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.

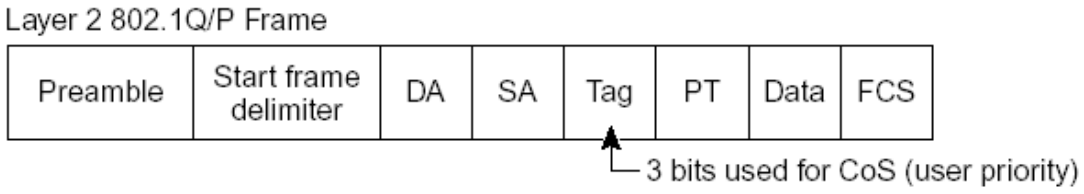


Fig 1-1 CoS priority

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.

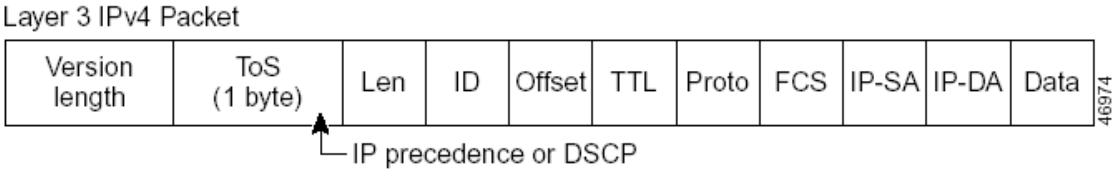


Fig 1-2 ToS priority

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.

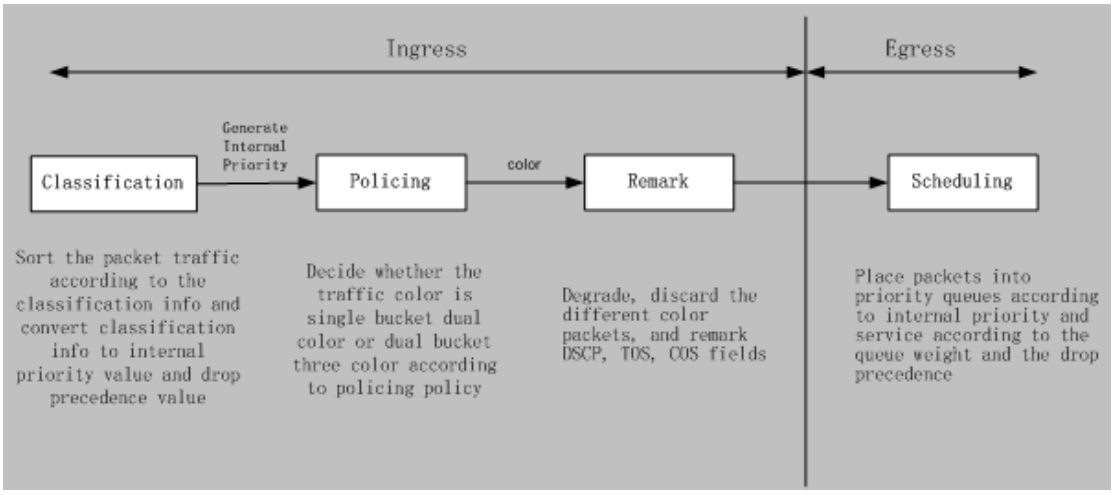


Fig 1-3 Basic QoS Model

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.

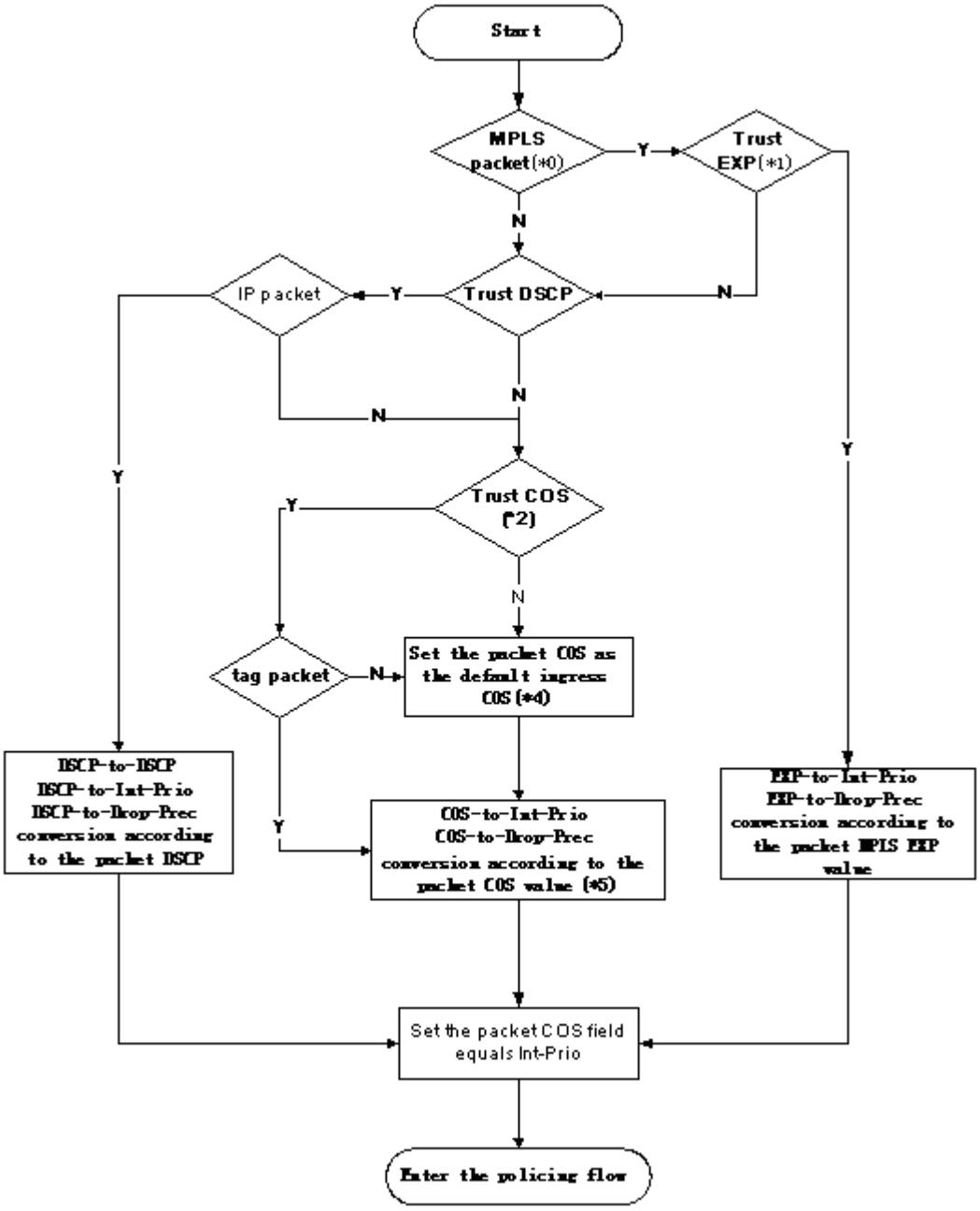


Fig 1-4 Classification process

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.

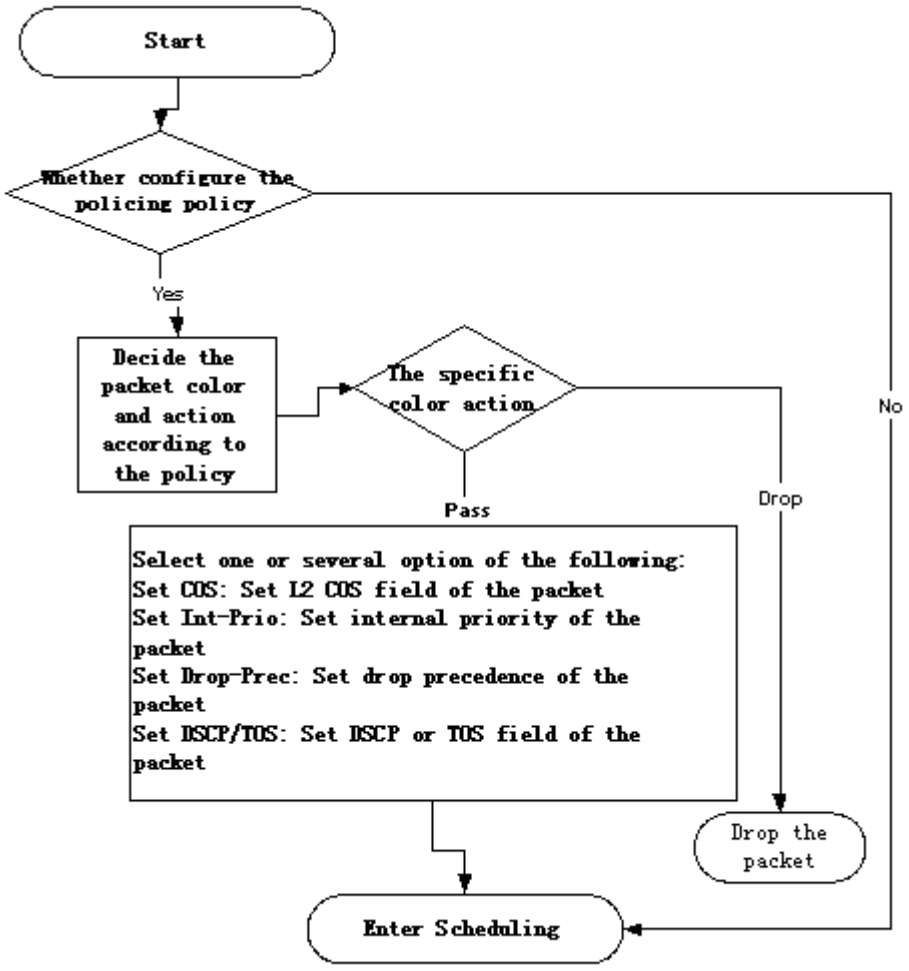


Fig 1-5 Policing and Remarking process

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.

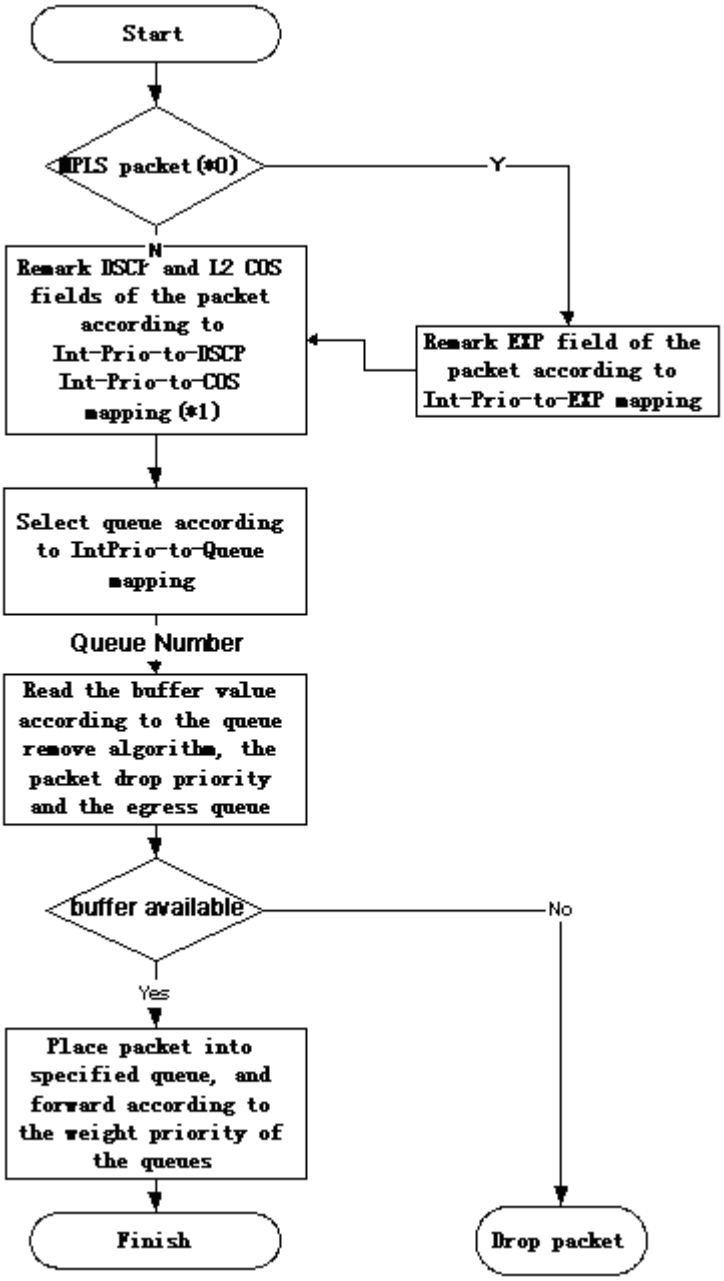


Fig 1-6 Queuing and Scheduling process

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 also supports to modify dynamically. 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*>	Create a policy map and enter policy

