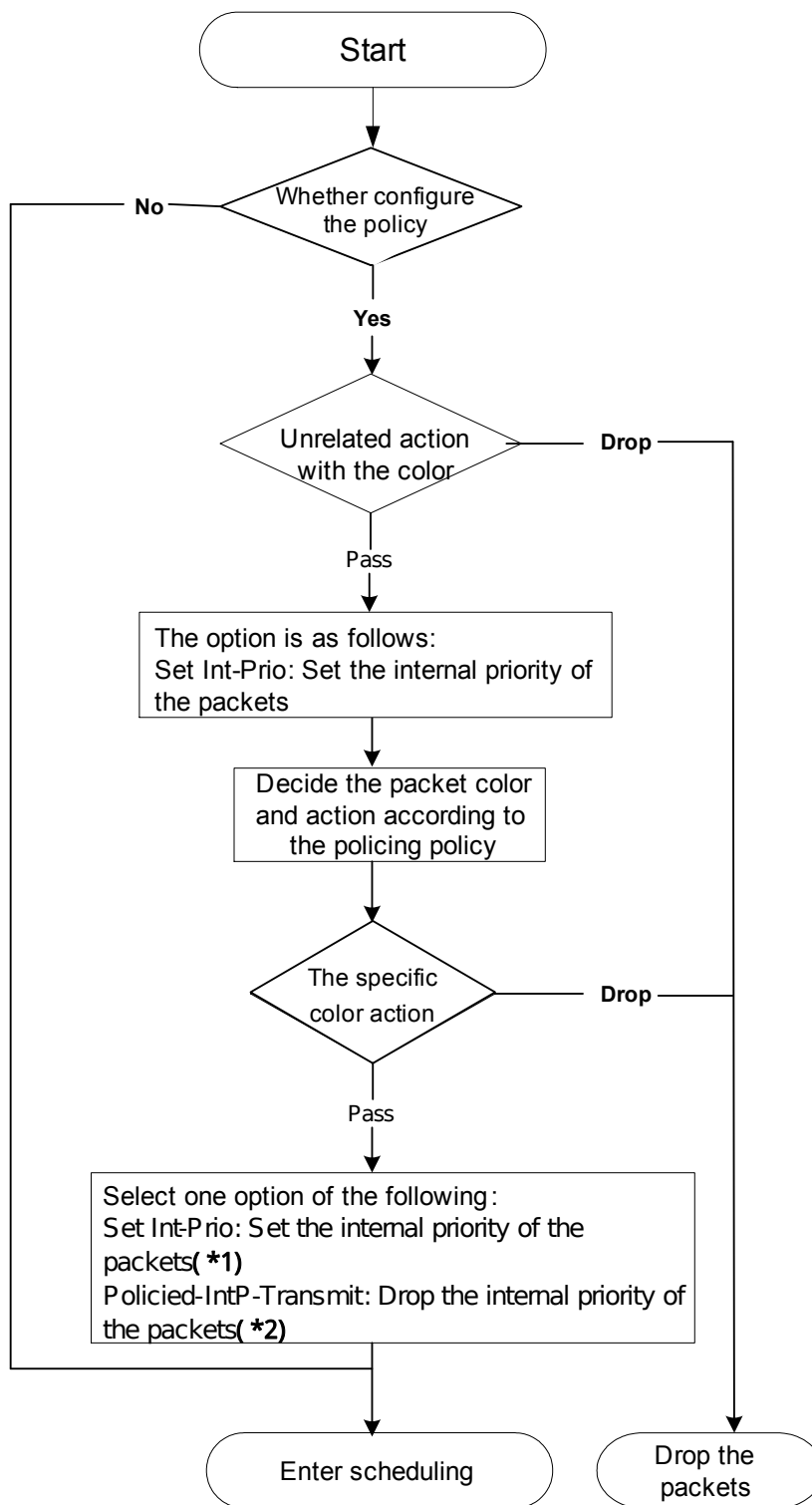
Fig 1- 5 Policing and Remarking process

Note 1: Int-Prio will be covered with the after setting, Set Int-Prio of the specific color action will cover Set Int-Prio of the unrelated action with the color.

Note 2: Drop the internal priority of the packets according to IntP-to-IntP map. Source Int-Prio means to the obtainable Int-Prio in Classification flow or Int-Prio set by the unrelated action with the color.

