Configuring Quality of Service and ACL

Overview of Quality of Service and ACL

Typically, networks operate on a best-effort delivery basis. By enabling the Quality of Service feature, you can provide preferential treatment to certain types of traffic using the congestion-management and congestion-avoidance techniques. Quality of Service (QoS) allows you to classify your network traffic, police and prioritize traffic flow, and provide congestion avoidance. You can configure QoS on physical ports and on switch virtual interfaces (SVIs).

To implement QoS, the device must perform the following tasks:

- Classify the traffic: Distinguish packets or flows from one another.
- Assign a label: Indicate the given QoS as the packets move through the device.
- Police and mark the traffic: Make the packets comply with the configured resource usage limits.
- Queue and schedule traffic: Provide a different treatment in all those situations where resource contentions exist.
- Shape traffic: Ensure that traffic sent from the device meets a specific traffic profile.

With QoS enabled, an Ethernet switching device uses Ethernet QoS technology to provide different levels of QoS guarantees to support traffic flows that have higher delay and jitter requirements.

Access control list (ACL) contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions that a packet must meet in order to match the ACEs. When an interface receives a packet, the device tests the packet against the conditions in the ACL. The first match decides whether the device accepts or rejects the packet. The device stops testing after the first match.

Combining QoS and ACL associates traffic rules with traffic operations that use ACL. You can perform QoS functions, such as, packet filtering, commit access rate, traffic mirroring, traffic redirection, and so on, by referencing an ACL.

Traffic Classification Based on QoS and ACL

Classification is the process of distinguishing one type of traffic from another by examining the fields in a packet.

You can use Standard, Extended, or Layer 2 ACL to define a group of packets with the same characteristics (class). After a traffic class is defined with an ACL, you can attach a policy to it. A policy contains multiple classes with actions that are specified for each one of them. A policy can also include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to the port on which it becomes effective.

Prioritization in Layer 2 Frames

Each host that supports IEEE 802.1Q protocol adds a 4-byte 802.1Q tag header to the source address when sending packets. A 3-bit priority field is a part of this 4-byte header. These three bits indicate the priority of the frame; this determines which packet is sent first when the device is blocked. There are eight priorities that range from 0 to 7.

Table 1: IEEE 802.1Q PRI Field Values

Class of Service (Decimal)	Class of Service (Binary)	Meaning
0	000	Spare
1	001	Background
2	010	Best effort
3	011	Excellent effort
4	100	Controlled load
5	101	Video
6	110	Voice
7	111	Network management

Prioritization in Layer 3 Packets

Layer 3 IP packets carry the classification information in the type of service (ToS) field that has eight bits. The ToS field carries either an IP precedence value or a Differentiated Services Code Point (DSCP) value. IP precedence values range from 0 to 7. DSCP values range from 0 to 63. Based on DSCP or IP precedence, traffic is put into particular service class. Packets within a service class are treated the same way.

If an IP precedence value is used, a 1-byte ToS field consists of three bits of IP precedence and four bits of ToS, and one unused bit. Four bits of ToS field represent minimum latency, maximum throughput, maximum reliability, and, minimal cost. If all the four bits are zero, the service is a general service.

Table 2: IP Precedence Values

IP Precedence（Decimal）	IP Precedence（Binary）	Meaning
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash override
5	101	Critical
6	110	Internet
7	111	Network

Differentiated Services, which is defined in RFC 2474, increases the number of definable priority levels. The Differenciated Services field in a packet makes per-hop behavior decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing.

In a Differenciated Services field, the first six bits (0 to 5) of a ToS field represent DSCP. The Differentiated Services network defines the following four types of traffic:

- Expedited Forwarding (EF) class, which is applicable to low-delay, low-loss, low-jitter, and bandwidth-priority services (such as virtual leased lines), regardless of whether other traffic share its link.
- Assured Forwarding (AF) class, which is divided into four subcategories (AF1, AF2, AF3, AF4). Each AF class is divided into three drop precedence, which is used to classify the AF business. An AF class has a lower QoS level than an EF class.
- Class Selector (CS) evolves from the IP ToS field, which has a total of eight categories.
- Best Effort (BE) is a special category of CS, and there is no guarantee. An AF class is downgraded to BE class after overrun. The existing IP network traffic is also defaulted to this category.

