DES-7200

ACL&QoS Command Reference Guide

Version 10.4(3)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.4(3)

Date:

Copyright Statement

D-Link Corporation ©2011

All rights reserved.

Without our written permission, this document may not be excerpted, reproduced, transmitted, or otherwise in all or in part by any party in any means.

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

📖 Network engineers

📖 Technical salespersons

📖 Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 ACL Configuration Commands

For IDs used in the following commands, refer to the command ID table below:

ID	Meaning
ID	Number of access list. Range: Standard IP ACL: 1 to 99, 1300 to 1999 Extended IP ACL: 100 to 199,2000 to 2699 Extended MAC ACL: 700 to 799 Extended expert ACL: 2700 to 2899
name	ACL name
sn	ACL SN (products can be set according to the priority)
start-sn	Start sequence number
inc-sn	Sequence number increment
deny	If matched, access is denied.
permit	If matched, access is permitted.
port	Protocol number. For IPv6, this field can be IPv6, icmp, tcp, udp and numbers 0 to 255. For IPv4, it can be one of eigrp, gre, ipinip, igmp, nos, ospf, icmp, udp, tcp, and ip, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as icmp/tcp/udp, are listed individually.
interface *idx*	Interface index
src	Packet source IP address (host address or network address)
src-wildcard	Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32.
src-ipv6-pfix	Source IPv6 network address or network type
dst-ipv6-pfix	Destination IPv6 network address or network type
pfix-len	Prefix mask length
src-ipv6-addr	Source IPv6 address
dst-ipv6-addr	Destination IPv6 address
dscp	Differential service code point, and code point value. Range:

ID	Meaning
	0 to 63
flow-label	Flow label in the range 0 to 1048575
dst	Packet destination IP address (host address or network address)
dst-wildcard	Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32
fragment	Packet fragment filtering. Note: Routers do not support the packet fragment filtering.
precedence	Packet precedence value (0 to 7)
range	The layer 4 port number range of the packet.
time-range *tm-rng-name*	Time range of packet filtering, named *tm-rng-name*
tos	Type of service (0 to 15)
cos	Class of service (0-7)
cos inner *cos*	COS of the packet tag
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name (0 to 255)
operator port[*port*]	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range) *port* indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number
src-mac-addr	Physical address of the source host
dst-mac-addr	Physical address of the destination host
VID vid	VLAN ID
VID inner vid	VID of the tag
ethernet-type	Ethernet protocol type. 0x value can be entered.
match-all *tcpf*	Match all bits of the TCP flag.
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface

ID	Meaning
{*rule mask offset*}$^{+}$	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table "+" sign indicates at least one group

The fields in the packet are as follows:

```
AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD
DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM
NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT
UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb
```

The corresponding offset table is as follows:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol number	35
C	Data frame length field	12	Q	IP check sum	36
D	VLAN tag field	14	R	Source IP address	38
E	DSAP (Destination Service Access Point) field	18	S	Destination IP address	42
F	SSAP (Source Service Access Point) field	19	T	TCP soure port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version number	26	XY	IP header length and reserved bits	58

Letter	Meaning	Offset	Letter	Meaning	Offset
K	TOS field	27	Z	Resrved bits and flags bit	59
L	Length of IP packet	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

The offsets of fields in the above table are their offsets in 802.3 data frames of SNAP+tag.

1.1 Configuration Related Commands

1.1.1 access-list

Use this command to create an access list rule to filter data packets. The **no** form of this command deletes the specified access list entries.