**Queuing and scheduling:** There are the internal priority for the egress packets, the scheduling operation assigns the packets to different priority queues according to the internal priority, and then forward the packets according to the priority queue weight and the drop precedence. The following flowchart describes the scheduling operation.
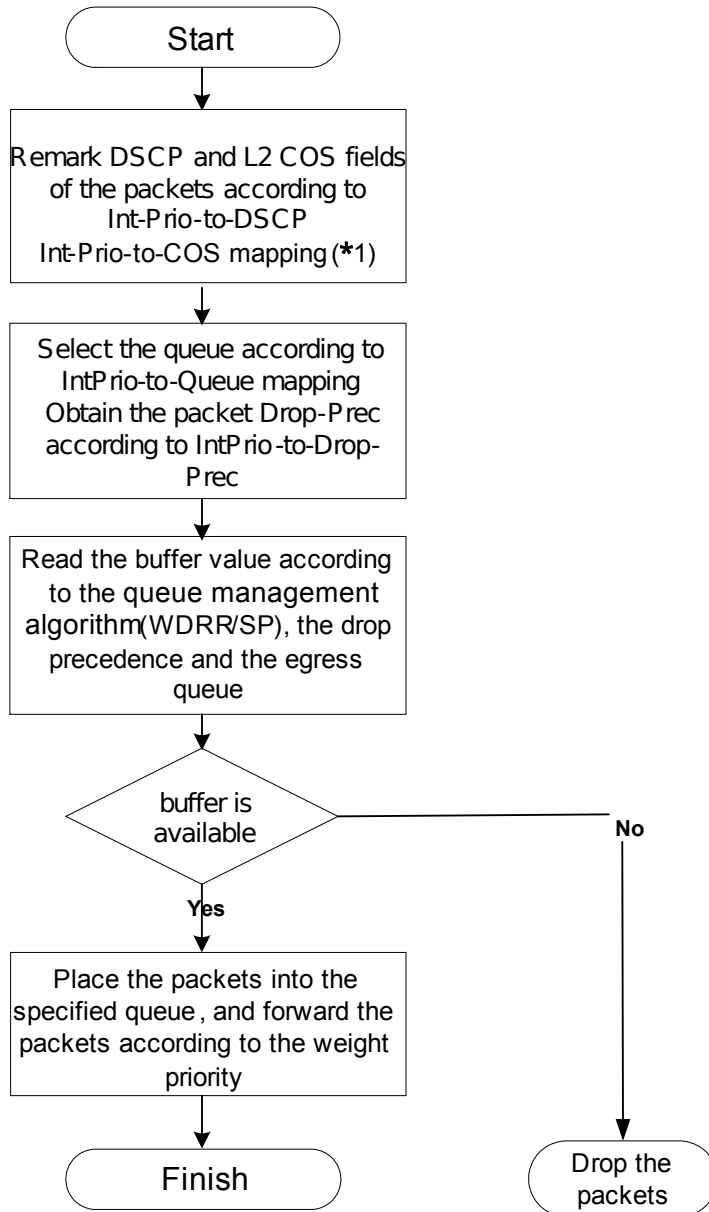
```
                    ┌───────────────────┐
                    │      Start        │
                    └───────────────────┘
                              │
                              ▼
          ┌───────────────────────────────────┐
          │ Remark DSCP and L2 COS fields      │
          │ of the packets according to        │
          │ Int-Prio-to-DSCP                   │
          │ Int-Prio-to-COS mapping (*1)       │
          └───────────────────────────────────┘
                              │
                              ▼
          ┌───────────────────────────────────┐
          │ Select the queue according to      │
          │ IntPrio-to-Queue mapping           │
          │ Obtain the packet Drop-Prec        │
          │ according to IntPrio-to-Drop-      │
          │ Prec                               │
          └───────────────────────────────────┘
                              │
                              ▼
          ┌───────────────────────────────────┐
          │ Read the buffer value according    │
          │ to the queue management            │
          │ algorithm(WDRR/SP), the drop       │
          │ precedence and the egress          │
          │ queue                              │
          └───────────────────────────────────┘
                              │
                              ▼
                      ╱───────────╲
                     ╱ buffer is    ╲──────────────── No
                     ╲ available    ╱                  │
                      ╲───────────╱                    │
                           │                           │
                          Yes                          │
                           │                           │
                           ▼                           ▼
          ┌───────────────────────────────┐   ┌─────────────┐
          │ Place the packets into the     │   │ Drop the    │
          │ specified queue, and forward   │   │ packets     │
          │ the packets according to the   │   └─────────────┘
          │ weight priority                │
          └───────────────────────────────┘
                           │
                           ▼
                    ┌───────────────┐
                    │    Finish     │
                    └───────────────┘
```

Fig 1- 6 Queuing and Scheduling process

Note 1: The ingress configures pass-through-cos, pass-through-dscp to forbid the rewrite of L2 CoS priority and dscp value. At the egress, obtain L2 CoS priority and dscp value according to the final Int-Prio of the packets, decide whether rewrite L2 CoS priority and dscp value according to pass-through-cos, pass-through-dscp.

## 1.2  QoS Configuration Task List

Configure class map

> Set up a classification rule according to ACL, CoS, VLAN ID, IPv4 Precedent, DSCP, IPV6 FL to classify the data stream. Different classes of data streams will be processed with different policies.

Configure a policy map

> After data steam classification, a policy map can be created to associate with the class map created earlier and enter class mode. Then different policies (such as bandwidth limit, priority degrading assigning new DSCP value) can be applied to different data streams. You can also define a policy set that can be use in a policy map by several classes.

Apply QoS to the ports or the VLAN interfaces

> Configure the trust mode for ports or bind policies to ports. A policy will only take effect on a port when it is bound to that port.

> The policy may be bound to the specific VLAN.

> It is not recommended to synchronously use policy map on VLAN and its port, or else the policy map priority of the port is higher.

Configure queue management algorithm

> Configure queue management algorithm, such as sp, wdrr, and so on.

> Configure QoS mapping

> Configure the mapping from CoS to IntP, DSCP to IntP, IntP to DSCP, COS, IntP, DP or queue.

**1. Configure class map.**

| Command | Explanation |
|---|---|
| Global Mode | |
| **class-map <*class-map-name*>**<br>**no class-map <*class-map-name*>** | Create a class map and enter class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map. |
| **match {access-group <acl-index-or-name>**<br>**\| ip dscp <dscp-list>\| ip precedence <ip-precedence-list>\| ipv6 access-group <acl-index-or-name> \| ipv6 dscp <dscp-list>\| ipv6 flowlabel <flowlabel-list>\|vlan <vlan-list> \| cos <*cos-list*>\| vlan range <vlan-list>}** | Set matching criterion (classify data stream by ACL, CoS, VLAN ID, IPv4 Precedent, IPv6 FL or DSCP, etc) for the class map; the no command deletes specified matching criterion. |

| no match {access-group \| ip dscp \| ip precedence \| ipv6 access-group \| ipv6 dscp \| ipv6 flowlabel \| vlan \| cos\| vlan range} | |
|---|---|

**2. Configure a policy map**

| Command | Explanation |
|---|---|
| Global Mode | |
| **policy-map <*policy-map-name*>**<br>**no policy-map <*policy-map-name*>** | Create a policy map and enter policy map mode; the no command deletes the specified policy map. |
| **class <*class-map-name*> [insert-before <class-map-name>]**<br>**no class <*class-map-name*>** | After a policy map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data streams in class mode; the no command deletes the specified class. |
| **set internal priority <new-intp>**<br>**no set internal priority** | Assign a new internal priority for the classified traffic; the no command cancels the new assigned value. |
| **Single bucket mode:**<br>**policy <bits_per_second> <normal_burst_bytes> ({exceed-action ACTION} )**<br>**Dual bucket mode:**<br>**policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] \| <maximum_burst_bytes> [{exceed-action ACTION \| violate-action ACTION }]**<br>**ACTION definition:**<br>**drop \| transmit \| set-internal-priority <intp_value> \| policied-intp-transmit**<br>**no policy** | Configure a policy for the classified flow. The non-aggregation policy command supports three colors. Analyze the working mode of the token bucket, whether it is singe rate single bucket, single rate dual bucket, dual rate dual bucket, set corresponding action to different color packets. The no command will delete the mode configuration. |
| **policy aggregate <*aggregate-policy-name*>**<br>**no policy aggregate** | Apply a policy to classified traffic; the no command deletes the specified policy set. |
| **accounting** | Set statistic function for the classified |

| | |
|---|---|
| **no accounting** | traffic. After enable this function under the policy class map mode, add statistic function to the traffic of the policy class map. In single bucket mode, the messages can only red or green when passing policy. In the print information, there are two colors(green and red) of the packets. In dual bucket mode, there are three colors(green, red and yellow) of the packets. |
| Policy class map configuration mode | |
| **drop** <br><br> **no drop** <br><br><br> **transmit** <br><br> **no transmit** | Drop or transmit the traffic that match the class, the no command cancels the assigned action. |

