QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

QoS and Flow-based Redirection Configuration

Оглавление

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.

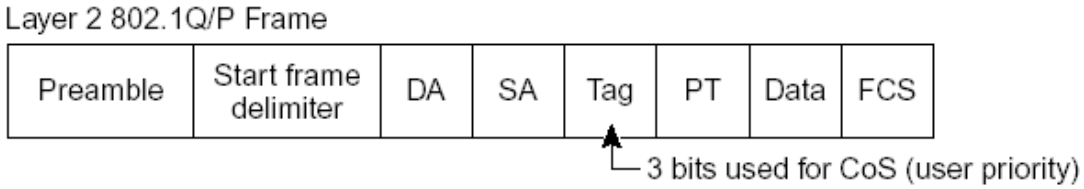

Fig 1-1 CoS priority

- **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.

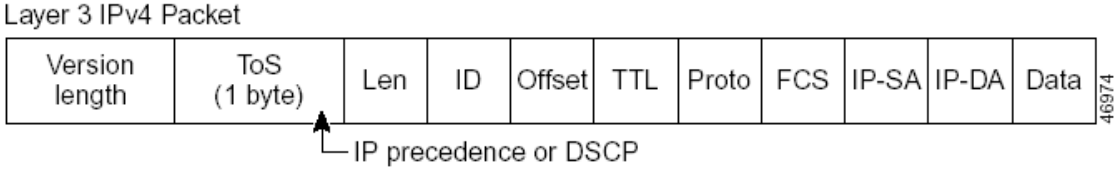

Fig 1-2 ToS priority

- **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.
- **MPLS TC*(EXP)*:**

A field of the MPLS packets means the service class, there are 3 bits, the ranging from 0 to 7.

- **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 0-2 in three color algorithm, the ranging is 0-1 in dual color algorithm. 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. Configure the weight for eight egress queues WRR (Weighted Round Robin).
- **In-Profile:** Traffic within the QoS policing policy range (bandwidth or burst value) is called In-Profile.
- **Out-of-Profile:** Traffic out the QoS policing policy range (bandwidth or burst value) is called Out-of-Profile.

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.

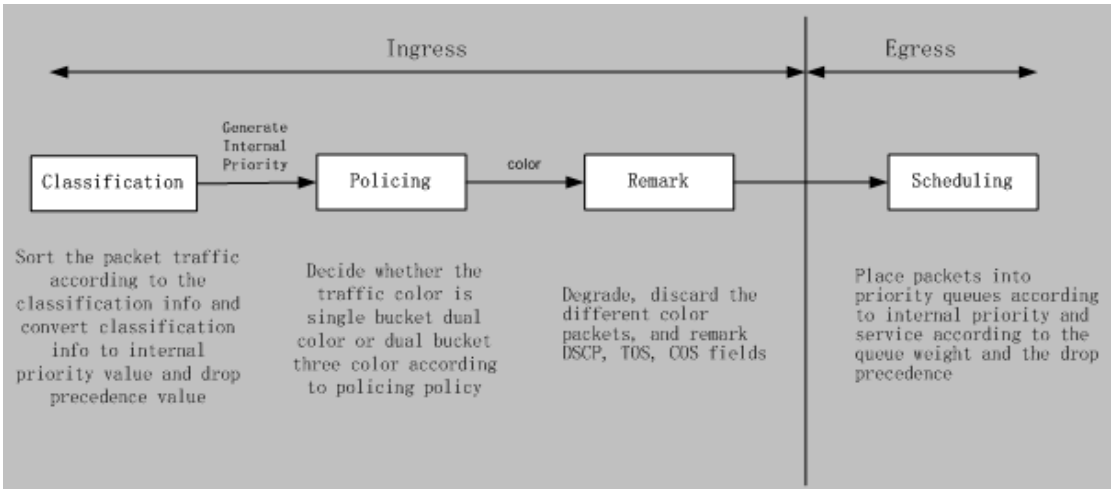

Fig 1-3 Basic QoS Model

Classification: Classify traffic according to packet classification information and generate internal priority and drop precedence based the classification information. For different packet types and switch configurations, classification is performed differently; the flowchart below explains this in detail.