no policy-map <*policy-map-name*>	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-policy-name*>**	Apply a policy to classified traffic; the no command deletes the 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*>	Apply a policy map to the specified VLAN interface; the no command

no service-policy input {<*policy-map-name*>} *vlan* <vlan-list>	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> || cos-intp < in-cos list > | dscp-dscp <in-dscp list> to <out-dscp> |dscp-intp <in-dscp list> to <intp>| dscp-dp <in-dscp list> to <dp> | intp-exp <exp1…exp8>) **no mls qos map (cos-dp | dscp-dscp | dscp-intp | dscp-dp)** **mls qos map intp-exp <exp1…exp8>** **no mls qos map intp-exp**	Set the priority mapping for QoS, the no command restores the default mapping value.

6. Clear accounting data of the specific ports or VLANs

Command	Explanation
Admin Mode	
clear mls qos statistics [in | out] {interface <interface-name> | vlan <vlan-id>}	Clear the in or out directions accounting data of the specified ports or VLAN Policy Map.

7. Show configuration of QoS

Command	Explanation
Admin Mode	
show mls qos maps [cos-dp | cos-intp |dscp-dscp | dscp-intp | dscp-dp |intp-exp]	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>}	Display QoS configuration information on a port.
show mls qos in {interface <interface-name> policy | vlan <vlan-id>}	Show the policy configuration information of the port or vlan of in direction.
show mls qos interface <interface-id> wred [queue <queue-id>] [dp<dp>]	Show the wred parameter corresponding to dp value of the appointed queue under the port.
Show mls qos vlan	Show the qos information of VLAN interface.
show mls qos aggregate-policy [policy-name]	Show the configuration information of aggregate-policy.

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 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:

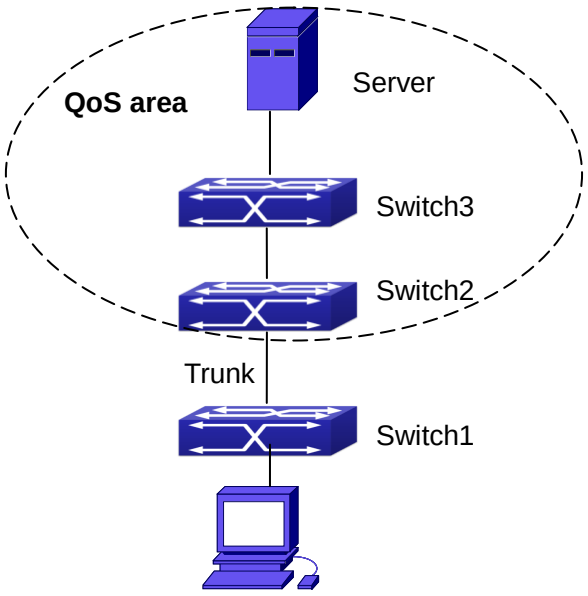


Fig 1-7 Typical QoS topology

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.

Chapter 2 PBR Configuration

2.1 Introduction to PBR

PBR（Policy-Based Routing）is a method which determines the next-hop of the data packets by policy messages such as source address, destination address, IP priority, TOS value, IP protocol, source port No, destination port No, etc.

2.2 PBR Configuration

1. Configure a class-map
2. Set match standard of the class-map
3. Configure a policy-map
4. Configure a policy map corresponding to a class map
5. Configure nexthop IPv4 address
6. Configure the port binding policy map
7. Configure the VLAN binding policy map

1. Configure a class-map

Command	Explanation
Global Configuration Mode	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	Set up or delete a class-map.

2. Set match standard of the class-map

Command	Explanation
Class-map Configuration Mode	
match ip {access-group <*acl-index-or-name*>} **no match ip {access-group}**	Set the match standard of the class-map

3. Configure a policy-map

Command	Explanation
Global Configuration Mode	

policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Set up or delete a policy-map.

4. Configure a policy map corresponding to a class map

Command	Explanation
Policy-map Configuration Mode	
class <*class-map-name*> **no class <*class-map-name*>**	Correspond a class-map, and enter the policy map mode.

5. Configure nexthop IPv4 address

Command	Explanation
Policy-class-map Mode	
set ipv4 [default] nexthop [vrf <vrf>] <*nexthop-ip*> **no set ipv4 nexthop**	Set nexthop IP for the classified traffic, the no command cancels the new assigned value.

6. Configure the port binding policy map

Command	Explanation
Port Mode	
service-policy {input <*policy-map-name*> | output <*policy-map-name*>} **no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**	Apply a policy map to the specified port. Only one policy map can be applied to each direction of each port. Egress policy map is not supported yet.

7. Configure the VLAN binding policy map

Command	Explanation
Global Configuration 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.

2.3 PBR Examples

Example:

On port ethernet1/0/1, apply policy-based routing on packages from 192.168.1.0/24 segment, and set the next-hop as 218.31.1.119, meanwhile the local network IP of this network ranges within 192.168.0.0/16. To assure normal communication in local network, messages from 192.168.1.0/24 to local IP 192.168.0.0/16 are not applied with policy routing.

Configuration procedure is as follows:

```
Switch#config
Switch(config)#access-list ip extended a1
Switch(Config-IP-Ext-Nacl-a1)#permit ip 192.168.1.0 0.0.0.255 any-destination
Switch(Config-IP-Ext-Nacl-a1)#deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.255.255
Switch(Config-IP-Ext-Nacl-a1)#exit
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group a1
Switch(Config-ClassMap-c1)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip nexthop 218.31.1.119
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
```

Configuration results:

First set an ACL a1 with two items. The first item matches source IP segments 192.168.1.0/24（allowed）. The second item matches source IP segments 192.168.1.0/24 and destination IP segments 192.168.0.0/16（rejected）. Turn on QoS function in global mode and create a class-map: c1 in which matches ACL a1, and create a policy-map in which quote c1. Set the next-hop IP as 218.31.1.119 and apply the policy-map at port ethernet1/0/1. After that, all messages on port ethernet 1/0/1 from segment 192.168.1.0/24 will be transmitted through 218.31.1.119 except those from 192.168.0.0/16 segment which are still be transmitted through normal L3 routing.

Chapter 3 IPv6 PBR Configuration

3.1 Introduction to PBR (Policy-based Router)

Policy-based routing provides a more powerful control over the forwarding and store of messages than traditional routing protocol to network managers. Traditionally, routers use the routing table derived from router protocol, and forward according to destination addresses. The policy-based router is more powerful and more flexible than the traditional one, because it enables network managers to choose the forwarding route not only according to destination addresses but also the size of messages, or source IP addresses. Policy can be defined as according to the balance of load in multiple routers or according to the quality of service (QOS) of the total flow forwarded in each line.

PBR (Policy-Based Routing) is a method which politically specifies the next hop when forwarding a data packet according to the source address, destination address, IP priority, TOS value, IP protocol, source port, destination port and other information of an IP packet.

3.2 PBR Configuration Task Sequence

1. Configure a class-map
2. Set the match standard in the class-map
3. Configure a policy-map
4. Configure to correlate a policy and a class-map
5. Configure the next hop IPv6 address
6. Configure the port binding policy map
7. Configure the VLAN binding policy map

1. Configure a class-map

Command	Explanation
Global Configuration Mode	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	Create or delete a class-map.

2. Set the match standard in the class-map

Command	Explanation
Class-map Mode	

match ipv6 {access-group <*acl-index-or-name*>} **no match ipv6 {access-group }**	Set the match standard in the class-map.

3. Configure a policy-map

Command	Explanation
Global Configuration Mode	
policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Create or delete a policy-map.

4. Configure to correlate a policy and a class-map

Command	Explanation
Policy-map Mode	
class <*class-map-name*> **no class <*class-map-name*>**	Correlate with a class, and enter the policy-map mode.

5. Configure the next hop IPv6 address

Command	Explanation
Policy-class-map Mode	
set ipv6 [default] nexthop [vrf <vrf>] <*nexthop-ip*> **no set ipv6 nexthop**	Set the next hop IP for the classified flow, the no command cancels the new assigned value.

6. Configure the port binding policy-map

Command	Explanation
Port Configuration Mode	
service-policy {input <*policy-map-name*> | output <*policy-map-name*>} **no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**	Apply a policy map to the specified port. Only one policy map can be applied to each direction of each port. Egress policy map is not supported yet.

7. Configure the VLAN binding policy map

Command	Explanation
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.

3.3 PBR Examples

Example:

On port ethernet 1/0/1, set the messages whose source IP is within the segment 2000:: /64 to do policy routing, the next hop is 3100::2.

The following is the configuration steps:

Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2000::1/64
Switch(Config-if-Vlan1)#ipv6 neighbor 2000::2 00-00-00-00-00-01 interface Ethernet 1/0/1
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 address 3000::1/64
Switch(Config-if-Vlan2)#ipv6 neighbor 3000::2 00-00-00-00-00-02 interface Ethernet 1/0/2
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ipv6 address 3100::1/64
Switch(Config-if-Vlan3)#ipv6 neighbor 3100::2 00-00-00-00-00-03 interface Ethernet 1/0/5
Switch(config)# ipv6 access-list extended b1
Switch(Config-IPv6-Ext-Nacl-b1)# permit tcp 2000:: /64 any-destination
Switch(Config-IPv6-Ext-Nacl-b1)#exit
Switch(config)#class-map c1
Switch(config-ClassMap)#match ipv6 access-group b1
Switch(config-ClassMap)# exit
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config-Policy-Class)# set ipv6 nexthop 3100::2
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
Switch(config)#interface ethernet 1/0/1
Switch(Config-Ethernet1/0/1)#service-policy input p1

Configuration result:

First, set an ACL containing one entry, names it as b1, matching source IP segment 2000::/64(permit). Globally enable QoS function, create a class-map:c1, and match ACL b1 in the class-map. Create a policy-map:p1, quoting c1 in p1, and set the next hop as 3100::2. Apply this policy-map on port ethernet 1/0/1. After that, the messages whose source IP are within the segment 2000::/64 received on port ethernet 1/0/1 will be forwarded through 3100::2.

3.4 PBR Troubleshooting Help

- ☞ At present, policy-map can only be bound to input port but not output port.
- ☞ Since hardware resources are limited, if the policy is too complicated to configure, relative information will be noticed to users.

Chapter 4 Flow-based Redirection

4.1 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.

4.2 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.

4.3 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

4.4 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 5 Egress QoS Configuration

5.1 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.