### 3. Apply QoS to port or VLAN interface

| Command | Explanation |
|---|---|
| Interface Configuration Mode | |
| **mls qos trust {cos \| dscp}** <br> **no** mls **qos trust {cos \| dscp}** | Configure port trust; the no command disables the current trust status of the port. |
| **mls qos cos {<*default-cos*>}** <br> **no mls qos cos** | Configure the default CoS value of the port; the no command restores the default setting. |
| **mls qos internal-priority {<*default-intp*> }** <br> **no mls qos internal-priority** | Configure the default internal priority value of the port, the no command restores the default setting. |
| **service-policy input <*policy-map-name*>** <br> **no**          **service-policy**        **input** **{<*policy-map-name*>}** | Apply a policy map on the port, the no command deletes the specified policy map applied to the port or deletes all the policy maps applied on the ingress direction of the port . At present, the egress does not support the egress policy map. |
| **pass-through-cos** | Forbid the packet to rewrite L2 CoS |

| | |
|---|---|
| **no pass-through-cos** | value at the egress, the no command allows the packet to rewrite L2 CoS value. |
| **pass-through-dscp**<br>**no pass-through-dscp** | Forbid the packet to rewrite dscp value at the egress, the no command allows the packet to rewrite dscp value. |
| Global Mode | |
| **service-policy input** *<policy-map-name>* **vlan** *<vlan-list>*<br>**no service-policy input {***<policy-map-name>***} vlan** *<vlan-list>* | Apply a policy map to the specified VLAN interface; the no command deletes the specified policy map applied to the VLAN interface or deletes all the policy maps applied in the ingress direction of the vlan interface . |

**4. Configure queue management algorithm and weight**

| Command | Explanation |
|---|---|
| Port Configuration Mode | |
| **mls qos queue algorithm {sp | wdrr}**<br>**no mls qos queue algorithm** | Set queue management algorithm, the default queue management algorithm is wdrr. |
| **Global Mode** | |
| **mls qos queue wdrr weight <weight0..weight7>**<br>**no mls qos queue wdrr weight** | Set wdrr queue weight for all ports globally, the default queue weight is 1 1 1 1 1 1 1 1. |

**5. Configure QoS mapping**

| Command | Explanation |
|---|---|
| Global Mode | |
| **mls qos map {cos-intp <intp1…intp8> | dscp-intp <in-dscp list> to <intp> | intp-cos <intp list> to <out-cos> | intp-dp <intp list> to <out-dp> | intp-dscp <intp list> to <out-dscp>| intp-intp <color> <intp list> to <intp> | intp-queue <intp list> to <out-queue> }**<br>**no mls qos map {cos-intp | dscp-intp |** | Set the priority mapping for QoS, the no command restores the default mapping value. |

| | |
|---|---|
| **intp-cos | intp-dp | intp-dscp | intp-intp \<color> | intp-queue}** | |

**6. Clear accounting data of the specific ports or VLANs**

| Command | Explanation |
|---|---|
| Admin Mode | |
| **clear mls qos statistics [interface \<interface-name> | vlan \<vlan-id>]** | Clear accounting data of the specified ports or VLAN Policy Map. If there are no parameters, clear accounting data of all policy map. |

**7. Show configuration of QoS**

| Command | Explanation |
|---|---|
| Admin Mode | |
| **show mls qos maps [cos-intp | dscp-intp | intp-intp | intp-cos | intp-dscp | intp-dp | intp-queue]** | Display the configuration of QoS mapping. |
| **show class-map [\<class-map-name>]** | Display the classified map information of QoS. |
| **show policy-map [\<policy-map-name>]** | Display the policy map information of QoS. |
| **show mls qos aggregate-policy [\<aggregate-policy-name>]** | Display the aggregate policy configuration of QoS. |
| **show mls qos interface [\<interface-id>] [policy | queuing]** | Display QoS configuration information on a port. |
| **show mls qos vlan \<v-id>** | Display QoS configuration on VLAN interface. |

# 1.3  QoS Example

Example 1:

Enable QoS function, change the global queue out weight to 1:1:2:2:4:4:8:8, set port ethernet 1/0/1 in trust CoS mode without changing DSCP value, and set the default CoS value of the port to 5.

The configuration steps are listed below:

Switch#config

Switch(config)# mls qos queue weight 1 1 2 2 4 4 8 8

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet 1/0/1)#mls qos trust cos

Switch(Config-If-Ethernet 1/0/1)#pass-through-dscp

Switch(Config-If-Ethernet1/0/1)#mls qos cos 5


Configuration result:

When QoS enabled in Global Mode, the egress queue bandwidth proportion of each port is 1:1:2:2:4:4:8:8. When packets have CoS value coming in through port ethernet1/0/1, it will be map to the internal priority according to the CoS value, CoS value 0 to 7 correspond to queue out 1, 2, 3, 4, 5, 6, 7, 8 respectively. If the incoming packet has no CoS value, it is default to 5 and will be put in queue6. All passing packets would not have their DSCP values changed


Example 2:

In port ethernet1/0/2, set the bandwidth for packets from segment 192.168.1.0 to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting will be dropped.


The configuration steps are listed below:

Switch#config

Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Switch(config)#class-map c1

Switch(Config-ClassMap-c1)#match access-group 1

Switch(Config-ClassMap-c1)#exit

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#policy 10000 4000 exceed-action drop

Switch(Config-PolicyMap-p1-Class-c1)#exit

Switch(Config-PolicyMap-p1)#exit

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#service-policy input p1


Configuration result:

An ACL name 1 is set to matching segment 192.168.1.0. Enable QoS globally, create a class map named c1, matching ACL1 in class map; create another policy map named p1 and refer to c1 in p1, set appropriate policies to limit bandwidth and burst value. Apply this policy map on port ethernet1/0/2. After the above settings done, bandwidth for packets from segment 192.168.1.0 through port ethernet 1/0/2 is set to 10 Mb/s, with a burst value

of 4 MB, all packets exceed this bandwidth setting in that segment will be dropped.