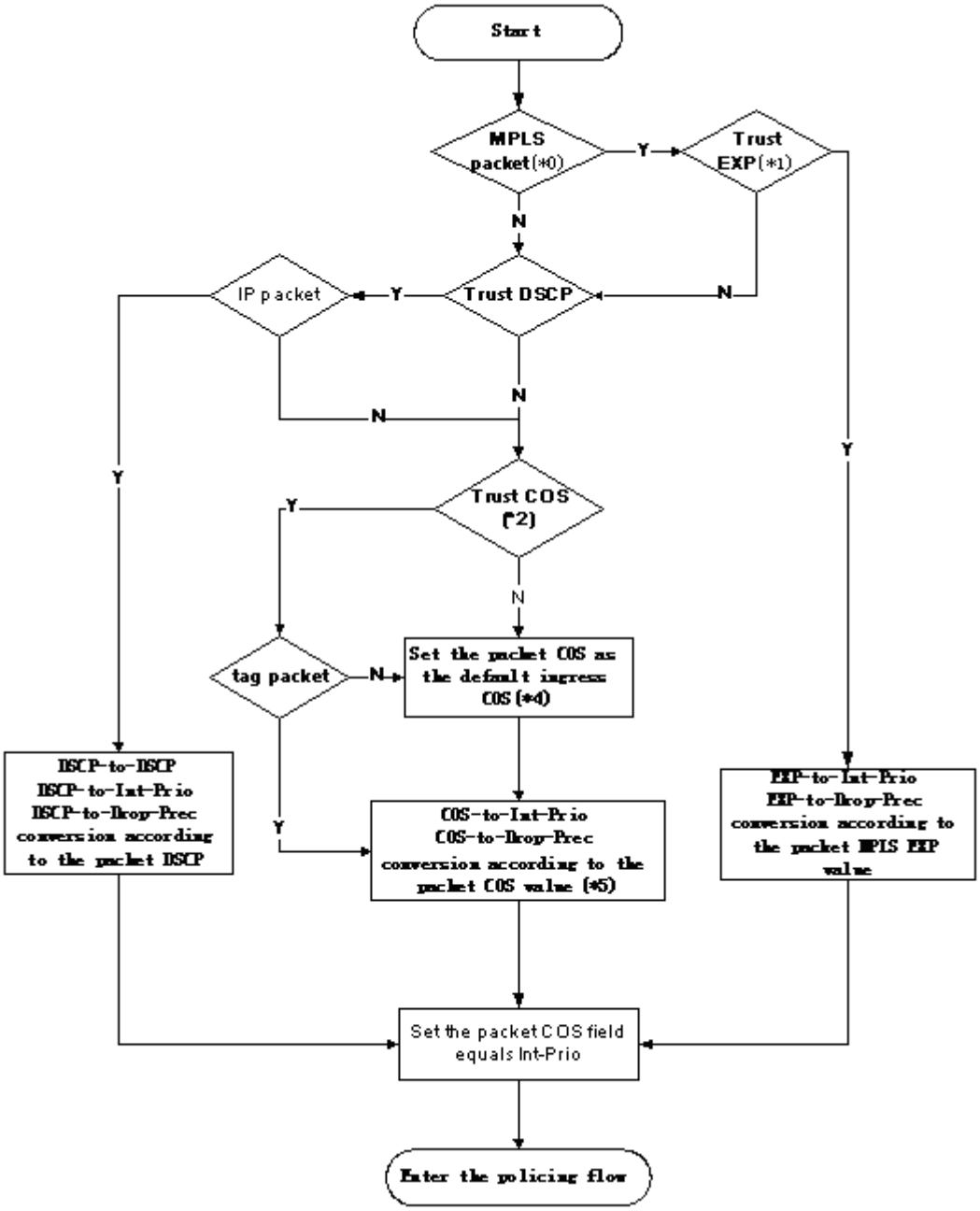

Fig 1-4 Classification process

Policing and remark: Each packet in classified ingress traffic is assigned an internal priority value and a drop precedence 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 dual 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 DSCP value of

lower priority to replace the original higher level DSCP value in the packet. The following flowchart describes the operations.