5.1.1 Egress QOS Terms

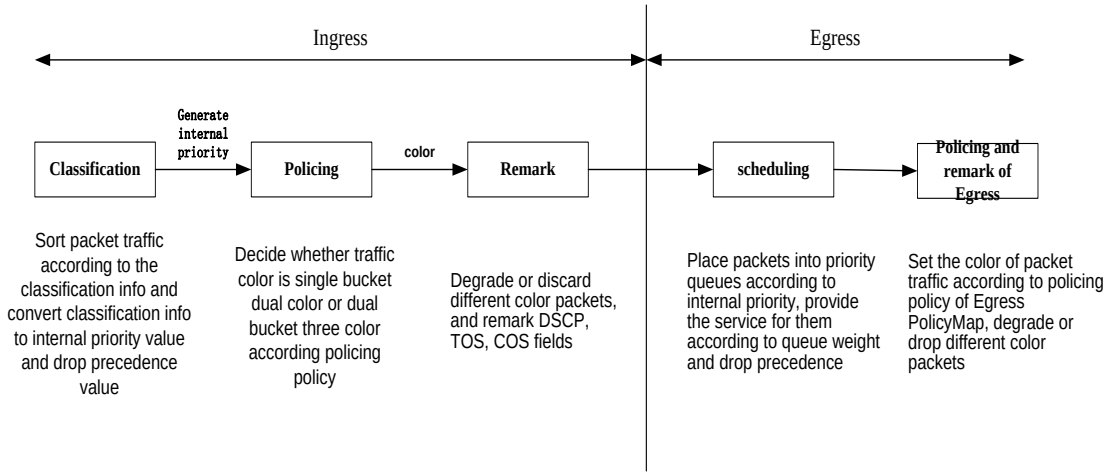
Egress QoS: Achieving QoS on egress of port.

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.

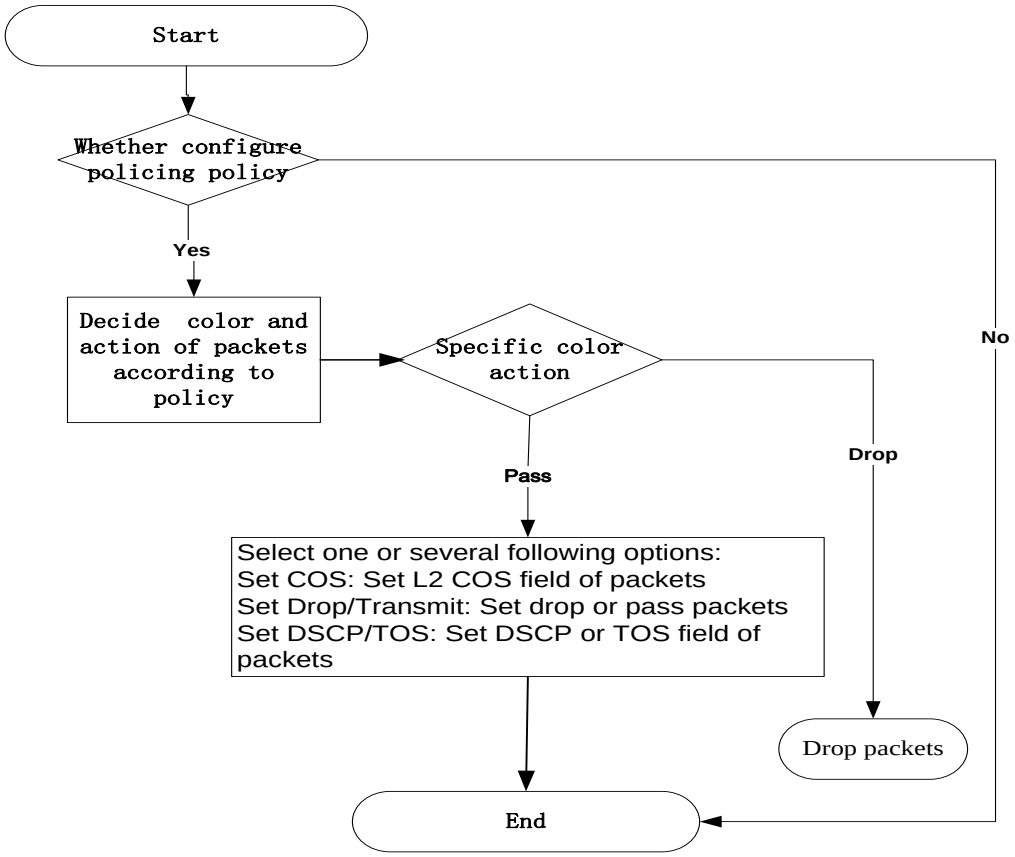
Outer_tpid: Protocol type of the network link layer header indicating the type of outer tag.

5.1.2 Basic Egress QoS Model



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:



5.2 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, it also supports to modify dynamically.

1. Configure a 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, 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*>} **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*> **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: **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-cos-transmit <*cos_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 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 **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*> **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*> **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. Clear accounting data of the specific ports or VLANs

Command	Explanation
Admin Mode	
clear mls qos statistics out [interface <*interface-name*> | vlan <*vlan-id*>]	Clear the out direction accounting data of the specified ports or VLAN Policy Map.

5. 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-dp| cos-intp | dscp-dscp | dscp-intp | dscp-dp |intp-exp] | [begin | include | exclude <regular-expression>]	Show the configuration of QoS global mapping.

5.3 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
```

5.4 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.

Chapter 6 Flexible QinQ Configuration

6.1 Introduction to Flexible QinQ

6.1.1 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.

6.1.2 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.

6.1.3 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.

6.2 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, it also supports to modify dynamically

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*> |c-vlan <vlan-list>| 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,CVid, 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 {s-vid <new-vid> | s-tpid <0x8100 | 0x88a8 | 0x9100> | c-vid <new-vid >} **no set {c-vid | s-vid | s-tpid}**	Assign the new cos and vid value to the packets which match the class map, no command cancels the operation.

add {s-vid <new-vid> | c-vid <new -vid>} **no add {s-vid | c-vid}**	Assign the new SVid and CVid value to the packets which match the class map, no command cancels the operation.
delete c-vid **no delete c-vid**	Delete the inner VLAN Tag for the packet which match the class map, no command cancels the operation.

3. Bind flexible QinQ policy-map to port

Command	Explanation
Port mode	
service-policy {input < policy-map-name >} **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.

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.

6.3 Flexible QinQ Example

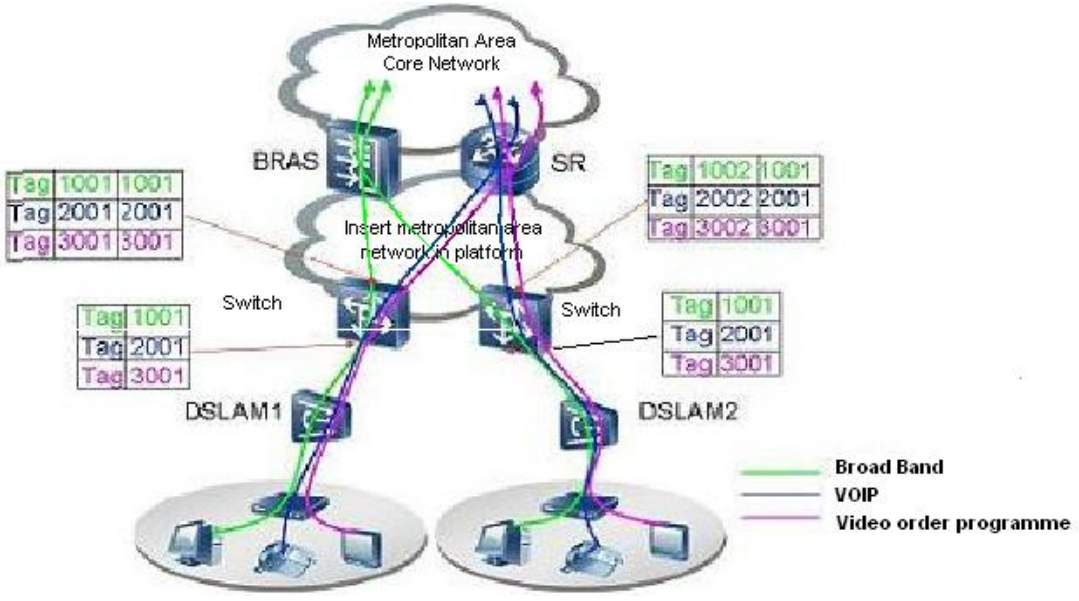


Fig 6-1 Flexible QinQ application topology

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 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 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 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 p1 in
```

6.4 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

Chapter 7 MPLS QoS Configuration

7.1 MPLS QoS Introduction

The exp segment of MPLS（MultiProtocol Label Switch）provides the support for QoS, and hence a better service for the network communication.

7.1.1 MPLS QoS Terms

CoS：Class of Service, the class information carried in L2 802.1Q frames. It takes up 3 bits in the Tag segment of the frame header, and is called the user priority, ranging from 0 to 7.

Fig 7-1 The CoS Priority

DSCP：Differentiated Services Code Point, the class information carried in L3 IP headers. It takes up 6 bits, ranging from 0 to 63, and is downward compatible with IP Precedence.

Fig 7-2 The MPLS EXP Priority

A segment in MPLS messages presenting the service class of MPLS messages. It takes up 3 bits, ranging from 0 to 7.

Internal DSCP: the internal priority configuration of the switch, used to distinguish the priorities of the switch internal data messages, ranging from 0 to 63.

In-Profile: we call the flow within the range specified by the QoS monitor policy (the bandwidth or burst value) In-Profile.

Out-of-Profile: we call the flow exceeding the range specified by the QoS monitor policy (the bandwidth or burst value) Out-of-Profile.

7.1.2 The Realization of MPLS QoS

To realize QoS of L3 switch software, a universal and mature reference model is a prerequisite. QoS can’t create any new bandwidth, but it can adjust and configure the existing bandwidth resource to achieve the maximum efficiency. A complete applicable QoS can fully control and manage the network data transmission.

The MPLS QoS based on differentiated services will specify a priority for every

packet at the entrance of the network. Such class information will be stored in the exp filed of the label. MPLS QoS provides same services to packets at the same priority level, and different services for packets with different priority. The switches or routers supporting MPLS QoS can provide different bandwidth to packets according to their class information, overwrite the class information of packets according to the monitor policy configuration and even drop some low-level packets when the bandwidth resource is tight.

7.2 MPLS QoS Configuration

The configuration task sequence of MPLS QoS is as follows:

1. Configure the class map

   After creating a class rule, such as matching according to exp, the switch will treat data flow of different classes with different policies.

2. Apply MPLS QoS to the port

   Set the trust mode of the interface as exp, or bind the policy. The polity can only take effect on a specific interface after being bound to the latter.

3. Configure the mapping relationship of MPLS QoS

   Configure the mapping from exp to internal priority, and the mapping from drop precedence and internal priority to exp.

4. Display the mapping relationship of MPLS QoS

1. Configure the match rule of the class map as exp

Command	Explanation
Global Configuration Mode	
match exp <exp-list> **no match exp**	Configure the match standard in class map, the no command deletes the specific match standard.

2. Configure trust exp

Command	Explanation
Port Configuration Mode	
mls qos trust exp **no mls qos trust**	Set the switch port to trust exp; the no operation will disable this trust state of the switch port. This command is not supported by switch.

3. Configure the MPLS QoS mapping

Command	Explanation

Global Configuration Mode	
mls qos map {exp-intp <intp1..intp8> | exp-dp <*dp1..dp8*>} **no mls qos map {exp-intp | exp-dp}** **mls qos map intp-exp <exp1..exp8>** **no mls qos map intp-exp**	Set the mapping from exp to internal priority, exp to drop priority and internal priority to exp.

4. Display the mapping relationship of MPLS QoS

Command	Explanation
Admin Mode	
show mls qos maps [exp-intp | exp-dp | intp-exp |]	Display the mapping relationship of MPLS QoS.