Example 3:
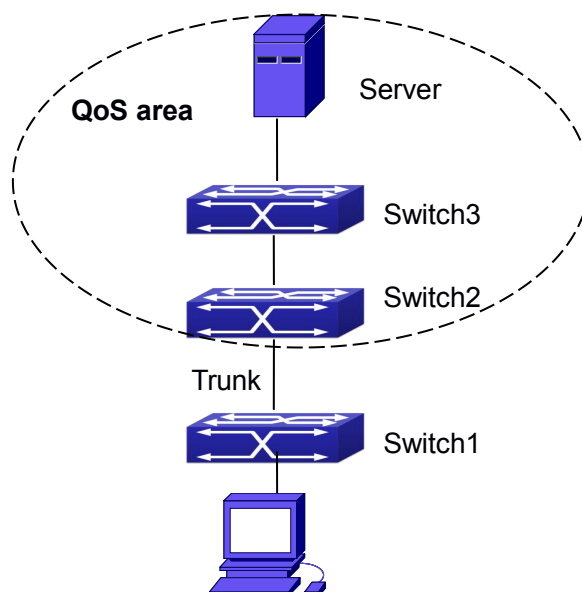


Fig 1-  7 Typical QoS topology

As shown in the figure, inside the block is a QoS domain, Switch1 classifies different traffics and assigns different IP precedences. For example, set CoS precedence for packets from segment 192.168.1.0 to 5 on port ethernet1/0/1(set the internal priority to 40, set the default intp-dscp mapping to 40-40, the corresponding IP precedence to 5). The port connecting to switch2 is a trunk port. In Switch2, set port ethernet 1/0/1 that connecting to swtich1 to trust dscp. Thus inside the QoS domain, packets of different priorities will go to different queues and get different bandwidth.

The configuration steps are listed below:

**QoS configuration in Switch1:**

Switch#config

Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Switch(config)#class-map c1

Switch(Config-ClassMap-c1)#match access-group 1

Switch(Config-ClassMap-c1)#exit

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 40

Switch(Config-PolicyMap-p1-Class-c1)#exit

Switch(Config-PolicyMap-p1)#exit

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#service-policy input p1


QoS configuration in Switch2:

Switch#config

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#mls qos trust dscp


# 1.4  QoS Troubleshooting


- trust cos and EXP can be used with other trust or Policy Map.
- trust dscp can be used with other trust or Policy Map. This configuration takes effect to IPv4 and IPv6 packets.
- trust exp, trust dscp and trust cos may be configured at the same time, the priority is: EXP>DSCP>COS.
- If the dynamic VLAN (mac vlan/voice vlan/ip subnet vlan/protocol vlan) is configured, then the packet COS value equals COS value of the dynamic VLAN.
- At present, it is not recommended to synchronously use policy map on VLAN and VLAN's port.

# Chapter 2 Flow-based Redirection

## 2.1 Introduction to Flow-based Redirection

Flow-based redirection function enables the switch to transmit the data frames meeting some special condition (specified by ACL) to another specified port. The fames meeting a same special condition are called a class of flow, the ingress port of the data frame is called the source port of redirection, and the specified egress port is called the destination port of redirection. Usually there are two kinds of application of flow-based redirection: 1. connecting a protocol analyzer (for example, Sniffer) or a RMON monitor to the destination port of redirection, to monitor and manage the network, and diagnose the problems in the network; 2. Special transmission policy for a special type of data frames.

The switch can only designate a single destination port of redirection for a same class of flow within a source port of redirection, while it can designate different destination ports of redirection for different classes of flows within a source port of redirection. The same class of flow can be applied to different source ports.

## 2.2 Flow-based Redirection Configuration Task Sequence

1. Flow-based redirection configuration
2. Check the current flow-based redirection configuration
3. Configure the vlan redirection function of the port
4. Configure the maximum number of vlan of redirect on each port

**1. Flow-based redirection configuration**

| Command | Explanation |
|---|---|
| Physical Interface Configuration Mode | |
| **access-group *<aclname>* redirect to interface [ethernet *<IFNAME>*|*<IFNAME>*]** <br> **no access-group *<aclname>* redirect** | Specify flow-based redirection for the port; the "**no access-group *<aclname>* redirect**" command is used to delete flow-based redirection. |

1

**2. Check the current flow-based redirection configuration**

| Command | Explanation |
|---|---|
| Global Mode/Admin Mode | |
| **show flow-based-redirect {interface [ethernet <IFNAME> |<IFNAME>]}** | Display the information of current flow-based redirection in the system/port. |

**3. Configure the vlan redirection function of the port**

| Command | Explanation |
|---|---|
| Port Mode | |
| **match vlan <1-4096> redirect interface (ethernet|) IFNAME** <br> **no match vlan <1-4096> redirect** | Configure the vlan redirection function of the port. |
| **port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME** <br> **no port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME** | Configure the vlan redirection function of the port. |

**4. Configure the maximum number of vlan of redirect on each port**

| Command | Explanation |
|---|---|
| Global Mode | |
| **vlan-port-redirect vlan maximum <1-1000>** <br> **no vlan-port-redirect vlan maximum** | Configure the maximum number of vlan of redirect on each port. |

## 2.3 Flow-based Redirection Examples

**Example:**

User's request of configuration is listed as follows: redirecting the frames whose source IP is 192.168.1.111 received from port 1 to port 6, that is sending the frames whose source IP is 192.168.1.111 received from port 1 through port6.

**Modification of configuration:**

1: Set an ACL, the condition to be matched is: source IP is 192.168.1.111;

2: Apply the redirection based on this flow to port 1.

**The following is the configuration procedure:**

Switch(config)#access-list 1 permit host 192.168.1.111

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)# access-group 1 redirect to interface ethernet 1/0/6

# 2.4  Flow-based Redirection Troubleshooting Help

When the configuration of flow-based redirection fails, please check that whether it is the following reasons causing the problem:

- The type of flow (ACL) can only be digital standard IP ACL, digital extensive IP ACL, nomenclature standard IP ACL, nomenclature extensive IP ACL, digital standard IPv6 ACL, and nomenclature standard IPv6 ACL;

- Parameters of **Timerange** and **Portrange** can not be set in ACL, the type of ACL should be Permit.

- The redirection port must be 1000Mb port in the flow-based redirection function.

- Do not implement the forward across VLAN for flow-based redirection.