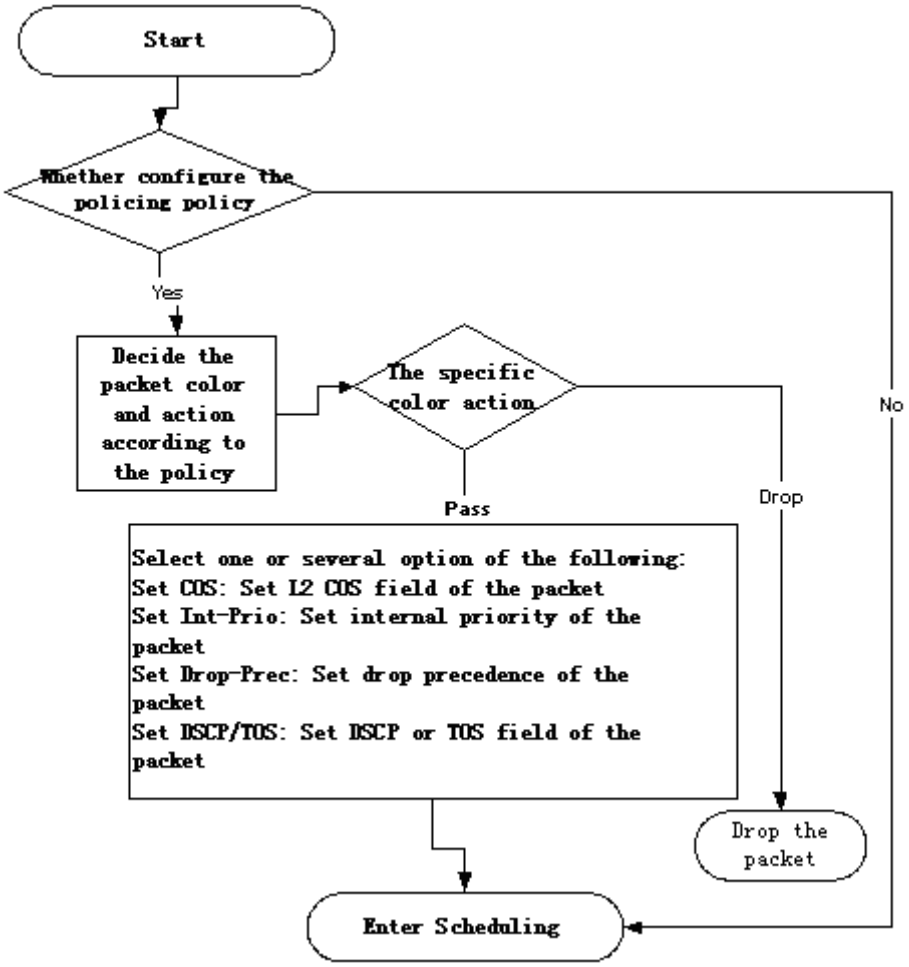

Fig 1-5 Policing and Remarking process

Queuing and scheduling: There are the internal priority and the drop precedence for the egress packets, the queuing operation assigns the packets to different priority queues according to the internal priority, while the scheduling operation perform the packet forwarding according to the priority queue weight and the drop precedence. The following flowchart describes the operations during queuing and scheduling.