1. Standard IP access list (1 to 99, 1300 to 1999)

   access-list *id* {**deny** | **permit**} {*source source-wildcard* | **host** *source* | **any| interface** *idx*} [**time-range** *tm-range-name*]

2. Extended IP access list (100 to 199, 2000 to 2699)

   access-list *id* {**deny** | **permit**} **protocol** {*source source-wildcard* | **host** *source* | **any| interface** *idx* } {*destination destination-wildcard* | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

3. Extended MAC access list (700 to 799)

   access-list *id* {**deny** | **permit**} {**any** | **host** *source-mac-address*} {**any** | **host** *destination-mac-address*} [*ethernet-type*][**cos** [*out*][**inner** *in*]]

4. Extended expert access list (2700 to 2899)

   access-list *id* {**deny** | **permit**} [**protocol** | [*ethernet-type*][**cos** [*out*][**inner** *in*]]] [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**}][**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- When you select the Ethernet-type field or cos field:

  access-list *id* {**deny** | **permit**} {*ethernet-type*| **cos** [*out*][**inner** *in*]} [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host**

destination | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

  access-list *id* {deny | permit} **protocol [VID** [*out*][**inne**r *in*]] {**source**

  source-wildcard | host *source* | **any**} {**host** *source-mac-address* | **any** }

  {destination *destination-wildcard* | **host** *destination* | **any} {host**

  destination-mac-address | **any} [precedence** *precedence*] [**tos** *tos*]

  [fragment] [**range** *lower upper*] **[time-range** *time-range-name*]

  Extended expert ACLs of some important protocols:

  Internet Control Message Protocol (ICMP)

  access-list *id* {**deny** | **permit**} **icmp** [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host**

  destination-mac-address | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]]

  | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**]

  [**time-range** *time-range-name*]

  Transmission Control Protocol (TCP)

  access-list *id* {**deny** | **permit**} **tcp** [**VID** [*out*][**inner** *in*]]{**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [**operator** port [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

  User Datagram Protocol (UDP)

  access-list *id* {**deny** | **permit**} **udp**[**VID** [*out*][**inner** *in*]] {**source** *source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [**operator port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**}{**host** *destination-mac-address* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

5. List remark

access-list *id* **list-remark** *text*

The following parameters are described in the sequence they appear. Once described, a parameter will not be described anymore.

Parameter description

Parameter	Description
id	Access list ID. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.
deny	If not matched, access is denied.
permit	If matched, access is permitted.
source	Specify the source IP address (host address or network address).
source-wildcard	It can be discontinuous, for example, 0.255.0.32.
protocol	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
destination	Specify the destination IP address (host address or network address).
destination-wildcard	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
fragment	Packet fragment filtering
precedence	Specify the packet priority.
precedence	Packet precedence value (0 to 7)
range	Layer4 port number range of the packet.
lower	Lower limit of the layer4 port number.
upper	Upper limit of the layer4 port number.
time-range	Time range of packet filtering

time-range-name	Time range name of packet filtering
tos	Specify type of service.
tos	ToS value (0 to 15)
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name
operator	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)
port [*port*]	Port number; *range* needs two port numbers, while other operators only need one port number.
host *source-mac-address*	Source physical address
host *destination-mac-address*	Destination physical address
VID *vid*	Match the specified VID.
ethernet-type	Ethernet type
match-all	Match all the bits of the TCP flag.
tcp-flag	Match the TCP flag.
text	Remark information

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

To filter the data by using the access control list, you must first define a series of rule statements by using the access list. You can use ACLs of the appropriate types according to the security needs:

The standard IP ACL (1 to 99, 1300 to 1999) only controls the source IP addresses.

The extended IP ACL (100 to 199, 2000 to 2699) can enforce strict control over the source and destination IP addresses.

The extended MAC ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type.

The extended expert access list (2700 to 2899) is a combination of the above and can match and filter the VLAN ID.

For the layer3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: **precedence** *precedence*/**tos** *tos*/**fragments**/**range** *lower upper*/**time-range** *time-range-name*

The TCP Flag includes part or all of the following:

- **urg**
- **ack**
- **psh**
- **rst**
- **syn**
- **fin**

The packet precedence is as below:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The service types are as below:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The ICMP message types are as below:

- **administratively-prohibited**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **fragment-time-exceeded**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **redirect**
- **device-advertisement**
- **device-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **ttl-exceeded**
- **unreachable**

The TCP ports are as follows. A port can be specified by port name and port number:

- **bgp**
- **chargen**
- **cmd**
- **daytime**
- **discard**
- **domain**
- **echo**
- **exec**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **ident**
- **irc**
- **klogin**
- **kshell**
- **ldp**
- **login**
- **nntp**
- **pim-auto-rp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- **biff**
- **bootpc**

- **bootps**
- **discard**
- **dnsix**
- **domain**
- **echo**
- **isakmp**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **netbios-ss**
- **ntp**
- **pim-auto-rp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

The Ethernet types are as below:

- **aarp**
- **appletalk**
- **decnet-iv**
- **diagnostic**
- **etype-6000**
- **etype-8042**
- **lat**
- **lavc-sca**
- **mop-console**
- **mop-dump**
- **mumps**
- **netbios**
- **vines-echo**
- **xns-idp**

Examples

1. Example of the standard IP ACL

The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

```
DES-7200 (config)#access-list 1 permit 192.168.1.64 0.0.0.63
```

2. Example of the extended IP ACL

The following extended IP ACL allows the DNS messages and ICMP messages to pass:

```
DES-7200(config)#access-list 102 permit tcp any any eq domain
DES-7200(config)#access-list 102 permit udp any any eq domain
DES-7200(config)#access-list 102 permit icmp any any echo
DES-7200(config)#access-list 102 permit icmp any any echo-reply
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 1/1. The configuration procedure is as below:

```
DES-7200(config)#access-list 702 deny host 00d0f8000c0c any aarp
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
DES-7200(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
DES-7200(config)# access-list 2702 permit any any any any
DES-7200(config)# show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.12.3 mac 00d0.f800.0044 any any
10 permit any any any any
```

Related commands

Command	Description
show access-lists	Show all the ACLs.

	mac access-group	Apply the extended MAC ACL on the interface.

1.1.2 deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

Use this command to set deny rules

1. Standard IP ACL

   [*sn*] **deny** {*source source-wildcard* | **host** *source* | **any| interface** *idx* }[**time-range** *tm-range-name*]

2. Extended IP ACL

   [*sn*] **deny protocol source** *source-wildcard* **destination** *destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragment**]

   [**range** *lower upper*] [**time-range** *time-range-name*]

Extended IP ACLs of some important protocols:

- **Internet Control Message Prot** (ICMP)

  [*sn*] **deny icmp** {**source** *source-wildcard* | **host** *source* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Prot** (TCP)

  [*sn*] **deny tcp** {**source** *source-wildcard* | **host** *Source* | **any**} [*operator*

  port [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Prot** (UDP)

  [*sn*] deny udp {**source** *source –wildcard* | **host** *source* | **any**} [*operator*

  port [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

3. Extended MAC ACL

[*sn*] **deny** {**any** | **host** *source-mac-address*}{**any** | **host** *destination-mac-address*} [*ethernet-type*][**cos** [*out*] [**inner** *in*]]

4. Extended expert ACL

[*sn*] **deny**[**protocol** | [*ethernet-type][* **cos** [*out*] [**inner** *in*]*]*] [[**VID** [*out*][**inner** *in*]]] {**source** *source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*][**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- When you select the ethernet-type field or cos field::

sn] **deny** {[*ethernet-type}[***cos** [*out*] [**inner** *in*]*]}* [[**VID** [*out*][**inner** *in*]]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

[*sn*] **deny protocol** [[**VID** [*out*][**inner** *in*]]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination**

destination-wildcard | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

[*sn*] **deny icmp** [[**VID** [*out*][**inner** *in*]]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

[*sn*] **deny tcp** [[**VID** [*out*][**inner** *in*]]]{**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

[*sn*] **deny udp** [[**VID** [*out*][**inner** *in*]]]{**source** *source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**}{**host**

destination-mac-address | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- **Address Resolution Protocol (ARP)**

  [*sn*] **deny arp** {**vid** *vlan-id*}[*source-mac-address source-wildcard* **|host** *source-mac-address* | **any**] [**host** *destination –mac-address* | **any**] {*sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any**} {*sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any**} {*target-ip target-ip–wildcard* | **host** *target-ip* | **any**}

5. Extended IPv6 ACL

[*sn*] **deny protocol**{*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} {*destination-ipv6-prefix / prefix-length* | **any** | *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended ipv6 ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

  [*sn*]**deny icmp** {*source-ipv6-prefix / prefix-length* | *any source-ipv6-address* | **host**} {*destination-ipv6-prefix / prefix-length* | **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** flow-label] [**fragment**] [**time-range** time-range-name]

- **Transmission Control Protocol** (TCP)

  [*sn*] **deny tcp** {*source-ipv6-prefix / prefix-length* | **host** *source-ipv6-address* | **any**}[*operator* **port**[*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

  [sn] **deny udp** {*source-ipv6-prefix/prefix-length* | **host** *source-ipv6-address* | **any**} [*operator* **port** [*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**}[*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

  For the parameters that are not mentioned below, please refer to the **access-list.**

Parameter description

Parameter	Description
sn	ACL entry sequence number
source-ipv6-prefix	Source IPv6 network address or network type
destination-ipv6-prefix	Destination IPv6 network address or network type
prefix-length	Prefix mask length
source-ipv6-address	Source IPv6 address
destination-ipv6-address	Destination IPv6 address
dscp	Differential Service Code Point
dscp	Code value, within the range of 0 to 63
flow-label	Flow label
flow-label	Flow label value, within the range of 0 to 1048575.
protocol	For the IPv6, the field can be ipv6 | icmp | tcp | udp and number in the range 0 to 255
time-range	Time range of the packet filtering
time-range-name	Time range name of the packet filtering

Default configuration

N/A.

Command mode

ACL configuration mode.

Usage guidelines

N/A.

Examples

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
DES-7200(config)#expert access-list extended 2702
DES-7200(config-exp-nacl)#deny tcp  host  192.168.4.12
host 0013.0049.8272 any any
DES-7200(config-exp-nacl)#permit any any any any
DES-7200(config-exp-nacl)#show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.4.12 host 0013.0049.8272 any
any
20 permit any any any any
DES-7200(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)# ip access-list extended ip-ext-acl
DES-7200(config-ext-nacl)# deny tcp host 192.168.4.12 eq
100 any
DES-7200(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
DES-7200(config-ext-nacl)#exit
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)#ip access-group ip-ext-acl in
DES-7200(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#mac access-list extended mac1
DES-7200(config-mac-nacl)#deny host 0013.0049.8272 any
aarp
DES-7200(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
DES-7200(config-mac-nacl)#exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mac access-group mac1 in
```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#ip access-list standard 34
```