7.3 MPLS QoS Examples

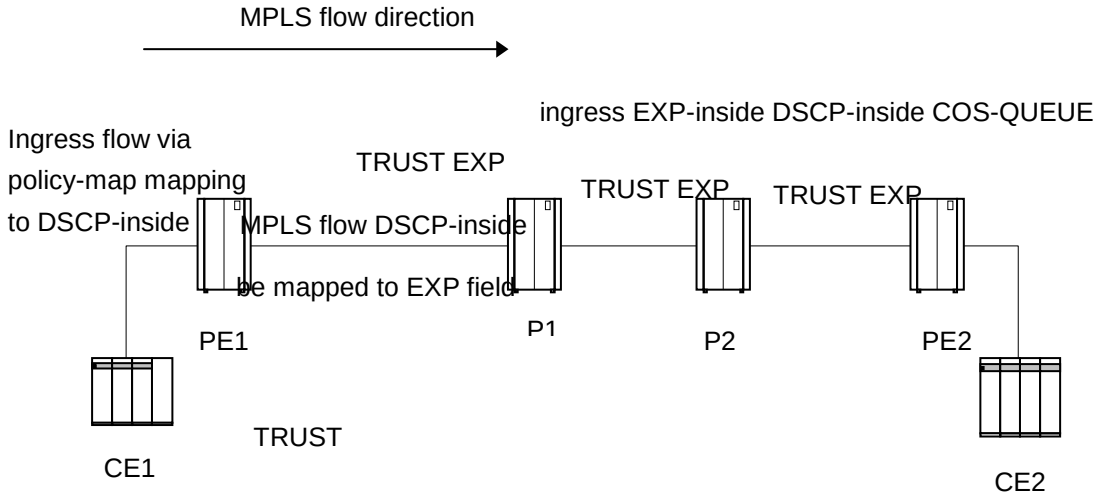


Fig 7-3 MPLS QoS Example

According to the diff-serv QOS model, the edge switch will classify the flow, and the core switch will forward the data packets according to their classes. As demonstrated in the above figure, the edge switch PE classifies the data flow according to the policy map, and store the result class in MPLS messages. The following switches P and PE, which are in the state of “trust EXP”, will forward the flow.

Configuration Examples:

Assume that normal data flows enter PE1 via vlan10, voip flows enter PE1 via vlan100, and the flows enter through Ethernet 1/0/1 and leave from Ethernet 1/0/2.

PE1：

Switch#config

Switch(config)#class-map voip

Switch(Config-ClassMap-voip)#match vlan 100

Switch(Config-ClassMap-voip)# exit

Switch(config)#class-map data

Switch(Config-ClassMap-data)#match vlan 10

Switch(Config-ClassMap-data)# exit

Switch(config)#policy-map p1

Switch(Config-Policy Map-p1)#class voip

Switch(Config-Policy Map-p1-Class-c1)#set Internal-Priority 1

Switch(Config-Policy Map-p1-Class-c1)#exit

Switch(Config-Policy Map-p1)#class data

Switch(Config-Policy Map-p1-Class-c1)#set Internal-Priority 0

Switch(Config-Policy Map-p1-Class-c1)#exit

Switch(Config-Policy Map-p1)#exit

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

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

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

Switch(Config-If-Ethernet1/0/2)# mls qos queue wrr weight 1 2 3 4 5 6 7 8

Data flows, whose internal priority is 0, leave from queue 0 according to the default Int-Prio-TO-QUEUE, and EXP, DSCP and COS fields of the data packets are set as 0 according to the default Int-Prio-TO-(EXP, DSCP, COS) mapping.

Voip flows, whose internal priority is 1, leave from queue 1 according to the default Int-Prio-TO-QUEUE, and EXP, DSCP and COS fields of the data packets are set as 1 according to the default Int-Prio-TO-(EXP, DSCP, COS) mapping.

P1, P2, PE2: will be forwarded according to their classes, all flows will enter through Ethernet 1/0/1 and leave from Ethernet 1/0/2.

Switch#config

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

Switch Config-If-Ethernet1/0/1)#

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

Switch(Config-If-Ethernet1/0/2)#mls qos queue wrr weight 1 2 3 4 5 6 7 8

Data flows, whose EXP is 0, egress from queue 0 according to the default EXP-TO-(Int-Prio, Drop-Prec) and Int-Prio-TO-QUEUE, and EXP, DSCP and COS fields of the data packets are set as 0 according to the default Int-Prio-TO-(EXP, DSCP, COS) mapping.

Voip flows, whose EXP is 1, egress from queue 0 according to the default

EXP-TO-(Int-Prio, Drop-Prec) and Int-Prio-TO-QUEUE, and EXP, DSCP and COS fields of the data packets are set as 1 according to the default Int-Prio-TO-(EXP, DSCP, COS) mapping.

7.4 MPLS QoS Troubleshooting Help

- ☞ The MPLS should be enabled on the switch port otherwise the MPLS QoS will be unavailable.
- ☞ After passing an interface with MPLS QoS enabled, the cos value of MPLS messages will be set to 0 while dscp will stay the same.

Chapter 8 Egress Queue Scheduling Configuration

8.1 Introduction to Egress Queue Scheduling

When forwarding packets results in congestion, with egress queue scheduling, high priority queue is served prior to low priority queue according to packet's priority, so as to implement QoS aim. The chip supports the scheduling arithmetics of SP, RR, WRR, and WDRR.Etc. According to different scheduling levels, there is single-stage scheduling and multi-stage scheduling. Under the single-stage scheduling, the data packet will come out from the egress after it wined in the queues competition. Under the multi-stage scheduling, the data packet will enter into the last level of scheduling node to join the competition after it wined in the queues competition, the physical port is the highest level of the scheduling node and only the data packet which wined in the highest level of scheduling node will be forwarded out from the port. This device supports the three-level scheduling.

8.1.1 Egress Queue Scheduling Terms

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.
Internal Priority: The internal priority setting of the switch chip, its valid range relates with the chip, its shortening is Int-Prio or IntP.
L2 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 in the range of 0 to 7.
ETS: Enhanced Transmission Selection, it processes multi-level scheduling for different traffic. (IEEE 802.1Qaz)
UC: known unicast packet, it is the only one of the forwarding destination port.
MC: non-unicast packet, it mainly includes the unknown unicast, multicast, broadcast, and mirror image.etc.

8.1.2 Egress Queue Scheduling Implement

Egress queue scheduling mechanism supports three-level scheduling, besides, UC packets and MC packets can configure scheduling mode respectively, WRR and WDRR scheduling modes can configured scheduling weight respectively. In queue scheduling,

UC packets include unicast packets, MC packets include broadcast packets, multicast packets (Except the Multicast traffic which is expected to have a single destination in the upstream direction), monitor data packets and DLF packets, and so on.

For packet flow, packets should distinguish UC packets or MC packets at first, and set the mapping from CoS to queue in COS_MAP table, form the corresponding mapping queue (at present, unicast packets with cos values from 0 to 7 are mapped to UC queues with number from 1 to 8, non-unicast packets with cos value of 0 are mapped to queue1 of MC, non-unicast packets with cos values from 1 to 3 are mapped to queue2 of MC, non-unicast packets with cos values from 4 to 6 are mapped to queue3 of MC, non-unicast packets with cos value of 7 are mapped to queue4 of MC) to process three-level scheduling. Scheduling flow is shown in the following:

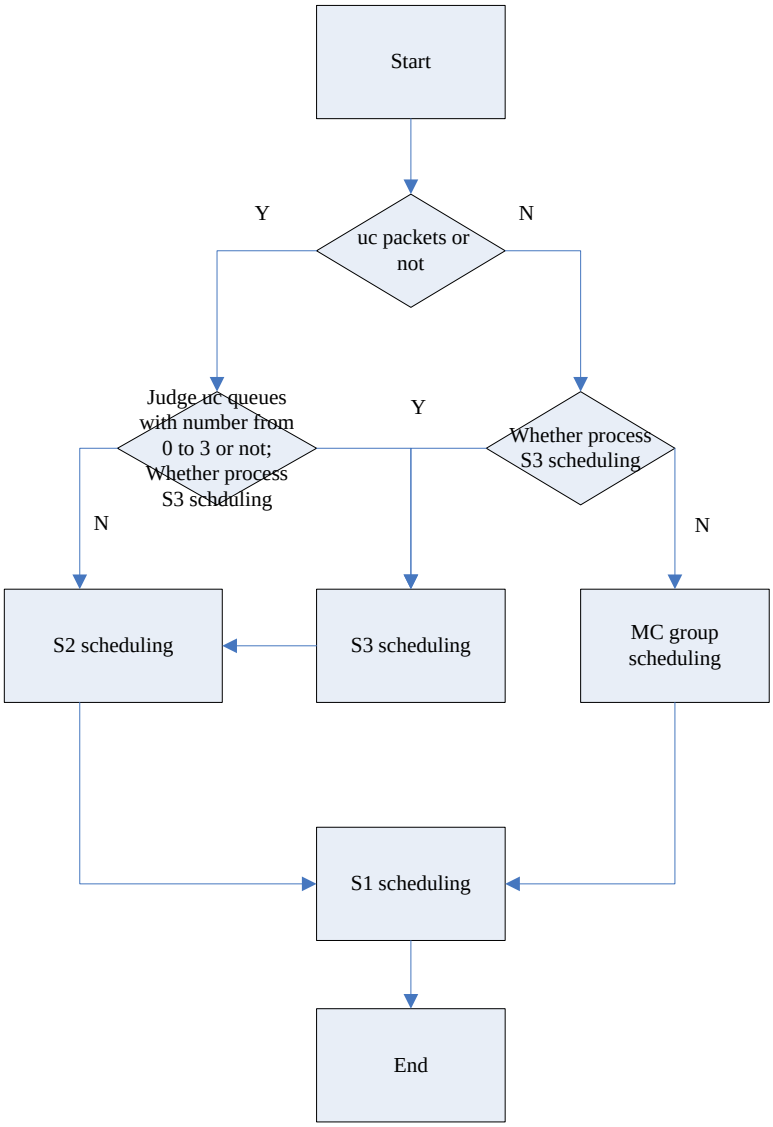


Fig 8-1 Three-level scheduling flow chart

In the above figure, packets will pass S3 scheduling, S2 scheduling (MC Group) and S1 scheduling in turn, S3 is able to schedule four queues with MC packets and 0-3 queues

with number from 0 to 3 about UC packets, set mapping from these queues to S2 scheduling node. S2 scheduling node includes three scheduling nodes, their scheduling results and other queues (UC queues, QM and SC queues of MC) enter S1 scheduling node. Besides, S3 is set as RR scheduling mode, S2 (including MC_GROUP) is set as WRR scheduling mode, S1 is set as SP scheduling mode by default. To be mentioned, only four MC queues can be scheduled to S3 scheduling, but all MC queues are scheduled to MAC-GROUP to directly enter S1 scheduling.

8.1.3 Basic Egress Queue Scheduling Model

There are two scheduling modes supported by port. One is the normal scheduling mode which is compatible with the previous command mode (it is called as the normal mode), the other is ETS scheduling mode.

Switch uses the normal mode as the default scheduling mode, its mechanism is shown in the following, thereinto S3 scheduling node uses RR scheduling algorithm, S2.1 uses WRR scheduling algorithm.