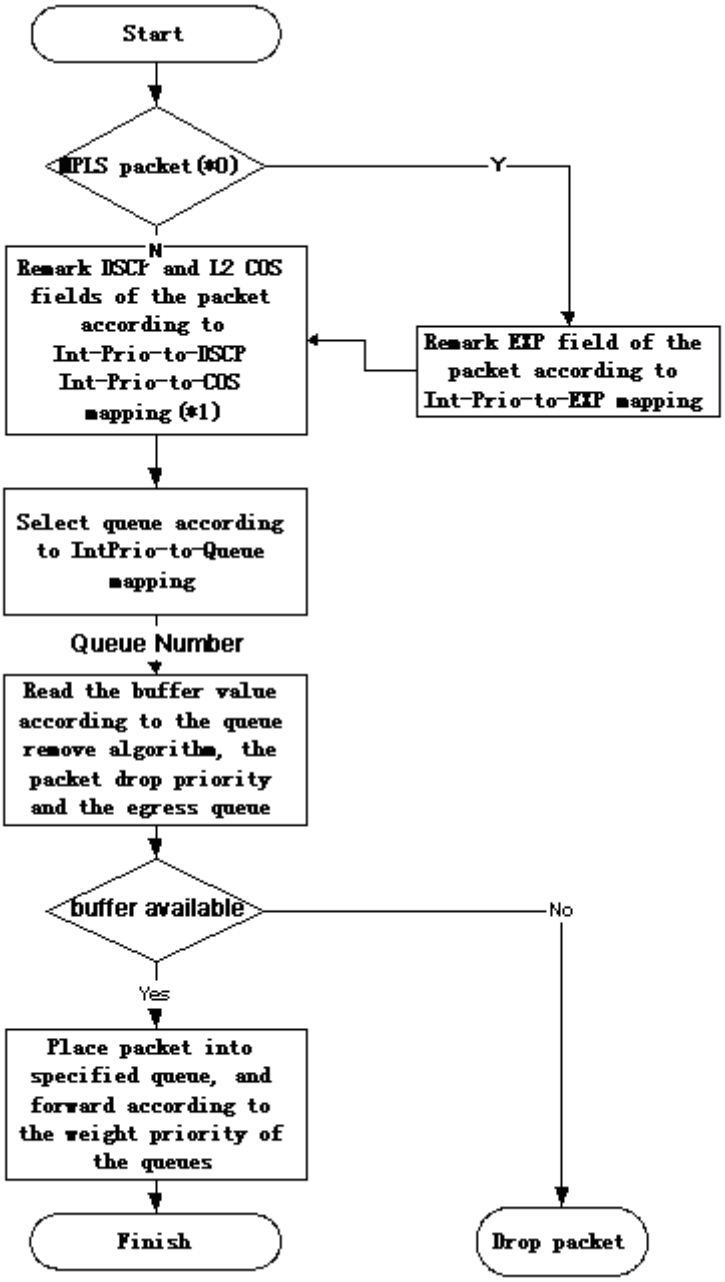

Fig 1-6 Queuing and Scheduling process

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.

Configure queue management algorithm

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

Configure QoS mapping

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

1. Configure class map.

Command	Explanation
Global Mode	
`class-map <class-map-name>` `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> | 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> | exp <exp-list>}` `no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos | exp}`	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.

2. Configure a policy map

Command	Explanation
Global Mode	
policy-map <policy-map-name> 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>] 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 {ip dscp <new-dscp> | ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | cos <new-cos>} no set {ip dscp | ip precedence | internal priority | drop precedence | cos }K	Assign a new DSCP, CoS, IP Precedence value for the classified traffic; the no command cancels the newly assigned value.
Single bucket mode: policy <bits_per_second> <normal_burst_bytes> ({conform-action ACTION | exceed-action ACTION}) Dual bucket mode: policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] | <maximum_burst_bytes> [{conform-action ACTION | exceed-action ACTION | violate-action ACTION }] ACTION definition: drop | transmit | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | set-cos-transmit <cos_value> | set-internal-priority <inp_value> | set-Drop-Precedence <dp_value> 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. Single bucket mode is supported by the specific switch.
policy aggregate <*aggregate-policy-name*> no policy aggregate <*aggregate-*	Apply a policy to classified traffic; the no command deletes the