```
DES-7200(config-ext-nacl)# deny host 192.168.4.12
DES-7200(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
DES-7200(config-ext-nacl)#exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# ip access-group 34 in
```

This example shows how to use the extended IPV6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#ipv6 access-list extended v6-acl
DES-7200(config-ipv6-nacl)#11 deny ipv6 host
192.168.4.12 any
DES-7200(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
DES-7200(config-ipv6-nacl)# exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# ipv6 traffic-filter v6-acl in
```

Related commands

Command	Description
show access-list	Show all the ACLs.
ipv6 traffic-filter	Apply the extended ipv6 ACL on the interface.
ip access-group	Apply the IP ACL on the interface.
match access-group	Apply the extended MAC ACL on the interface.
ip access-list	Define the IP ACL.
mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.
permit	Permit the access.

1.1.3 expert access-group

Use this command to apply the specified expert ACL on the specified interface. Use the **no** form of the command to remove the application.

expert access-group {*id*|*name*} {**in**|**out**}

no expert access-group {*id*|*name*} {**in**|**out**}

		Parameter	Description
Parameter description		*id*	ID of the expert ACL (2700 to 2899)
		name	Name of the expert ACL
		in	Filter the inputting packets of the interface
		out	Filter the outputting packets of the interface

Default configuration	No Expert ACL is applied on the interface.
Command mode	Interface configuration mode.
Usage guidelines	N/A.