# Chapter 3 Egress QoS Configuration

## 3.1 Introduction to Egress QoS

In traditional IP networks, all packets are treated in the same way. All network equipments treat them by the first-in-first-out policy and try best effort to send them to the destination. However, it does not guarantee the performance like reliability and transmission delay. Network develops so fast that new demand has been raised for the quality of service on IP network with the continual emergence of new applications. For example, delay-sensitive services like VoIP and video put higher demands on packet transmission delay and users cannot accept too long transmission delay (by contrast, E-mail and FTP services are not sensitive to the time delay). In order to support services with different service requirement like voice, video and data service, the network is required to be able to distinguish between different communications and provide appropriate service. The traditional best-effort IP network cannot identify and distinguish various kinds of communications while this ability is the very premise of providing differentiated services for different communications. Therefore, the best-effort service mode of traditional network cannot meet the demand of applications. The emergence of QoS techniques is committed to solve this problem.

Egress PolicyMap is the QoS policy in egress which performs QoS control of packets in the egress direction and provides better service for specified network communication with kinds of techniques. Egress PolicyMap includes class-map and policy-map, of which class-map is used for selecting packets to operate and policy-map is used for specifying the operation to use. Not all equipments support Egress QoS currently.
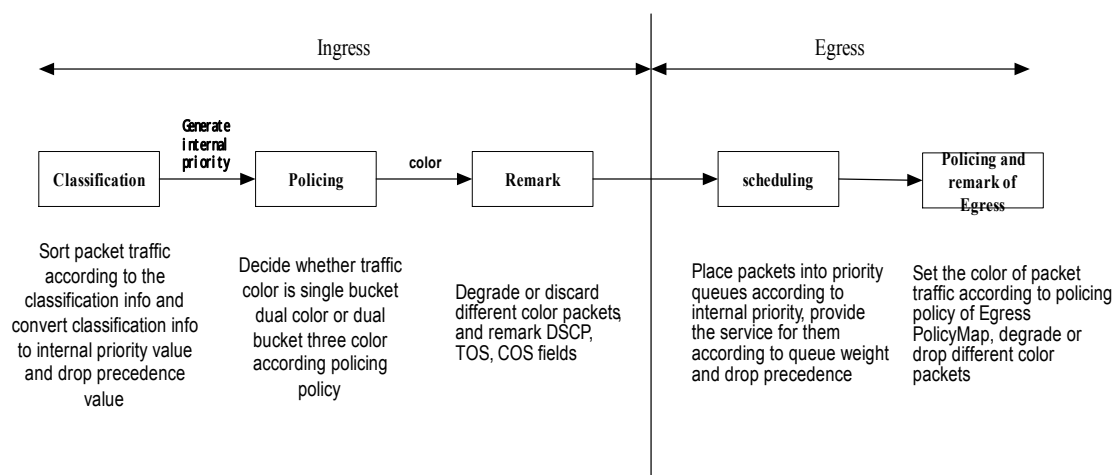
### 3.1.1 Egress QOS Terms

**Egress QoS:** Achieving QoS on egress of port.
**Inner_vid:** VLAN ID brought by the TAG near the header of network layer when double TAGs exist.
**Outer_vid:** VLAN ID brought by the TAG near the header of network link layer when double TAGs exist. The TAG is considered to be outer tag by default when only one TAG exists.
**Outer_tpid:** Protocol type of the network link layer header indicating the type of outer tag.

### 3.1.2 Basic Egress QoS Model

| Ingress | | | Egress | |
|---|---|---|---|---|
| Classification | Policing | Remark | scheduling | Policing and remark of Egress |
| Sort packet traffic according to the classification info and convert classification info to internal priority value and drop precedence value | Decide whether traffic color is single bucket dual color or dual bucket three color according policing policy | Degrade or discard different color packets and remark DSCP, TOS, COS fields | Place packets into priority queues according to internal priority, provide the service for them according to queue weight and drop precedence | Set the color of packet traffic according to policing policy of Egress PolicyMap, degrade or drop different color packets |

According to the characters (including field values like COS and DSCP) of upstream packets, policing and rewriting of Egress make the last QoS change on the packet prior to the packet egress.

Policing configures different policing policy based on the flow and distributes bandwidth for the flow classified. The distribution policy of bandwidth can be either dual bucket dual color or dual bucket three color. Different colors can be assigned to different flows and approaches of discard or passage can be chosen for them; you can add rewriting action for packets with passage approach chosen. See the following flow chart for detailed description of Egress QoS:
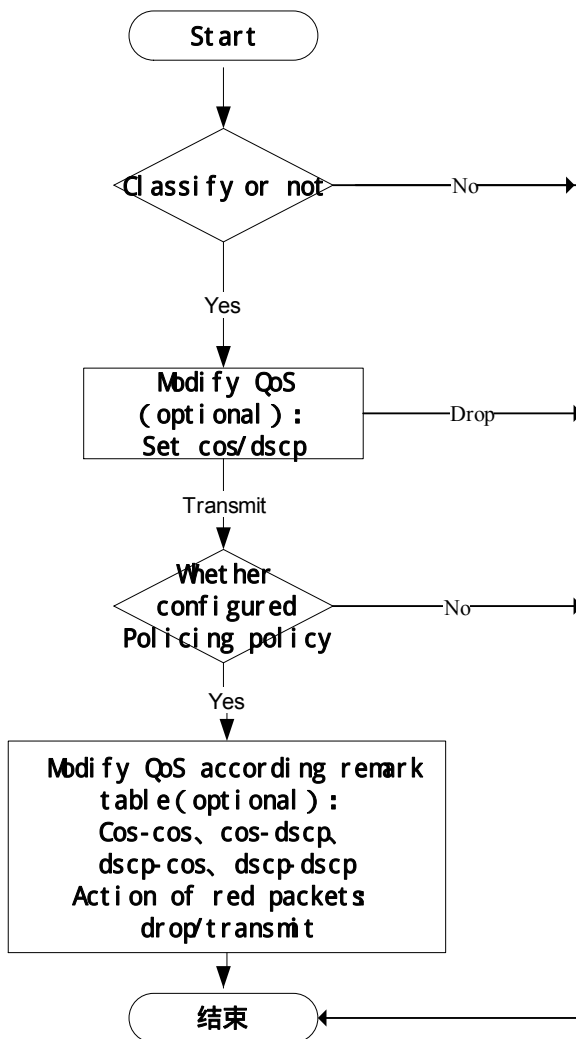
Description of action that modify QoS attribute according to egress remark table:

cos-cos：for cos value of packets, modify cos value of packets according to cos table of

QoS remarking

cos-dscp：for cos value of packets, modify dscp value of packets according to cos table of

QoS remarking

dscp-cos：for dscp value of packets, modify cos value of packets according to dscp table

of QoS remarking

dscp-dscp：for dscp value of packets, modify dscp value of packets according to dscp

table of QoS remarking

# 3.2 Egress QoS Configuration

Egress QoS Configuration Task List:

Configure class map

Set up a classification rule according to ACL, CoS, VLAN ID, IPv4 Precedent, DSCP, IPV6 DSCP to classify the data stream. Different classes of data streams will be processed with different policies.