policy-name>	specified policy set.
accounting no accounting	Set statistic function for the classified 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, in-profile means green and out-profile means red. In dual bucket mode, there are three colors of the packets. In the print information, in-profile means green and out-profile means red and yellow.
Policy class map configuration mode	
drop no drop transmit no transmit	Drop or transmit data package 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 dscp no mls qos trust dscp	Configure port trust; the no command disables the current trust status of the port.
mls qos cos {*<default-cos>*} no mls qos cos	Configure the default CoS value of the port; the no command restores the default setting.
service-policy input *<policy-map-name>* no service-policy input {*<policy-map-name>*}	Apply a policy map to the specified port; the no command deletes the specified policy map applied to the port. Egress policy map is not supported yet or deletes all the policy maps applied on the ingress

	direction of the port
Global Mode	
service-policy input <policy-map-name> vlan <vlan-list> 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 | wrr | wdrr} no mls qos queue algorithm	Set queue management algorithm, the default queue management algorithm is wrr.
mls qos queue wrr weight <weight0..weight7> no mls qos queue wrr weight	Set queue weight based a port, the default queue weight is 1 2 3 4 5 6 7 8.
mls qos queue wdrr weight <weight0..weight7> no mls qos queue wdrr weight	Set queue weight based a port, the default queue weight is 10 20 40 80 160 320 640 1280.
mls qos queue <queue-id> bandwidth <minimum-bandwidth> <maximum-bandwidth> no mls qos queue <queue-id> bandwidth	Set bandwidth guarantee based a port.

5. Configure QoS mapping

Command	Explanation
Global Mode	
mls qos map (cos-dp <dp1…dp8> | dscp-dscp <in-dscp list> to <out-dscp> | dscp-intp <in-dscp list> to <intp> | dscp-dp <in-dscp list> to <dp>) no mls qos map (cos-dp | dscp-dscp	Set the priority mapping for QoS, the no command restores the default mapping value.

| dscp-intp | dscp-dp) mls qos map intp-dscp <dscp1..dscp8> no mls qos map intp-dscp	

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-dp | dscp-dscp | dscp-intp | dscp-dp | intp-dscp]	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 {interface [<interface-id>] [policy | queuing] | vlan <vlan-id>}	Displays QoS configuration information on a port.

1.3 QoS Example

❖ **Example 1:**

Enable QoS function, change the queue out weight of port ethernet 1/0/1 to 1:1:2:2:4:4:8:8, set the port 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)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# mls qos queue wrr weight 1 1 2 2 4 4 8 8
Switch(Config-If-Ethernet1/0/1)#mls qos cos 5
```

Configuration result:

When QoS enabled in Global Mode, the egress queue bandwidth proportion of port ethernet1/0/1 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 queue out 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:**

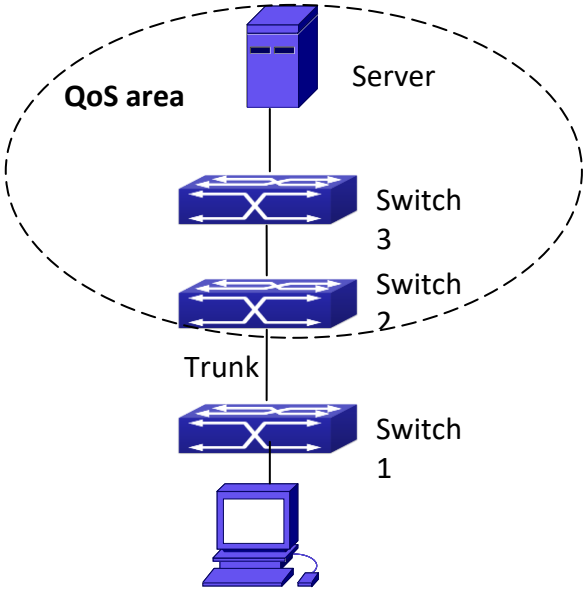

Fig 1-7 Typical QoS topology

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. The port connecting to switch2 is a trunk port. In Switch2, set port ethernet 1/0/1 that connecting to swtich1 to trust cos. 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 5
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
```

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.
- Policy map can only be bound to ingress direction, egress is not supported yet.
- At present, it is not recommended to synchronously use policy map on VLAN and VLAN's port.