Examples

The following example shows how to apply the **access-list *accept*_**00d0f8xxxxxx only to Gigabit interface 1:

```
DES-7200(config)# interface GigaEthernet 0/1
DES-7200(config-if)# expert access-group
accept_00d0f8xxxxxx_only in
```

Related commands

Command	Description
show access-group	Show the ACL configuration.

Platform description -

1.1.4 expert access-list

Use this command to create an extended expert ACL. Use the **no** form of the command to remove the ACL.

expert access-list extended {*id* | *name*}

no expert access-list extended {*id* | *name*}

Parameter description

Parameter	Description
id	ID of the extended expert ACL (2700 to 2899)
name	Name of the extended expert ACL

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

Use **show access-lists** to display the ACL configurations**.**

Examples

Create an extended expert ACL:

```
DES-7200(config)# expert access-list extended exp-acl
DES-7200(config-exp-nacl)# show access-lists expert
access-list extended exp-acl
DES-7200(config-exp-nacl)#
```

Create an extended expert ACL:

```
DES-7200(config)# expert access-list extended 2704
DES-7200(config-exp-nacl)# show access-lists
access-list extended 2704
DES-7200(config-exp-nacl)#
```

Related commands

Command	Description
show access-lists	Show the extended expert ACLs

Platform description

-

1.1.5 ip access-group

Use this command to apply a specific ACL to an interface. The **no** form of this command cancels the application.

ip access-group {*id*|*name*} {**in**|**out**} **[unreflect | reflect]**

no ip access-group {*id*|*name*} {**in**|**out**}

Parameter description

Parameter	Description
id	ID of the IP ACL (1 to 199, 1300 to 2699)
name	Name of the IP ACL
in	Filter the incoming packets of the interface.
out	Filter the outgoing packets of the interface.
unreflect	Disable the Reflexive-ACL.
reflect	Enable the Reflexive-ACL.

Default configuration

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage guidelines

Use the **ip access-group** command to apply the specified ACL to the interface, when the firewall is enabled.

Examples

The following example applies the ACL 120 on the fastEthernet0/0 to filter the incoming packets:

```
DES-7200(config)# interface fastEthernet 0/0
DES-7200(config-if)# ip access-group 120 in
```

Related commands

Command	Description
access-list	Define the ACL.
show access-lists	Show all the ACLs.
show ip access-list	Show the IP ACL (1 to 199, 1300 to 2699, 3000 to 3199).

ip access-list

Use this command to create a standard IP ACL or extended IP ACL. Use the **no** form of the command to remove the ACL.

ip access-list {**extended** | **standard**} {*id*|*name*}

no ip access-list {**extended** | **standard**} {*id*|*name*}

Parameter description

Parameter	Description
id	ID of the ACL 1 to 99 and 1300 to 1999 for standard ACL) or 100 to 199 and 2000 to 2699 for extended ACL
name	Name of the ACL

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

There are differences between a standard ACL and an extended ACL. The extended ACL is more precise. Refer to **deny** or **permit** in the two modes. Use **show access-lists** to display the ACL configurations**.**

Examples

Create a standard ACL:

```
DES-7200(config)# ip access-list extended 123
DES-7200(config-ext-nacl)# show access-lists
ip access-list extended 123
DES-7200(config-ext-nacl)#
```

Create an extended ACL:

```
DES-7200(config)# ip access-list standard std-acl
DES-7200(config-std-nacl)# show access-lists
ip access-list standard std-acl
DES-7200config-std-nacl)#
```

Related commands

Command	Description
show access-lists	Show the ACLs.

Platform description	N/A

1.1.6 ip access-list resequence

Use this command to reassign the sequence of the IP ACL entries and enter the corresponding configuration mode. Use the **no** form of this command to restore it to the default configuration.

ip access-list resequence {*id*|*name*} *start-sn inc-sn*

no ip access-list resequence {*id*|*name*}

Parameter description

Parameter	Description
id	ACL ID
name	ACL name
start-sn	Start sequence
inc-sn	Sequence increment

Default configuration	The start sequence is 10 and the sequence increment is 10.
Command mode	Global configuration mode
Usage guidelines	You can use the **show access-lists** command to show the configuration result.