Configure policy map

After data steam classification, a policy map can be created to associate with a class map created earlier and enter policy class mode. Then different policies (such as bandwidth limit, assigning new DSCP value) can be applied to different data streams.

Apply Egress QoS to port or VLAN

Configure the trust mode or binding policies for ports. A policy will only take effect on a port when it is bound to that port.

The policy may be bound to the specific VLAN.

Set Egress QoS remark mapping

If modify QoS attribute by using Egress QoS remark in policy, it should set the corresponding mapping. If it needs to take effect to green packets, modifying switch of green packets should be enabled and ingress needs to trust the corresponding QoS attribute (qos/dscp/exp).

## 1. Configure a class-map

| Command | Explanation |
|---|---|
| Global Mode | |
| **class-map <*class-map-name*>** <br> **no class-map <*class-map-name*>** | Create a class-map and enter class-map mode, no command deletes the specified class-map. |
| **match {access-group <*acl-index-or-name*> \| ip dscp <*dscp-list*> \| ip precedence <*ip-precedence-list*> \| ipv6 dscp <*dscp-list*> \| vlan <*vlan-list*> \| cos <*cos-list*> \| ipv6 access-group <*acl-index-or-name*>}** <br> **no match {access-group \| ip dscp \| ip precedence \| ipv6 dscp \| vlan \| cos \| ipv6 access-group}** | Configure the matched standard of the class map to classify the data stream according to ACL, CoS, VLAN ID, IPv4 Precedence, DSCP, IPv6 DSCP priority; no command deletes the specific matched standard. |

## 2. Configure a policy-map

| Command | Explanation |
|---|---|
| Global Mode | |

| | |
|---|---|
| **policy-map <*policy-map-name*>** <br> **no policy-map <*policy-map-name*>** | Create a policy-map and enter policy-map mode, no command deletes the specific policy-map. |
| **class <*class-map-name*>** **[insert-before <*class-map-name*>]** **no class <*class-map-name*>** | Create a policy map to associate with a class map and enter policy class map mode, then different data streams can apply different policies and be assigned a new DSCP value. No command deletes the specified policy class map. |
| **set {ip dscp <*new-dscp*> \| ip precedence <*new-precedence*> \| cos <*new-cos*> \| c-vid <*new-c-vid*> \| s-vid <*new-s-vid*> \| s-tpid <*new-s-tpid*>}** **no set {ip dscp \| ip precedence \| cos \| c-vid \| s-vid \| s-tpid}** | Assign a new DSCP, CoS and IP Precedence value for the classified flow, no command cancels the operation. |
| **Single bucket mode:** <br> **policy <*bits_per_second*> <*normal_burst_bytes*> ({action ACTION} \| exceed-action drop \| transmit})** <br><br> **Dual bucket mode:** <br> **policy <*bits_per_second*> <*normal_burst_bytes*> [pir <*peak_rate_bps*>] \| <*maximum_burst_bytes*> [{action ACTION \| violate-action drop \| transmit}]** <br><br> **ACTION definition:** <br> **policied-cos-to-cos-transmit \|** <br> **policied-cos-to-dscp-transmit \|** <br> **policied-dscp-exp-to-cos-transmit \|** <br> **policied-dscp-exp-to-dscp-transmit** <br> **no policy** | Configure a policy for the classified flow. The non-aggregation policy command supports three colors. Analyze the working mode of the token bucket, whether it is single rate single bucket, single rate dual bucket or dual rate dual bucket, set corresponding action to different color packets. The no command will delete the configuration. Only specific switch supports single bucket mode. |
| **accounting** <br> **no accounting** | Set statistic function for the classified flow. After enable this function under the policy class map mode, add statistic |

| | function to the flow of the policy class map. In single bucket mode, packets can only red or green when passing policy. In the print information, in-profile means green and out-profile means red. In dual bucket mode, there are three colors of packets in-profile means green and out-profile means red and yellow. |
|---|---|

### 3. Apply policy to port or VLAN

| Command | Explanation |
|---|---|
| Interface Mode | |
| **service-policy output <policy-map-name>** <br> **no service-policy output {<policy-map-name>}** | Apply a policy map to the egress of the port; the no command deletes the specified policy map applied to the port or deletes all the policy maps applied on the egress direction of the port . |
| Global Mode | |
| **service-policy output <policy-map-name> vlan <vlan-list>** <br> **no service-policy output {<policy-map-name>} vlan <vlan-list>** | Apply a policy map to the egress of the VLAN; the no command deletes the specified policy map applied to the VLAN interfaceor deletes all the policy maps applied in the egress direction of the vlan interface . |

### 4．Set Egress QoS remark mapping

| Command | Explanation |
|---|---|
| Global Mode | |
| **mls qos map {cos-cos | cos-dscp} {green | yellow | red} <value1> <value2>···<value8>** <br> **no mls qos map {cos-cos | cos-dscp} {green | yellow | red}** | Set Egress cos mapping, no command resotores the default configuration. |
| **mls qos map {dscp-cos | dscp-dscp} {green | yellow | red} <dscp list> to <value>** <br> **no mls qos map {dscp-cos | dscp-dscp} {green | yellow | red}** | Set Egress dscp mapping, <dscp-list> means 1 to 8 dscp values, no command restores the default configuration. |

| mls qos egress green remark<br><br>no mls qos egress green remark | Set Egress QoS remark mapping to take effect for green packets, no command does not take effect to green packets. |
|---|---|

**5. Clear accounting data of the specific ports or VLANs**

| Command | Explanation |
|---|---|
| Admin Mode | |
| **clear mls qos statistics [interface <interface-name> | vlan <vlan-id>]** | Clear accounting data of the specified ports or VLAN Policy Map. If there are no parameters, clear accounting data of all policy map. |

**6. Show QoS configuration**

| Command | Explanation |
|---|---|
| Admin Mode | |
| **show mls qos {interface [<*interface-id*>] [policy | queuing] | vlan <*vlan-id*>}** | Show QoS configuration of the port. |
| **show class-map [<*class-map-name*>]** | Show the class map information of QoS. |
| **show policy-map [<*policy-map-name*>]** | Show the policy map information of QoS. |
| **show mls qos maps {cos-cos | cos-dscp | dscp-cos | dscp-exp} {green | yellow | red |}** | Show mapping relation of Egress QoS remark. |

# 3.3  Egress QoS Examples

Example1:

On the egress of the port1, change cos value as 4 for the packet with dscp value of 0.