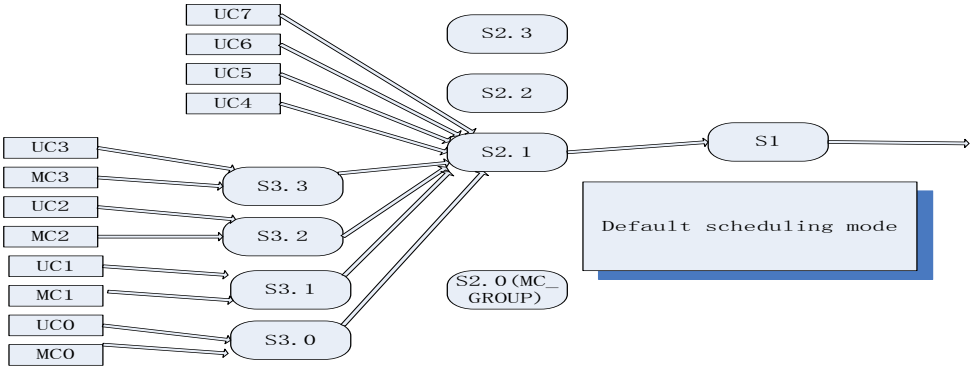


Fig 8-2 Default scheduling mode

To provide many selections, ETS scheduling mode includes UC-MC mode and advanced ETS mode. UC-MC scheduling mechanism is shown in the following, thereinto S2.1 and mc-group nodes use WRR scheduling algorithm, S1 node uses SP scheduling algorithm. Under the UC-MC mode, S1 node adopts SP scheduling arithmetic always, so there is the strict priority relation. User can select to schedule UC or MC flow first.

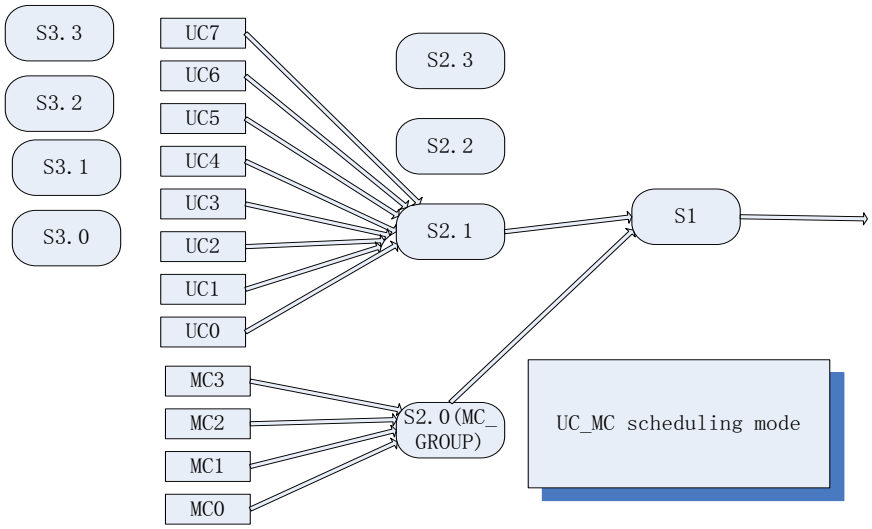


Fig 8-3 UC-MC scheduling mode

Advanced ETS scheduling mechanism is shown in the following, a UC queue, a MC queue or a scheduling node can be mapped to one queue of upper node only, at the same time, there is only one input source for each queue of any scheduling node. UC7~UC4 can be mapped to S2.1/S2.2/S2.3 node only, UC3~UC0 can be mapped to S2.1/S2.2/S2.3 node or S3.3~S3.0 node (If they are mapped to S3 scheduling node, UC3~UC0 must be mapped S3.3~S3.0 respectively). MC3~MC0 can be mapped to S3 scheduling node or S2.0 (MC_GROUP) node (If they are mapped to S3 scheduling node, MC3~MC0 must be mapped to queue with number 0 on S3.3~S3.0 respectively). S3.3~S3.0 only be mapped to S2.1/S2.2/S2.3, and S2.3~S2.0 only be mapped to queues with number from 0 to 3 in S1 scheduling node. Under the advanced ETS mode, the chip provides the most flexibility, user can configure the levels of flow joining scheduling in the range that chip can bear.

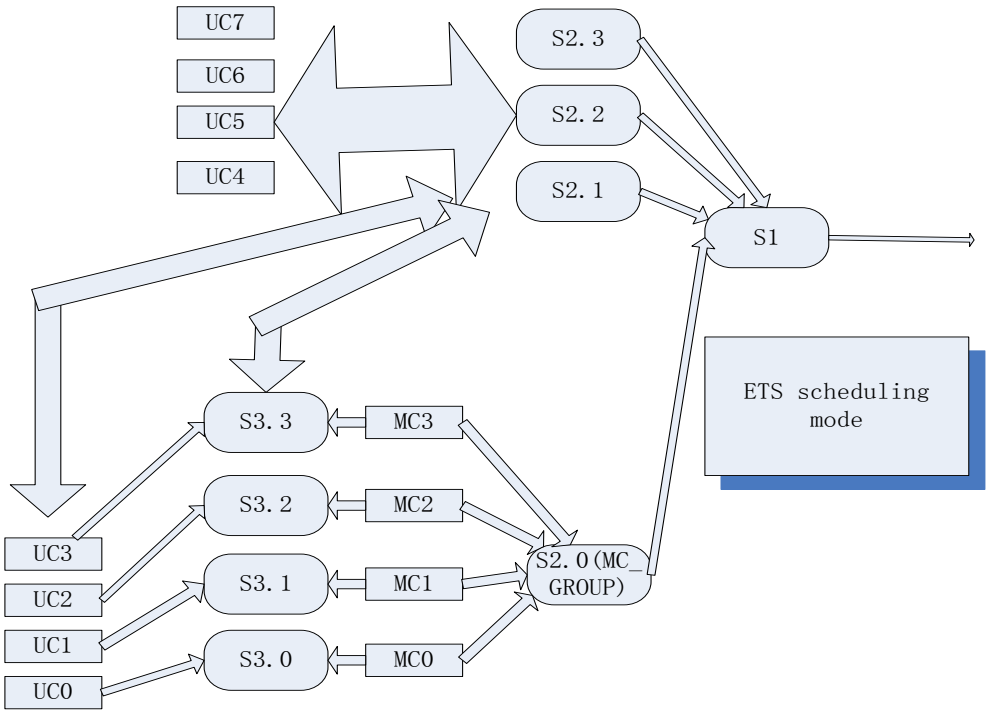


Fig 8-4 Advanced ETS scheduling mode

8.2 Egress Queue Scheduling Configuration

Egress queue scheduling configuration task list:

1. Configure scheduling mode for ports

Configure egress queue scheduling as normal mode, UC-MC mode or advanced ETS mode.

2. The scheduling policy table can be configured if enabled advanced ETS mode on the port

Create ETS scheduling policy table under the global mode. This table is configured globally, it can be applied onto multi-ports.

3. Configure scheduling node

Create the scheduling node under the scheduling policy table mode. Currently, S1 node only can configure one node, named S1.1. 4 can be configured at most in S2, named S2.1~S2.4, S2.1 only can be used in scheduling MC flow, S2.2~S2.4 cannot be used in scheduling MC flow. 4 can be configured at most in S3, named S3.1~S3.4.

4. Configure the data source of every subqueue of the scheduling node

User can define the the data source of every subqueue of the scheduling node. The multi-stage scheduling can be reflected through this command.

5. Configure the maximum and minimum bandwidth of scheduling arithmetic, scheduling weight, scheduling node

Under the scheduling node mode, user can configure the scheduling arithmetic used in scheduling node and configure the queue weight of every subqueue. User can also configure the integral maximum and minimum bandwidth of this scheduling node. Actually, there are no commands that can configure the maximum and minimum bandwidth of every subqueue. So configuring the integral maximum and minimum bandwidth of the scheduling node is equivalent to configuring the maximum and minimum bandwidth of the last level node of this scheduling node.

6. Configure the maximum and minimum bandwidth of multicast and unicast queues

Configure the maximum and minimum bandwidth of multicast and unicast queues.

7. Bind scheduling policy map to port's egress

A policy will only take effect on a port when it is bound to that port. The policy only can be bond to the port which has enabled ETS but not enabled UC-MC mode.

Configure queue scheduling when ETS is not enabled on a port

When port does not enable ETS, the corresponding queue scheduling configuration is also configured in normal node, such as queue scheduling algorithm, queue weight.

Configure bandwidth limit of queue

When port enables ETS, MC and UC queue bandwidth limit can be configured. When port does not enable ETS, UC queue bandwidth limit can be configured.

Show queue scheduling command

Check queue scheduling configuration of port by show command.

1. Configure scheduling mode for ports

Command	Explanation
Port mode	
mls qos ets enable **no mls qos ets enable**	Enable ETS queue scheduling mode for a port, the no command disables ETS mode.
mls qos queue {uc | mc} higher **no mls qos queue {uc | mc} higher**	Configure the priority of UC or MC, the no command disables the priority configuration.

2. Configure ETS scheduling policy map

Command	Explanation
Global mode	
mls qos schedule policy <polcicyName> **no mls qos schedule policy <polcicyName>**	Create a scheduling policy and enter the scheduling policy mode, the no command deletes the specified scheduling policy.

Scheduling policy mode	
mls qos schedule level <levelID> node <nodeID> **no mls qos schedule level <levelID> node<nodeID>**	Create a scheduling node and enter the corresponding scheduling node mode, the no command cancels the specified scheduling node configuration.
Scheduling node mode	
mls qos schedule queue <queueID> input {{UC <ucID>} | {MC <mcID>} | {node <nodeID>}} **no mls qos schedule queue <queueID> input {{UC <ucID>} | {MC <mcID>} | {node <nodeID>}}**	Configure the input data source of a queue on a scheduling node, the no command cancels the operation.
mls qos bandwidth <min-bandwidth> <max-bandwidth> **no mls qos bandwidth <min-bandwidth> <max-bandwidth>**	Configure the bandwidth limit for a scheduling node, the no command cancels the configuration.
mls qos schedule algorithm {sp | wdrr | wrr} **no mls qos schedule algorithm**	Configure queue scheduling algorithm for a scheduling node, the no command restores the default scheduling algorithm.
mls qos schedule {wrr | wdrr} weight <weight0..weight17> **no mls qos schedule {wrr | wdrr} weight**	Configure queue scheduling weight when the port does not enable ETS, the no command restores the default weight.

3. Apply egress scheduling policy to port

Command	Explanation
Port mode	
mls qos schedule policy bind <policyName> **no mls qos schedule policy bind <policyName>**	Bind a scheduling policy to a port, the no command cancels the binding between the scheduling policy and the port.

4. Configure queue scheduling when ETS is not enabled on a port

Command	Explanation
Port mode	
mls qos queue algorithm {sp | wrr | wdrr}	Configure queue scheduling algorithm

no mls qos queue algorithm	for a port in normal scheduling mode, the no command restores the default scheduling algorithm.
mls qos queue {wrr | wdrr} weight <weight0..weight17> **no mls qos queue {wrr | wdrr} weight**	Configure queue scheduling weight when the port does not enable ETS, the no command restores the default weight.