Examples

Resequence the entries of the ACL:

```
DES-7200# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
DES-7200# config
DES-7200# (config)#ip access-list resequence 1 21 43
DES-7200# (config)# exit
DES-7200# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

	Command	Description
Related commands	**show access-lists**	Show the ACLs.

1.1.7 ipv6 traffic-filter

Use this command to apply the specified IPV6 ACL on the specified interface. Use the **no** form of the command to remove the application.

ipv6 traffic-filter *name* {**in**|**out**}

no ipv6 traffic-filter *name* {**in** | **out**}

		Parameter	Description
Parameter description		*name*	Name of Ipv6 ACL
		in	Filter the incoming packets of the interface
		out	Filter the outgoing packets of the interface

Default configuration	No ACL is applied on the interface.
Command mode	Interface configuration mode.
Usage guidelines	Apply the specified IPV6 ACL on the specified interface to control the interface traffic. You can view the configuration by command **show ipv6 traffic-filter.**

Examples	The following example shows how to apply the **access-list v6-acl** to Gigabit interface Gigabit 0/1:
	`DES-7200(config)# interface GigaEthernet 0/1`
	`DES-7200(config-if)# ipv6 traffic-filter v6-acl in`

	Command	Description
Related commands	**show access-group**	Show the ACL configurations.

1.1.8 ipv6 access-list

Use this command to create an extended IPV6 ACL. Use the **no** form of the command to remove the ACL.

ipv6 access-list *name*

no mac access-list *name*

Parameter description

Parameter	Description
name	ACL name

Command mode

Global configuration mode.

Usage guidelines

Use **show access-lists** to view ACL configuration.

Examples

Create an extended ipv6 ACL**:**

```
DES-7200(config)# ipv6 access-list extended v6-acl
DES-7200(config-ipv6-nacl)# show access-lists
ipv6 access-list v6-acl
DES-7200(config-ipv6-nacl)#
```

Related commands

Command	Description
show access-lists	Show the extended ipv6 ACLs

1.1.9 mac access-group

Use this command to apply the specified MAC ACL on the specified interface. Use the **no** form of the command to remove the application.

mac access-group {*id*|*name*}{**in**|**out**}

no mac access-group {*id*|*name*}{**in**|**out**}

Parameter description

Parameter	Description
id	ID of the MAC ACL (700 to 799)
name	Name of the MAC ACL

in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface

Default configuration

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage guidelines

You can use the **show running-config** command to show the configuration result.

Examples

The following example shows how to apply the **access-list accept**_00d0f8xxxxxx only to Gigabit interface 1:

```
DES-7200(config)#interface GigaEthernet 1/1
DES-7200(config-if)#mac access-group accept__00d0f8xxxxxx_only in
```

Related commands

Command	Description
show access-group	Show the ACL configuration.

Platform description

-

1.1.10 mac access-list

Use this command to create an extended MAC ACL. Use the **no** form of the command to remove the ACL.

mac access-list extended { *id*|name }

no mac access-list extended {*id*|*name*}

Parameter description

Parameter	Description
id	ID of the extended MAC ACL (700 to 799)
name	Name of the extended MAC ACL

Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	Use **show access-lists** to display the ACL configurations**.**

Examples	Create an extended MAC ACL**:**
	`DES-7200(config)# mac access-list extended mac-acl`
	`DES-7200(config-mac-nacl)# show access-lists mac access-list extended mac-acl`
	Create an extended ACL:
	`DES-7200(config)# mac access-list extended 704`
	`DES-7200(config-mac-nacl)# show access-lists mac access-list extended 704`

Related commands

Command	Description
show access-lists	Show the extended MAC ACLs

Platform description	-

1.1.11 no sn

Use this command to delete an entry of the ACL.

no <*sn*>

Parameter description

Parameter	Description
sn	Sequence number of the ACL entry

Command mode	ACL configuration mode.
Usage guidelines	Use this command to delete an ACL entry in ACL configuration mode.

Examples