Create a class map:

switch(config)#class-map 1

switch(config-classmap-1)#match ip dscp 0

switch(config-classmap-1)#exit

Create a policy map:

switch(config)#policy-map 1

switch(config-policymap-1)#class 1

switch(config-policymap-1-class-1)#set cos 4

switch(config-policymap-1-class-1)#exit

switch(config-policymap-1)#exit


Bind a policy to the port:

switch(config)#in e 1/0/1

switch(config-if-ethernet1/0/1)#service-policy output 1


Example2:

On the egress of vlan10, change cos value as 4 for the packet with ipv6 dscp value of

7.

Create a class map:

switch(config)#class-map 1

switch(config-classmap-1)#match ipv6 dscp 7

switch(config-classmap-1)#exit


Create a policy map:

switch(config)#policy-map 1

switch(config-policymap-1)#class 1

switch(config-policymap-1-class-1)#set cos 4

switch(config-policymap-1-class-1)#exit

switch(config-policymap-1)#exit


Bind a policy to VLAN

switch(config)#service-policy output 1 vlan 10


Example 3:

In egress of port 1, limit the speed of packets. Set the bandwidth for packets to 1 Mb/s,

with the normal burst value of 1 MB, the max burst value of 4 MB, set dscp value of 1 as

10 for green packets, set dscp value of yellow packets as 9 and drop red packets.

Create a class map

switch(config)#class-map c1

switch(config-classmap-c1)#match ip dscp 1

switch(config-classmap-c1)#exit

Create a policy map

switch(config)#policy-map p1

switch(config-policymap-p1)#class c1

switch(config-policymap-p1-class-c1)#policy          1000       1000       4000          action policied-dscp-exp-to-dscp-transmit violate-action drop

switch(config-policymap-p1-class-c1)#exit

switch(config-policymap-p1)#exit

Set Egress dscp remark mapping

switch(config)#mls qos map dscp-dscp green 1 to 10

switch(config)#mls qos map dscp-dscp yellow 1 to 9

Set Egress remark to take effect for green packets

switch(config)#mls qos egress green remark

Set trust dscp mode on ingress

switch(config-if-port-range)#mls qos trust dscp

Bind policy to egress of port1

switch(config-if-ethernet1/0/1)#service-policy output p1

# 3.4 Egress QoS Troubleshooting Help

- ⚭  Not all equipments support Egress QoS presently, so please make sure the current device supports this function.

- ⚭  If the policy configured cannot bind to the port or VLAN, please check whether the match option in classification table is supported by the current device.

- ⚭  If terminal printing suggests lack of resource, please make sure there is enough resource to send the current policy.

- ⚭  If the policy with match acl configured cannot bind to the port or VLAN, please make sure rules including permit exist in ACL.

- ⚭  If modifying QoS attribute is invalid by Egress QoS remark, please ensure whether ingress sets the correspondsing QoS attribute with trust.

- ⚭  If egress set QoS attributes (set cos/ip dscp) for modifying all packets, and it uses Egress remark to modify QoS attributes for packets of different colors, previous modification is preferential for modifying packets.

# Chapter 4 Flexible QinQ Configuration

## 4.1 Introduction to Flexible QinQ

### 4.1.1 QinQ Technique

Dot1q-tunnel is also called QinQ (802.1Q-in-802.1Q), which is an expansion of 802.1Q. Its dominating idea is encapsulating the customer VLAN tag (CVLAN tag) to the service provider VLAN tag (SPVLAN tag). The packet with two VLAN tags is transmitted through the backbone network of the ISP internet to provide a simple layer-2 tunnel for the users. It is simple and easy to manage, applicable only by static configuration, and especially adaptive to small office network or small metropolitan area network using layer-3 switch as backbone equipment.

There are two kinds of QinQ: basic QinQ and flexible QinQ, the priority of flexible QinQ is higher than basic QinQ.

### 4.1.2 Basic QinQ

Basic QinQ based the port. After a port configures QinQ, whether the received packet with tag or not, the device still packs the default VLAN tag for the packet. Using basic QinQ is simple, but the setting method of VLAN tag is inflexible.

### 4.1.3 Flexible QinQ

Flexible QinQ based data flow. It selects whether pack the external tag and packs what kind of the external tag by matching the material flow. For example: implement the property of flexible QinQ according to the user's VLAN tag, MAC address, IPv4/IPv6 address, IPv4/IPv6 protocol and the port ID of the application, etc. So, it can encapsulate the external tag for the packet and implements different scheme by different users or methods.

## 4.2 Flexible QinQ Configuration Task List

The match of flexible QinQ data flow uses policy-map rule of QoS to be sent, the configuration task list is as follows:
1. Create class-map to classify different data flows

2. Create flexible QinQ policy-map to relate with the class-map and set the corresponding operation

3. Bind flexible QinQ policy-map to port

**1. Configure class map**

| Command | Explanation |
|---|---|
| Global mode | |
| **class-map <*class-map-name*>**<br>**no class-map <*class-map-name*>** | Create a class-map and enter class-map mode, the no command deletes the specified class-map. |
| **match {access-group <*acl-index-or-name*> \| ip dscp <*dscp-list*>\| ip precedence <*ip-precedence-list*>\| ipv6 access-group <*acl-index-or-name*>\| ipv6 dscp <*dscp-list*> \| ipv6 flowlabel <flowlabel-list> \| vlan <vlan-list> \| cos <*cos-list*>}**<br>**no match {access-group \| ip dscp \| ip precedence\|ipv6 access-group\| ipv6 dscp \| ipv6 flowlabel \| vlan \| cos}** | Set the match standard of class-map, (classify data flow by ACL, CoS, VLAN ID, IPv4 Precedent or DSCP, etc for the class map); the no command deletes the specified match standard. |

**2. Configure policy-map of flexible QinQ**

| Command | Explanation |
|---|---|
| Global mode | |
| **policy-map <*policy-map-name*>**<br>**no policy-map <*policy-map-name*>** | Create a policy-map and enter policy-map mode, the no command deletes the specified policy-map. |
| **class <*class-map-name*> [insert-before <class-map-name>]**<br>**no class <*class-map-name*>** | After a policy-map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data flows in class mode; the no command deletes the specified class-map. |
| **set s-vid < vid>**<br>**no set s-vid** | Set external VLAN Tag for the classified traffic, no command cancels the operation. |
| **add s-vid <vid>**<br>**no add s-vid <vid>** | Add external VLAN Tag for the classified traffic, no command cancels the operation. |