5. Configure bandwidth limit of queue

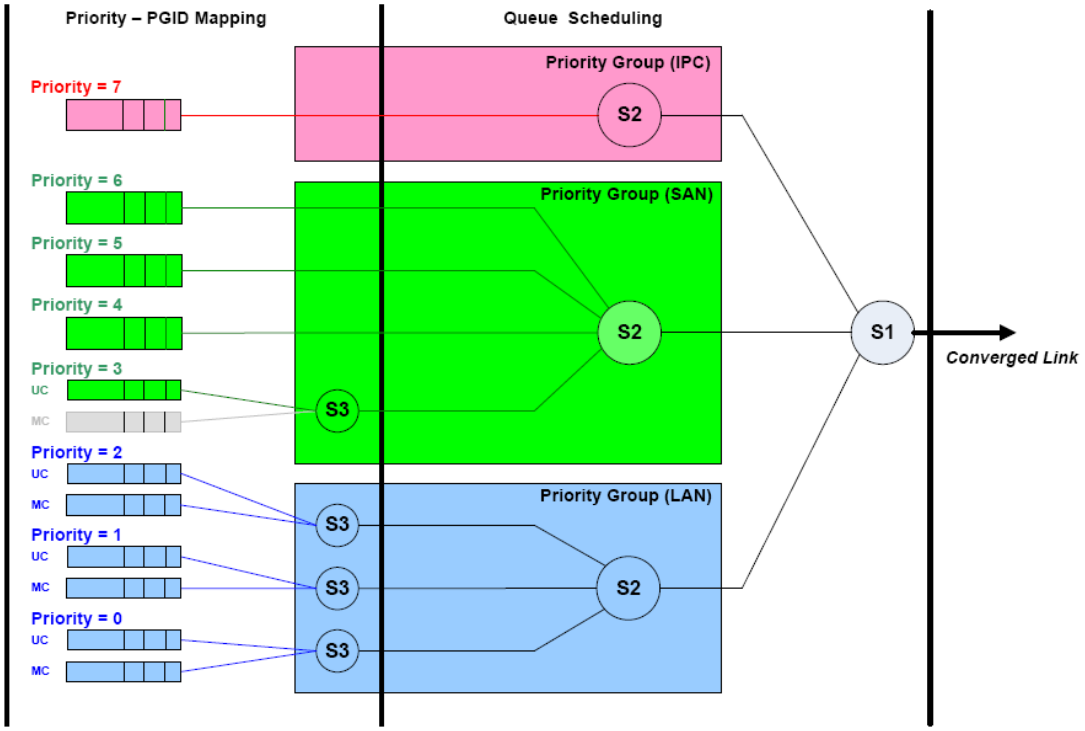
Command	Explanation
Port mode	
mls qos mc queue <queue-id> bandwidth <min-bandwidth> <max-bandwidth> **no mls qos mc queue <queue-id> bandwidth**	Configure the bandwidth limit for a MC queue after a port enables ETS. The no command cancels the configuration.
mls qos queue <queue-id> bandwidth <minimum-bandwidth> <maximum-bandwidth> **no mls qos queue <queue-id> bandwidth**	Configure the bandwidth limit for UC queue on a port. The no command cancels the configuration.

6. Show queue scheduling command

Command	Explanation
Admin mode, global mode, port mode	
show mls qos ets interface [<interface-name> | <interface-list>]	Show whether the interface enables ETS scheduling.
show mls qos schedule interface [<interface_name> | <interface_list>]	Show queue scheduling configuration for the interfaces.

8.3 Egress Queue Scheduling Examples

Example:



To distinguish the priority of different data streams and schedule them in DCB (DATA CENTER BRIDGE) environment, there are three kinds of data stream, they are LAN, SAN (Storage Area Network), IPC (Inter Process Communication). Thereinto, IPC priority is the highest, the second is SAN data (usually, it is UC data). Configuration is shown in figure, UC7 packets are the high priority IPC packets with the low latency, such as voice, they enter S2.2 scheduling directly. UC4-6 is SAN packets, UC3 and MC3 belong to LAN packets, they enter S3.3 scheduling node directly to be scheduled to S2.1 scheduling. UC0-2 and MC0-2 will enter S3.0~S3.2 scheduling node, so as to be scheduled by S2.1 scheduling node. Besides, S1 scheduling is configured as SP+WDRR scheduling mode, namely, IPC packets can be scheduled by queue scheduling firstly as long as they exist, other packets are scheduled with WDRR scheduling algorithm according to the configured weight.

Configuration procedure:

Switch(config)#mls qos schedule policy p

Switch (config-sche-policy-p)#mls qos schedule level 3 node 1

Switch (config-sche-policy-p-lel3nod1)#mls qos schedule queue 1 input mc 1

Switch (config-sche-policy-p-lel3nod1)#mls qos schedule queue 2 input uc 1

Switch (config-sche-policy-p-lel3nod1)#exit

Switch (config-sche-policy-p)#mls qos schedule level 3 node 2

Switch (config-sche-policy-p-lel3nod2)#mls qos schedule queue 1 input mc 2

Switch (config-sche-policy-p-lel3nod2)#mls qos schedule queue 2 input uc 2

Switch (config-sche-policy-p-lel3nod2)#exit

Switch (config-sche-policy-p)#mls qos schedule level 3 node 3

```
Switch (config-sche-policy-p-lel3nod3)#mls qos schedule queue 1 input mc 3
Switch (config-sche-policy-p-lel3nod3)#mls qos schedule queue 2 input uc 3
Switch (config-sche-policy-p-lel3nod3)#exit
Switch (config-sche-policy-p)#mls qos schedule level 3 node 4
Switch (config-sche-policy-p-lel3nod4)#mls qos schedule queue 1 input mc 4
Switch (config-sche-policy-p-lel3nod4)#mls qos schedule queue 2 input uc 4
Switch (config-sche-policy-p-lel3nod4)#exit
Switch (config-sche-policy-p)#mls qos schedule level 2 node 2
Switch (config-sche-policy-p-lel2nod2)#mls qos schedule queue 1 input node 1
Switch (config-sche-policy-p-lel2nod2)#mls qos schedule queue 2 input node 2
Switch (config-sche-policy-p-lel2nod2)#mls qos schedule queue 3 input node 3
Switch (config-sche-policy-p-lel2nod2)#exit
Switch (config-sche-policy-p)#mls qos schedule level 2 node 3
Switch (config-sche-policy-p-lel2nod3)#mls qos schedule queue 1 input node 4
Switch (config-sche-policy-p-lel2nod3)#mls qos schedule queue 2 input uc 5
Switch (config-sche-policy-p-lel2nod3)#mls qos schedule queue 3 input uc 6
Switch (config-sche-policy-p-lel2nod3)#mls qos schedule queue 4 input uc 7
Switch (config-sche-policy-p-lel2nod3)#exit
Switch (config-sche-policy-p)#mls qos schedule level 2 node 4
Switch (config-sche-policy-p-lel2nod4)#mls qos schedule queue 1 input uc 8
Switch (config-sche-policy-p-lel2nod4)#exit
Switch (config-sche-policy-p)#mls qos schedule level 1 node 1
Switch (config-sche-policy-p-lel1nod1)#mls qos schedule algorithm wdrr
Switch (config-sche-policy-p-lel1nod1)#mls qos schedule wdrr weight 1 2 4 0 0 0 0 0
Switch (config)#interface ethernet 1/0/2
Switch (config-if-ethernet1/0/2)#mls qos ets enable
Switch (config-if-ethernet1/0/2)#mls qos schedule policy bind p
```

8.4 Egress Queue Scheduling Troubleshooting

- ☞ Whether enable ETS of the port, the egress flow will always be scheduled according to UC and MC.
- ☞ When configuring UC/MC preference of port, it must firstly enable ETS for port.
- ☞ MC3~MC0 can be mapped to S3 scheduling node or S2.0 (MC_GROUP) scheduling node. If they are mapped to S3 scheduling node, MC3~MC0 must be mapped to queue with number 0 of S3.3~S3.0 respectively.
- ☞ If ETS is not enabled for port, mls qos queue <queue-id> bandwidth <minimum-bandwidth> <maximum-bandwidth> takes effect to UC queues. To be

mentioned, only bandwidth limit of UC5-8 queues take effect due to chip disfigurement in this condition.

- ☞ Egress queue scheduling supports the dynamic configuration. In global mode, the relative operation of multi-level queue scheduling will prompt the information (existing the unsupported line card) as long as the switch exists the line card without multi-level queue scheduling.
- ☞ We suggest user to use **show mls qos schedule interface** command to check the scheduling configuration message of some ports. Even the same scheduling policy is applied on multi-ports, the actual port scheduling configuration message may be different because of the different functions of the port.

Chapter 9 Vlan-shaping Configuration

9.1 Introduction to Vlan-shaping

VLAN Shaping is the differentiated service to achieve flow plastic for the specified VLAN. In Vlan Shaping, vlan id in the packet is equivalent to the number of the differentiated service, it is the core difference compared with the traditional flow plastic. The traditional flow plastic is based on the port and the queue, and the foundation to achieve differentiated service is the field of cos/dscp/exp of the packet mainly. So the traditional QOS is based on the business mainly. It cannot provide independent QOS service for different users under the current application of multi-user and multi-service sharing data link.

9.1.1 Vlan-shaping 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.

VID：VLAN ID is in Vlan Tag and used for distinguishing the 12bit of vlan, the range is 1 to 4094.

Queue：It is the egress scheduling queue of Cos.

EUC Queue: Extended Unicast Queue, is the extend unicast queue and used for Vlan flow scheduling queue. So in this text, euc queue is the same as vlan shaping queue.

Forwarding-class: Forwarding class is used to sign a class of flow and it is the original input source in multi-level scheduling. If the multi-level scheduling is treated as a tree, S1 is equivalent to the root, S2 and S3 are equivalent to branch node, the original input queue (unicast queue, multicast queue, extend unicast queue) is equivalent to the leaf node and it is the forwarding class. Currently, the forwarding class is specific to the extend unicast queue (vlan shaping).

Forwarding-class_match: It is the matching rules of forwarding class and used to classify the flow. The flow in accordance with the classification rules will enter the original queue that the forwarding class corresponded to participate the egress queue scheduling. Currently, the forwarding class is only matching the vlan id in outer tag.

Forwarding-profile：It is used to configure the action related to the queue scheduling for some flow configuration, such as queue scheduling algorithm, queue scheduling weight,

the minimum and maximum bandwidth and so on. Currently, the forwarding class can only configure the minimum and maximum bandwidth and quote some drop policy. A forwarding policy can be quoted by a forwarding class, it means scheduling the action for the queue configured by flow of the forwarding class.

Drop-profile: It is used to configure the action related to the queue drop for some flow configuration, such as configuring the parameter of wred. A drop policy can be quoted by a forwarding policy, it means dropping queue according to the wred algorithm configured by the drop policy.

9.1.2 Vlan-shaping Implementation

The following is the schematic of vlan flow egress scheduling plastic:

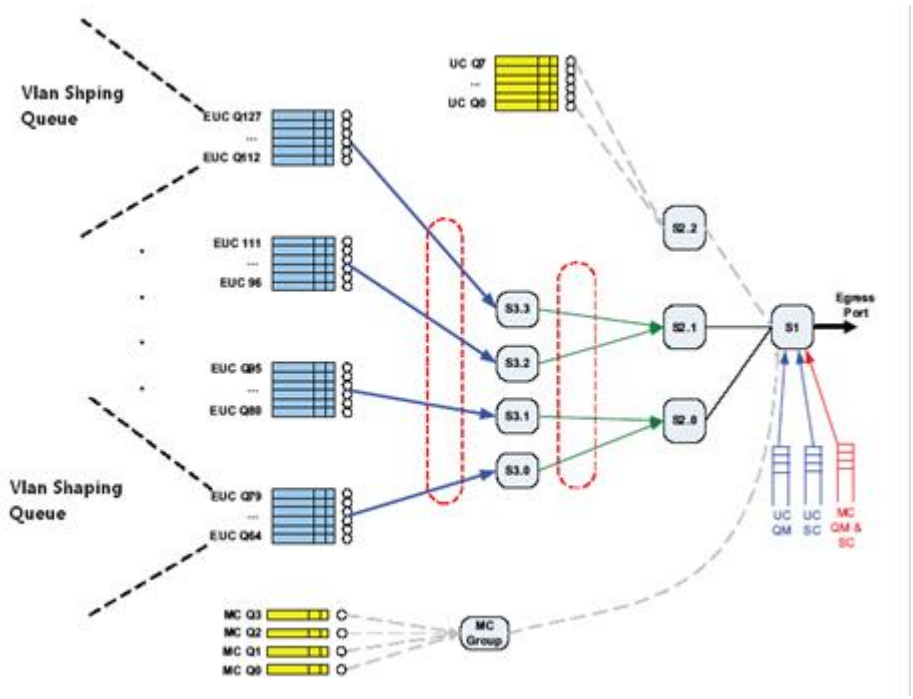


Fig 0-1 vlan-shaping scheduling achieving

In the figure above, the switch supports 64 vlan shaping. The 64 queues are into 4 groups and there are 16 queues per group. There are 4 nodes of S3 and in every node there is a queue group of vlan shaping. Every node of S3 supports 18 queues, the first two are MC and UC and the last 16 are the queues of vlan shaping. So vlan shaping is the same as a mechanism of S3 essentially.