```
DES-7200(config)# ipv6 access-list extended v6-acl
DES-7200(config-ipv6-nacl)# permit ipv6
host ::192.168.4.12 any
DES-7200(config-ipv6-nacl)#12 deny ipv6 host any any
DES-7200(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
12 deny ipv6 any any
DES-7200(config-ipv6-nacl)# no 12
DES-7200(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
DES-7200(config-ipv6-nacl)#
```

Related commands

Command	Description
show access-list	Show all the ACLs.
ip access-list	Define the IP ACL.
ipv6 access-list	Define the extended IPV6 ACL.
deny	Define the deny rule.
permit	Define the permit rule.

1.1.12 permit

One or multiple **permit** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

Use this command to set the permit rules.

1. Standard IP ACL

[*sn*] **permit** {*source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*]

2. Extended IP ACL

[*sn*] **permit protocol source** *source-wildcard* **destination**

destination-wildcard [**precedence** *precedence*] [**tos** *tos*] **[fragment]**

[**time-range** *time-range-name*]

Extended IP ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

[*sn*] **permit icmp** {**source** *source-wildcard* | **host** *source* | **any**}

{**destination** *destination-wildcard* | **host** *destination* | **any**}

[*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

  [*sn*] **permit tcp** {**source** *source-wildcard* | **host** *Source* | **any**} [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

  [*sn*] **permit udp** {**source** *source -wildcard*|**host** *source* |**any**} [*operator* **port** [*port*]] {**destination** *destination-wildcard* |**host** *destination* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

3. Extended MAC ACL

[*sn*] **permit** {**any** | **host** *source-mac-address*} {**any** | **host**

destination-mac-address} [*ethernet-type*][**cos** [*out*] [**inner** *in*]]

4. Extended expert ACL

[*sn*] **permit** [**protocol** | [*ethernet-type][* **cos** [*out*] [**inner** *in*]*]*] [**VID** [*out][***inner** *in]*] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source*-mac-*address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*][**fragment**] [**time-range** *time-range-name*]

- When you select the Ethernet-type field or cos field:

  [*sn*] **permit** {*ethernet-type*| **cos** [*out*] [**inner** *in*]*}* [**VID** [*out][***inner** *in]*] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

  [*sn*] **permit protocol** [**VID** [*out][***inner** *in]*] {**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

  [*sn*] **permit icmp** [**VID** [*out][***inner** *in]*] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**}[*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

  [*sn*] **permit tcp** [**VID** [*out][***inner** *in]*]{**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

  [*sn*] **permit udp** [**VID** [*out][***inner** *in]*]{**source** *source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

5. Extended IPv6 ACL

[*sn*] **permit protocol** {*source-ipv6-prefix / prefix-length* | **any** | **host** *source-ipv6-address*} {*destination-ipv6-prefix / prefix-length* | **any** | *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]

Extended IPv6 ACLs of some important protocols:

- **Internet Control Message Protocol** (ICMP)

  [*sn*] **permit icmp** {*source-ipv6-prefix / prefix-length* | **any**

  source-ipv6-address | **host**} {*destination-ipv6-prefix / prefix-length*

  | **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type*

  [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*]

  [**fragment**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

  [*sn*] **permit tcp** {*source-ipv6-prefix / prefix-length* | **host**

source-ipv6-address | **any**} [*operator* **port** [*port*]]

{*destination-ipv6-prefix / prefix-length* | **host**

destination-ipv6-address | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*]

[**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]

[**match-all** *tcp-flag*]

- **User Datagram Protocol** (UDP)

[*sn*] **permit udp** {*source-ipv6-prefix / prefix-length* | **host**

source-ipv6-address | **any**} [*operator* **port** [*port*]]

{*destination-ipv6-prefix / prefix-length* | **host**

destination-ipv6-address | **any**} [*operator* **port** [**port**]] [**dscp** *dscp*]

[**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]

Parameter description	For those not listed below, see **deny**.
Default configuration	N/A.
Command mode	ACL configuration mode.
Usage guidelines	Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.
Examples	The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
DES-7200(config)#expert access-list extended exp-acl
DES-7200(config-exp-nacl)#permit tcp  host
192.168.4.12 host 0013.0049.8272 any any
DES-7200(config-exp-nacl)#deny any any any any
DES-7200(config-exp-nacl)#show access-lists
expert access-list extended exp-acl
10 permit tcp  host  192.168.4.12 host 0013.0049.8272 any
any
20 deny any any any any
DES-7200(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)# ip access-list extended 102
DES-7200(config-ext-nacl)# permit tcp host 192.168.4.12
eq 100 any
DES-7200(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
DES-7200(config-ext-nacl)#exit
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)#ip access-group 102 in
DES-7200(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#mac access-list extended 702
DES-7200(config-mac-nacl)#permit host 0013.0049.8272 any
aarp
DES-7200(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
DES-7200(config-mac-nacl)#exit
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)#mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#ip access-list standard std-acl
DES-7200(config-std-nacl)#permit host 192.168.4.12
DES-7200(config-std-nacl)#show access-lists
ip access-list standard std-acl
  10 permit host 192.168.4.12
DES-7200(config-std-nacl)#exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# ip access-group std-acl in
```