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

1. Flow-based redirection configuration

Command	Explanation
Physical Interface Configuration Mode	
`access-group <aclname> redirect to interface [ethernet <IFNAME>|<IFNAME>]` `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.

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.

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.

3. FLEXIBLE QINQ CONFIGURATION

3.1 Introduction to Flexible QinQ

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.2 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>` `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>}` `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>` `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>]` `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 nested-vlan <vid>` `no set nested-vlan`	Add the external tag to the classified flow, the no command cancels the operation.

3. Bind flexible QinQ policy-map to port

Command	Explanation
Port mode	
`service-policy <policy-map-name> in` `no service-policy <policy-map-name> in`	Apply a policy-map to a port, the no command deletes the specified policy-map applied to the port.

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.

3.3 Flexible QinQ Example

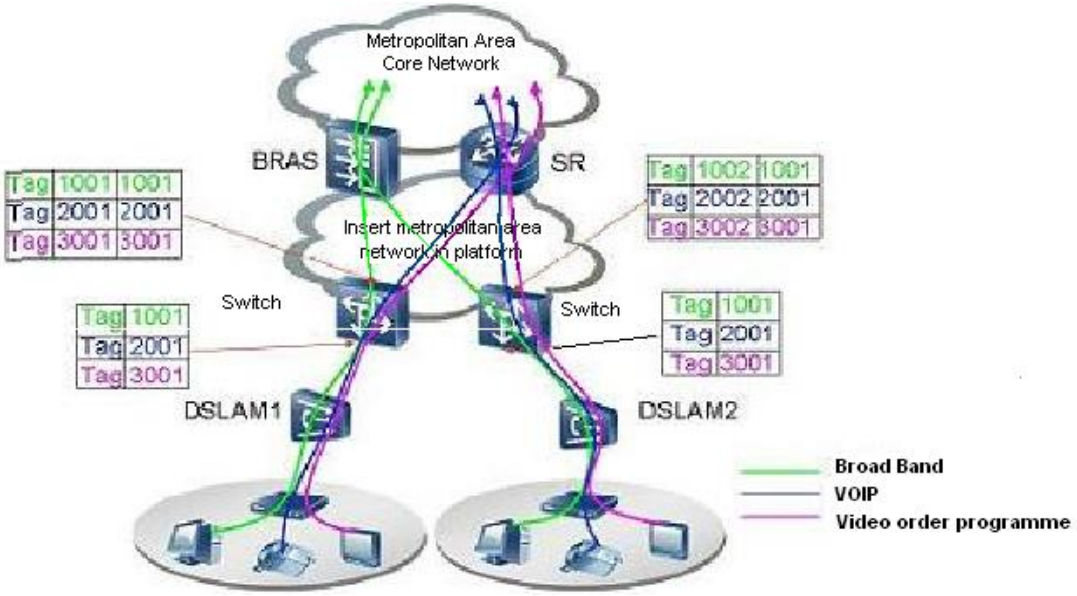

Fig 6-1 Flexible QinQ application topology

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 nested-vlan 1001
Switch(config-policymap-p1)#class c2
Switch(config-policymap-p1-class-c2)# set nested-vlan 2001
Switch(config-policymap-p1)#class c3
Switch(config-policymap-p1-class-c3)# set nested-vlan 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 p1 in
```

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 nested-vlan 1002
Switch(config-policymap-p1)#class c2
Switch(config-policymap-p1-class-c2)# set nested-vlan 2002
Switch(config-policymap-p1)#class c3
Switch(config-policymap-p1-class-c3)# set nested-vlan 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 p1 in
```

3.4 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