In the occasion of enabling the function of vlan shaping, the packet is put into the specified queue of vlan shaping to participate scheduling according to vlan id in tag. The cos/dscp/exp of the original packet cannot decide the number of the queue now. In the occasion of not enabling the function of vlan shaping, the packet decides the number of the queue according to the trust style of the port (trust cos/trust dscp/trust exp).

9.1.3 Basic QoS Model

VLAN Shaping model includes VLAN, CE, PE and PCN, the following is the basic concept:

VLAN: VLAN in VLAN Shaping means OUTER VLAN. The operators identify different users or business through Outer Vlan Id.

CE (Custom Edge): It is the users' side-edge equipment. The one side supports the uplink port from link to the network of operators and another side supports the downlink port from link to the network of users.

PE (Provider Edge): It is the operators' side-edge equipment. Its uplink port is connected to the network of operators and the downlink port supports the access to the network of users through connecting to the uplink port of CE.

PCN (Provider Core Network): It is the core network of the operators.

A typical application of vlan shaping is that support the specified QoS service for different vlan flow which comes from different users through vlan shaping on the uplink port of PE.

In the figure below, there are voice, data and video in the network. The requirement to the detention and the bandwidth of the network in these three kinds of business is different. The requirement of voice business to the bandwidth is not high, but it is very high to the detention of the network. The requirement to the detention and the bandwidth of the network of video business is high. The requirement to the detention and the bandwidth of the network of the common data is in between. The traditional QOS can support differentiation service for different businesses.

In practical application, the link access that operators support to the users is limited. Multiple users share one uplink access. In the figure bellow, there are two kinds of users and they located in VLAN2-199 and VLAN200-300. These users share one link access to go to the PE through the equipment convergence to CE.

For the operators, supporting different QOS services on the sharing link to different users can protect and utilize the hardware resource existing as much as possible. The operators have not to support different link accesses for different users. They support the relevant QOS with user on every link access. On this sharing link access, the only thing to do is to distinguish which user the flow comes from. Vlan id can sign this kind of users and support QOS on the uplink port of PE.

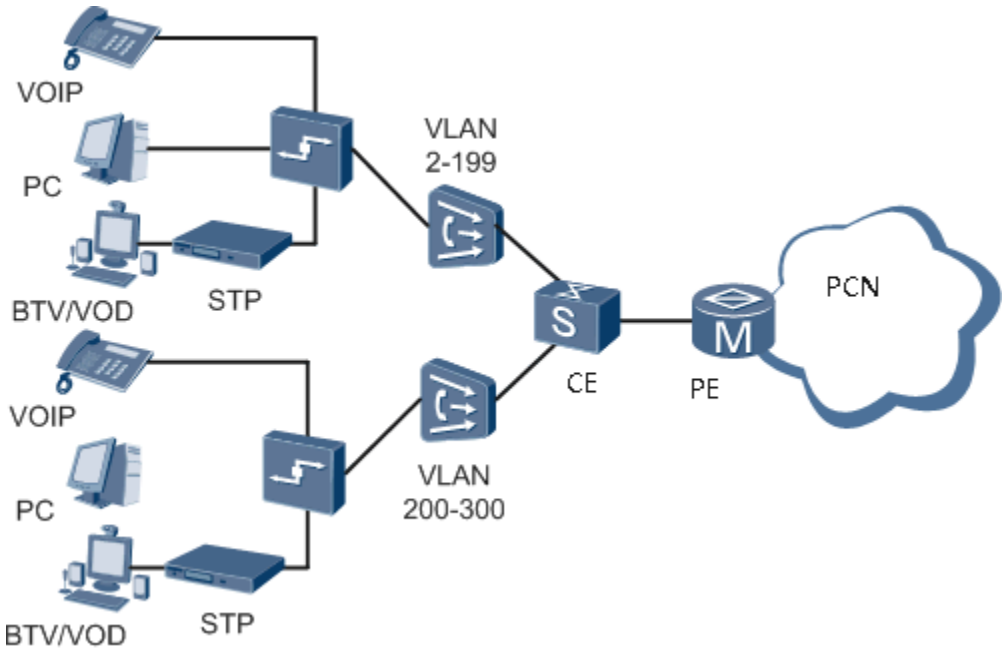


Fig 0-2 the typical application of vlan shaping under the application of multi-user and multi-service

9.2 Vlan-shaping Configuration Task List

The following is the vlan-shaping configuration task list:

Forwarding-class Configuration

Create a forwarding class and it can match different vlan. Then bind different forwarding class to different schedule policy and take different policies to the data flow in this forwarding class. This configuration is required.

Drop-profile Configuration

Create a drop policy to configure the parameters of WRED. This configuration is not required. Before enabling wred or using the parameter of wred, this configuration has not to be configured.

Forwarding- policy Configuration

Create a forwarding policy, it can configure the bandwidth and quote the drop policy. Then it can be binding to the schedule policy with the forwarding class to control the data flow in the forwarding class. This configuration is not required. If this configuration is not be configured, there is not the bandwidth restriction and the parameter of wred is default.

Schedule Policy Configuration

Create a schedule policy, and then map the forwarding class and forwarding policy to every queue of the four nodes of level3. Configure the queue scheduling algorithm and the queue weight. This configuration is required but quoting the forwarding policy is not required. If the forwarding policy is not quoted, there is not the bandwidth restriction and

the parameter of wred is default.

Enable the Function of ets on the Port (Multi-level Scheduling)

Only enable the function of ets on the port, the custom schedule policy can be bond to the port. This configuration is required.

Utilize Vlan-shaping to the Port

Configure the binding policy of the port. Only the policy is bond to the specific port, the policy in this port can be effective. This configuration is required.

1. Forwarding-class Configuration

Command	Explanation
Global Mode	
mls qos forwarding-class <fc-name> [id <fc-id>] **no mls qos forwarding-class <fc-name>**	Create a forwarding class and enter the mode of forwarding class; the **no** command deletes the specified forwarding class.
Forwarding Class Mode	
match s-vid<svid-list> **no match s-vid[svid-list]**	Configure the matching standard of the forwarding class; the data flow can be classified according to vlan-id. The **no** command deletes the specified matching standard.

2. Forwarding-profile Configuration

Command	Explanation
Global Mode	
mls qos forwarding-profile <fp-name> [id <fp-id>] **no mls qos forwarding-profile <fp-name>**	Create a forwarding policy and enter the mode of forwarding policy. The **no** command deletes the specified forwarding policy.
Forwarding Policy Mode	
Bandwidth <minBandwidth> <maxBandwidth> **no bandwidth**	Configure the minimum and the maximum bandwidth in the forwarding policy. The **no** command deletes the bandwidth.
drop <dp-name> **no drop**	Quote the drop policy in the forwarding policy. The **no** command cancels the quotation.

3. Schedule Policy Configuration

Command	Explanation
Global Mode	

mls qos schedule policy <fp-name> **no mls qos schedule policy <fp-name>**	Create a schedule policy and enter the mode of schedule policy; The **no** command deletes the specified schedule policy.
Schedule Policy Mode	
mls qos schedule level <level-id> node <node-id> **no mls qos schedule level <level-id> node <node-id>**	Enter the configuration of schedule node; The **no** command deletes the specified node configuration.
Schedule Node Mode	
mls qos schedule algorithm {sp|wrr|wdrr} **no mls qos schedule algorithm**	Configure the queue scheduling algorithm. For the switch which supports this function, it should configure this command under the mode of S3 schedule node, the default is rr.
mls qos schedule {wrr|wdrr} weight <weight1…weight18> **no mls qos schedule {wrr|wdrr} weight**	Configure the queue weight of vlan shaping. For the switch which supports this function, it should configure this command under the mode of S3 schedule node; the node of S3.1 has 18 queues. The default of wrr is 1, 2, 3 and so on. The default of wdrr is 10, 20, 40, 80, 127, 127, 127 and so on.
mls qos bandwidth <minBandwidth> <maxBandwidth> **no mls qos bandwidth**	Configure the minimum and the maximum bandwidth in the forwarding policy. For the switch which supports this function, it should configure this command under the mode of S3 schedule node. The **no** command deletes the configuration of bandwidth restriction.
mls qos schedule queue <queueID> input forwarding-class <fc-name> [profile <fp-name>] **no mls qos schedule queue <queueID> input forwarding-class <fc-name>**	Configure the input source of the queue of schedule node as forwarding class. And it can assign the forwarding policy for forwarding class selectively. The **no** command deletes the binding

	configuration.

4. Drop Policy

Command	Explanation
Global Mode	
mls qos drop-profile <dp-name> [id <dp-id>] **no mls qos drop-profile <dp-name>**	Create the drop policy and enter the mode of drop policy. The no command deletes the specified drop policy.
Drop Policy Mode	
dp <dp> drop-startpoint <start> drop-endpoint <end> max-drop-rate <rate> **no dp [dp]**	Configure the parameter of wred in the drop policy including type of color, minimum value, maximum value and the maximum drop probability. The **no** command deletes the configuration of color and return to the default.

5. Show the Information of Vlan-shaping Configuration

Command	Explanation
Global Mode	
show mls qos vlan shaping capable ports	Show all the names of the ports which support vlan shaping now.
show mls qos forwarding-class [fc-name]	Show the information of the specified forwarding class.
show mls qos drop-profile [dp-name]	Show the information of the specified drop policy.
Show mls qos forwarding-profile [fp-name]	Show the information of the specified forwarding policy.
show mls qos schedule interface [<interface-name>|<interface-list>]	Show the information of vlan shaping on the specified port including the queue scheduling algorithm of vlan shaping, the weight of the queue and so on. The information of S3 shows the information of the queue of vlan shaping.

9.3 Vlan-shaping Examples

Case1:

Create the forwarding class of fc1 and fc2, configure the matching rules as vlan1, vlan2, vlan3 and vlan4 flow. Create the drop policy of dp1 and configure it. For the packet whose drop priority is 0, it begins to drop packets when the queue length is up to 20% of the maximum length. It begins to drop packets in full speed when the queue length is up to 40% of the maximum length, but the drop packets account for the proportion of all packets to be 80%. Create the forwarding policy of fp1, its minimum bandwidth pledge is 10kbps and its maximum bandwidth restriction is 200kbps. Associate the forwarding policy to the drop policy of dp1. Create the scheduling policy of p1 and configure its first queue's inputting source of node of S3.1 as fc1, associate it to the forwarding policy of fp1. Configure its second queue's inputting source of node of S3.1 as fc2. Configure the minimum bandwidth pledge is 64kbps and its maximum bandwidth restriction is 256kbps of node of S3.1 of vlan-shaping queue. Configure the wrr queue's weights of vlan-shaping queue of 1 to 8 as 1, 3, 5, 2, 7, 4, 9, 14. And configure the wrr queue's weights of vlan-shaping queue of 9 to 18 as 8, 3, 2, 14, 17, 4, 7, 0, 0, 0. At last, bind p1 to the port of ethernet1/0/1.