Table 3: DSCP Values

DSCP（Decimal）	DSCP（Decimal）	Meaning
0	000000	BE
46	101110	EF
10	001010	AF1
18	010010	AF2
26	011010	AF3
34	100010	AF4

DSCP（Decimal）	DSCP（Decimal）	Meaning
8	001000	CS1
16	010000	CS2
24	011000	CS3
32	100000	CS4
40	101000	CS5
48	110000	CS6
56	111000	CS7

Configure Quality of Service and ACL

The following sections provide information about the various tasks involved in configuring QoS and ACL.

Configure Traffic Speed Limit

You can monitor the rate of traffic that enters a switch. If the traffic rate exceeds a configured threshold, you can define policies to take suitable measures.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**rate-limit input** { [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } **[subitem** *subitem*]] } *target-rate* **Example:** `Device(config)# rate-limit input ip-group 4 100`	(Optional) Sets the traffic rate limit. Some devices support traffic only in the inbound direction. Some other devices support both inbound and outbound traffic.

Configure Message Redirection

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**traffic-redirect** { [**ip-group {** *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] } { [**interface** *interface-num* | **cpu**] } **Example:** `Device(config)# traffic-redirect link-group link1 interface ethenet0/1`	(Optional) Sets an instruction to forward the messages to an egress port.

Copy Messages to a CPU

You can copy specific messages that are defined by the ACL rule to a CPU.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**traffic-copy-to-cpu** { [**ip-group** { *num* | *name*} [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] } **Example:** `Device(config)# traffic-copy-to-cpu ip-group 3`	Copies the packets that match an ACL rule to a CPU.

Configure Traffic Statistics

You can get the statistics of the packets that match an ACL rule on the specified ports, in terms of packet numbers and bytes.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**traffic-statistic** { [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]] } **Example:**	(Optional) Configures the device to collect traffic statistics. This command displays a cumulative value of the count of the number of packets that match the ACL rule.

	Command or Action	Purpose
	`Device# traffic-statistic ip-group 4`	If you reconfigure traffic statistics, the packet count information is lost.
Step 3	**clear traffic-statistic** { [**all** | [**ip-group** { *num* | *name* } [**subitem** *subitem*]] [**link-group** { *num* | *name* } [**subitem** *subitem*]]] } **Example:** `Device# clear traffic-statistic all`	(Optional) Clears the traffic statistics information.

Display Quality of Service and ACL Configurations

Use the following **show** commands to view the QoS and ACL configurations and perform maintenance operations.

Table 4: QoS and ACL show Commands

Command	Operation
show qos-info all	Displays all parameters of QoS that are set for a device.
show qos-info statistic	Displays the total number of rules that are configured for each QoS parameter.
show qos-info traffic-copy-to-cpu	Displays the parameter settings for copying the messages to a CPU.
show qos-info mirrored-to	Displays the ports to which the messages are copied.
show qos-info traffic-priority	Displays the parameters that are configured for priority marking of the packets that match an ACL rule.
show qos-info traffic-redirect	Displays the parameters that are configured for redirecting the packets that match an ACL rule.
show qos-info traffic-statistic	Displays the statistics for the QoS traffic.
show qos-interface all	Displays the configurations of rate limit on a port.
show qos-interface rate-limit	Displays the rate-limit configuration information of all ports.
show qos-interface statistic	Displays all the rules for rate limit that are set on a device.

Example: Configuring Quality of Service and ACL

Consider a network topology where device A and device B are connected by an Ethernet switch, which is in turn connected to the internet. A and B do not belong to the same network segment. A connects to the switch through its Ethernet port e1/1, and B connects to the switch through its Ethernet port e1/2.

The following example shows how you can redirect traffic through port e1/1 using HTTP to access internet through e1/2:

```
Device# configure terminal
Device(config)# time-range a
Device(config-timerange-a)# periodic weekdays daily 08:30:00 to 18:00:00
Device(config-timerange-a)# exit

Device(config)# time-range b
Device(config-timerange-b)# periodic weekdays 00:00:00 to 08:30:00
Device(config-timerange-b)# periodic weekend 00:00:00 to 23:59:00
Device(config-timerange-b)# exit
```

The following example shows to configure an ACL to access the internet using HTTP message classification at different time periods:

```
Device(config)# access-list 100 permit tcp any 192.168.0.1 0 80 time-range a
Device(config)# access-list 100 permit tcp any 192.168.0.1 0 80 time-range b
```