**3. Bind flexible QinQ policy-map to port**

| Command | Explanation |
|---|---|
| Port mode | |
| **service-policy input<*policy-map-name*>**<br>**no service-policy input<*policy-map-name*>** | Apply a policy-map to a port, the no command deletes the specified policy-map applied to the port. |
| Global mode | |
| **service-policy input<*policy-map-name*> vlan<*vid*>**<br>**no service-policy input<*policy-map-name*> vlan <*vid*>** | Apply a policy-map to a VLAN, the no command deletes the specified policy-map applied to the VLAN. |

**4. Show flexible QinQ policy-map bound to port**

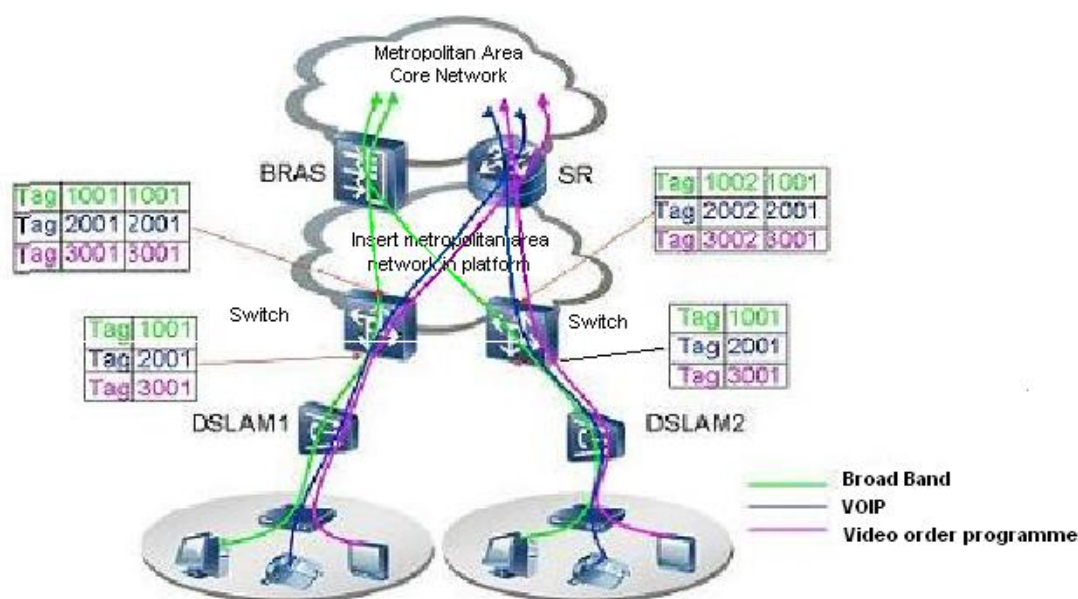| Command | Explanation |
|---|---|
| Admin mode | |
| **show mls qos {interface [<interface-id>]** | Show flexible QinQ configuration on the port. |

# 4.3  Flexible QinQ Example



Fig 4-  1 Flexible QinQ application topology

As shown in the figure, the first user is assigned three VLANs that the tag values are 1001, 2001, 3001 respectively in DSLAM1. VLAN1001 corresponds to Broad Band Network, VLAN2001 corresponds to VOIP, VLAN3001 corresponds to VOD. After the downlink port enables flexible QinQ function, the packets will be packed with different external tags according to VLAN ID of users. The packet with tag 1001 will be packed an external tag 1001 directly(This tag is unique in public network), enter Broad Band Network-VLAN1001 and classfied to BRAS device. The packet with tag 2001(or 3001) will be packed an external tag 2001(or 3001) and classfied to SR device according to the flow rules. The second user can be assigned different VLAN tags for different VLANs in DSLAM2. Notice: The assigned VLAN tag of the second user may be same with the first user and the packet with tag will be also packed an external tag. In the above figure, the external tag of the second user is different to the first user for distinguishing DSLAM location and locating the user finally.

The configuration in the following:

If the data flow of DSLAM1 enters the switch's downlink port1, the configuration is as follows:

Switch(config)#class-map c1

Switch(config-classmap-c1)#match vlan 1001

Switch(config-classmap-c1)#exit

Switch(config)#class-map c2

Switch(config-classmap-c2)#match vlan 2001

Switch(config-classmap-c2)#exit

Switch(config)#class-map c3

Switch(config-classmap-c3)#match vlan 3001

Switch(config-classmap-c3)#exit

Switch(config)#policy-map p1

Switch(config-policymap-p1)#class c1

Switch(config-policymap-p1-class-c1)# set s-vid 1001

Switch(config-policymap-p1)#class c2

Switch(config-policymap-p1-class-c2)# set s-vid 2001

Switch(config-policymap-p1)#class c3

Switch(config-policymap-p1-class-c3)# set s-vid 3001

Switch(config-policymap-p1-class-c3)#exit

Switch(config-policymap-p1)#exit

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#service-policy input p1

If the data flow of DSLAM2 enters the switch's downlink port1, the configuration is as follows:

Switch(config)#class-map c1

Switch(config-classmap-c1)#match vlan 1001

Switch(config-classmap-c1)#exit

Switch(config)#class-map c2

Switch(config-classmap-c2)#match vlan 2001

Switch(config-classmap-c2)#exit

Switch(config)#class-map c3

Switch(config-classmap-c3)#match vlan 3001

Switch(config-classmap-c3)#exit

Switch(config)#policy-map p1

Switch(config-policymap-p1)#class c1

Switch(config-policymap-p1-class-c1)# set s-vid 1002

Switch(config-policymap-p1)#class c2

Switch(config-policymap-p1-class-c2)# set s-vid 2002

Switch(config-policymap-p1)#class c3

Switch(config-policymap-p1-class-c3)# set s-vid 3002

Switch(config-policymap-p1-class-c3)#exit

Switch(config-policymap-p1)#exit

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)# service-policy input p1

# 4.4  Flexible QinQ Troubleshooting

If flexible QinQ policy can not be bound to the port, please check whether the problem is caused by the following reasons:

- Make sure flexible QinQ whether supports the configured class-map and policy-map
- Make sure ACL includes permit rule if the class-map matches ACL rule
- Make sure the switch exists enough TCAM resource to send the binding
- Priority of flexible QinQ and vlan ingress filtering for processing packets is: flexible QinQ > vlan ingress filtering