Case Configuration:

(config)#mls qos forwarding-class fc1

(config-forwarding-class-fc1)#match vlan 1-2

(config-forwarding-class-fc1)#exit

(config)#mls qos forwarding-class fc2

(config-forwarding-class-fc1)#match vlan 3-4

(config-forwarding-class-fc1)#exit

(config)# mls qos drop-profile dp1

(config-drop-profile-dp1)# dp 0 drop-startpoint 20 drop-endpoint 40 max-drop-rate 80

(config-drop-profile-dp1)#exit

(config)#mls qos forwarding-policy fp1

(config-forwarding-policy-fp1)# bandwidth 10 200

(config-forwarding-policy-fp1)#drop dp1

(config-forwarding-policy-fp1)#exit

(config)#mls qos schedule policy p1

(config-schedule-policy-p1)#mls qos schedule level 3 node 1

(config-schedule-policy-p1-lel3nod1)#mls qos schedule queue 3 input forwarding-class fc1 profile fp1

(config-schedule-policy-p1-lel3nod1)#mls qos schedule queue 4 input forwarding-class fc2

(config-schedule-policy-p1-lel3nod1)#mls qos bandwidth 64 256

(config-schedule-policy-p1-lel3nod1)#mls qos schedule algorithm wrr

(config-schedule-policy-p1-lel3nod1)#mls qos schedule wrr weight 1 3 5 2 7 4 9 14 8 3 2 14 17 4 7 0 0 0

(config-schedule-policy-p1-lel3nod1)#exit

(config-schedule-policy-p1)#exit

(config)#interface ethernet1/0/1

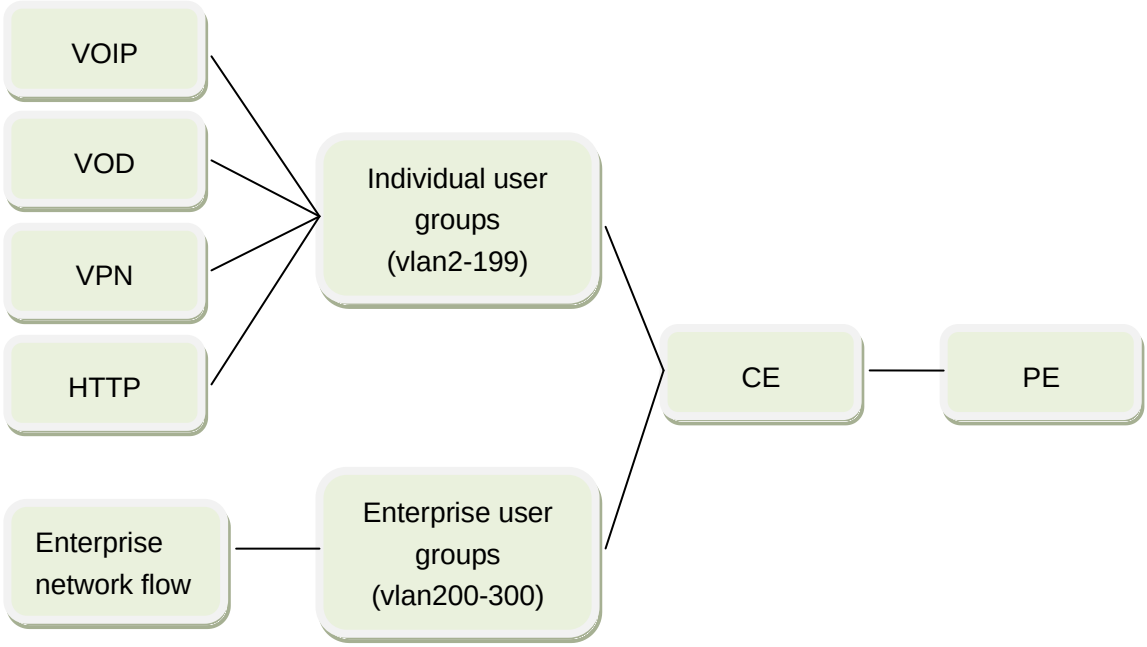
(config-if-ethernet1/0/1)#mls qos ets enable

(config-if-ethernet1/0/1)#mls qos schedule policy bind p1

Configuration Result:

Enable the function of vlan-shaping in global; the egress of ethernet1/0/1 is bond to p1 of vlan-shaping. When the flow of entering ethernet1/0/1 exceeds the load line and happens to the congestion, the flow of vlan1,2 will enter to level 3 node 1 queue 3 to schedule and the flow of vlan3, 4 will enter to level 3 node 1 queue 4 to schedule. The minimum bandwidth of queue3, 4 which participate the vlan-shaping scheduling is 64kbs and the maximum is 256kbs. The minimum bandwidth of queue3 is 10kbs and the maximum is 200kbs. Queue3, 4 do the schedule according to the wrr algorithm and the proportion of the out flow is 5:2. For the packet whose drop priority is 0 in queue3, it begins to drop packets when the queue length is up to 20% of the maximum length. It begins to drop packets in full speed when the queue length is up to 40% of the maximum length, but the drop packets account for the proportion of all packets to be 80%.

Case2:



In the group network of service-vlan, the users who access the WAN can be divided to individual user and enterprise user. The individual users' business types are consistent

and the flow management requirements are consistent too. The enterprise users' business types are different and it requires distinguishing that different enterprise users do different flow management.

Items	Requirement content
the flow policy of individual user groups	The range of service vlan id which carries individual user groups of A is 100 to 299; The individual business can be divided to four kinds: ①VoIP business: The priority of 802.1p is 6 and 7, the minimum bandwidth of the flow whose priority is 6 is 20M, and it is 30M for 7 ②Vod business: The priority of 802.1p is 4 and 5. ③VPN business: The priority of 802.1p is 2 and 3. ④http browsing business: the priority of 802.1p is 0 and 1. ⑤Schedule VoIP business in priority. For the enterprise network flow, Vod, VPN and http business, they can be scheduled according to the proportion of 4:3:2:1.
the flow policy of enterprise user groups	The range of service vlan id which carries enterprise user groups is 500 to 506; Because there are two groups of enterprise users, the two groups' different service vlan carry different enterprise users. ①Enterprise users of group A: The range of service vlan id is 501 to 503. ② Enterprise users of group B: The range of service vlan id is 504 to 506. ③ The whole flow requirement of enterprise user groups: The speed limit is 100M; the minimum bandwidth is 50M. ④When scheduling the flow of group A and group B, the proportion is 2:1.

Configuration Thinking:

①Put the enterprise user data into the vlan shaping queues and put the individual user data into the common cos queues. The enterprise users decide the queue number according to vlan id and the individual users decide the queue number according to the priority.

②The individual user data can schedule through S2 and the enterprise user data can schedule through S3.1. the output of S3.1 can be put on S2 for scheduling.

③The queue numbers of VoIP, Vod, VPN and http on S2.2 should be decided according to the priority of 802.1p. So the queue numbers of VoIP are 6 and 7; the queue numbers of Vod are 4 and 5; the queue numbers of VPN are 2 and 3; the queue numbers of http are 0 and 1.

④The flow of VoIP is scheduled for priority and then the flow of Vod, VPN, http and enterprise network are scheduled by the proportion of 3: 2: 1: 4. So put the output of S3.1 and VoIP, VPN, http onto S2.2 to schedule according to WRR. Because S2.2 can support 8 queues at most, the flow of VoIP cannot be put onto S2.2 but can be put onto S2.3 only. Then configure S1 to schedule according to SP, it can ensure that the flow of VoIP can schedule for priority.

⑤There are two groups of enterprise users of A and B. Because there is no differentiation service need of enterprise user in the group, it just need to construct two vlan shaping queues and match them with Vlan501~503 and Vlan504~506 respectively.

⑥A and B do the scheduling as the proportion of 2: 1. So the scheduling algorithm of S3.1 should be configured to be WRR. The queue weight of A is 2 and it is 1 for B.

⑦Because the whole flow requirement of enterprise user groups is 100M for the maximum bandwidth and it is 50M for the minimum bandwidth, it is equivalent to configure the overall minimum and maximum bandwidth of S3.1 as 50M and 100M respectively.

⑧VoIP business has the minimum and maximum bandwidth demand. It is equivalent to configure the minimum and maximum bandwidth for the corresponding queue 6 and 7.

Configuration Steps:

①Configure the minimum and maximum bandwidth demand of VoIP business firstly.

(config)#interface ethernet1/0/1

(config-if-ethernet1/0/1)#mls qos queue 6 bandwidth 20000 0

(config-if-ethernet1/0/1)#mls qos queue 7 bandwidth 0 30000

②Construct two forwarding class and match them with vlan id501～503 and vlan id504～506 respectively.

(config)#mls qos forwarding-class enterpriseA

(config-forwarding-class-enterpriseA)#match s-vid 501-503

(config-forwarding-class-enterpriseA)#exit

(config)#mls qos forwarding-class enterpriseB

(config-forwarding-class-enterpriseB)#match s-vid 504-506

③Create the scheduling policy of p1 and configure the scheduling manner of S1.1 as SP.

(config)#mls qos schedule policy p1

(config-schedule-policy-p1)#mls qos schedule level 1 node 1

(config-schedule-policy-p1-lel1nod1)#mls qos schedule algorithm sp

④Configure the scheduling algorithm of vlan shaping as wrr. The weight of the first vlan shaping queue is 2 and it is 1 for the second queue. Please pay attention that the first and second queues of S3 are not the vlan shaping queues in the switch, from the third, they are vlan shaping queues.

(config-schedule-policy-p1)#mls qos schedule level 3 node 1

(config-schedule-policy-p1-lel3nod1)#mls qos schedule algorithm wrr

(config-schedule-policy-p1-lel3nod1)#mls qos schedule wrr weight 0 0 2 1

⑤Configure the input source of vlan shaping queue. The input source of the first vlan shaping queue is the forwarding class of enterpriseA and the input source of the second is enterpriseB.

(config-schedule-policy-p1-lel3nod1)#mls qos schedule queue 3 input forwarding-class enterpriseA

(config-schedule-policy-p1-lel3nod1)#mls qos schedule queue 4 input forwarding-class enterpriseB

⑥Configure the overall minimum bandwidth of vlan shaping scheduling node as 50M and the maximum is 100M.

(config-schedule-policy-p1-le3nod1)#mls qos bandwidth 50000 100000

⑦Configure the input source of S2.2 as user business and enterprise data. Among of them, the user business is decided the queue numbers according to the priority of 802.1p.

(config-schedule-policy-p1)#mls qos schedule level 2 node 2

(config-schedule-policy-p1-lel2nod2)#mls qos schedule queue 1 input uc 1

(config-schedule-policy-p1-lel2nod2)#mls qos schedule queue 2 input uc 2

(config-schedule-policy-p1-lel2nod2)#mls qos schedule queue 3 input uc 3

(config-schedule-policy-p1-lel2nod2)#mls qos schedule queue 4 input uc 4

(config-schedule-policy-p1-lel2nod2)#mls qos schedule queue 5 input uc 5

(config-schedule-policy-p1-lel2nod2)#mls qos schedule queue 6 input uc 6

(config-schedule-policy-p1-lel2nod2)#mls qos schedule queue 7 input node 1

⑧Configure the scheduling algorithm of S2.2 as wr and configure the corresponding queue weight.

(config-schedule-policy-p1-lel2nod2)#mls qos schedule algorithm wrr

(config-schedule-policy-p1-lel2nod2)#mls qos schedule wrr weight 1 1 2 2 3 3 4

⑨Configure the input source of S2.3 as VoIP.

(config-schedule-policy-p1)#mls qos schedule queue 1 input uc 7

(config-schedule-policy-p1)#mls qos schedule queue 2 input uc 8

⑩Bind the scheduling policy of p1 to the port of 1/0/1

(config)#interface ethernet1/0/1

(config-if-ethernet1/0/1)#mls qos ets enable

(config-if-ethernet1/0/1)#mls qos schedule policy bind p1

9.4 Vlan-shaping Troubleshooting

When the effect of the actual flow scheduling does not meet the actual user configuration, the following is the possible problems and the solutions under the premise that the hardware and the cable do not have problems:

1. Make sure that the function of vlan-shaping has been bond to the egress port. The relevant flow will transport according to the relevant queue of vlan-shaping after binding. Otherwise, the general QoS schedule will be conducted according to cos of the flow.
2. Confirm if the flow had been congestion, otherwise, the actual effect may not meet the configuration.
3. Confirm if vlan will be matched to the forwarding class and bond to the schedule policy.
4. The function of vlan shaping is only effective to the unicast packet known; it is not effective to the broadcast packet, multicast packet and the unicast packet unknown.