This example shows how to use the extended IPV6 ACL.

The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
DES-7200(config)#ipv6 access-list extended v6-acl
DES-7200(config-ipv6-nacl)#11 permit ipv6
host ::192.168.4.12 any
DES-7200(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
DES-7200(config-ipv6-nacl)# exit
DES-7200(config)#interface gigabitethernet 1/1
DES-7200(config-if)#ipv6 traffic-filter v6-acl in
```

Related commands

Command	Description
show access-lists	Show all the ACLs.
ipv6 traffic-filter	Apply the extended ipv6 ACL on the interface.
ip access-group	Apply the IP ACL on the interface.
match access-group	Apply the extended MAC ACL on the interface.
ip access-list	Define the IP ACL.
mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.
deny	Deny the access.

1.2 Showing Related Commands

1.2.1 show access-group

Use this command to show the ACL configured on the interface.

show access-group[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode
Usage guidelines	Show the ACL configured of the interface. If no interface is specified, the associated ACLs of all the interfaces will be shown.

Examples	`DES-7200# show access-group`
	`ip access-list standard ipstd3`
	`Applied On interface GigabitEthernet 0/1.`
	`ip access-list standard ipstd4`
	`Applied On interface GigabitEthernet 0/2.`
	`ip access-list extended 101`
	`Applied On interface GigabitEthernet 0/3.`
	`ip access-list extended 102`
	`Applied On interface GigabitEthernet 0/8.`

Related commands

Command	Description
ip access-group	Apply the IP ACL to the interface.
mac access-group	Apply the mac ACl to the interface.
expert access-group	Apply the expert ACL to the interface.
ipv6 traffic-filter	Apply the IPv6 ACL to the interface.

1.2.2 show access-lists

Use this command to show all ACLs or the specified ACL.

show access-lists [*id*|*name*]

Parameter description

Parameter	Description
id	ID of the IP ACL
name	Name of the IP ACL

Command mode	Privileged mode.

Usage guidelines

Use this command to show the specified ACL. If no ID or name is specified, all the ACLs will be shown.

Examples

```
DES-7200# show access-lists n_acl
ip access-list standard n_acl
DES-7200# show access-lists 102
ip access-list extended 102
DES-7200# show access-lists
ip access-list standard n_acl
ip access-list extended 101
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
```

Related commands

Command	Description
ip access-list	Define the IP ACL.
mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.

1.2.3 show expert access-group

Use this command to show the configured expert ACL of the interface.

show expert access-group[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode

Privileged mode.

Usage guidelines

Show the expert ACL configured on the interface. If no interface is specified, the associated expert ACLs of all the interfaces will be shown.

Examples

```
DES-7200# show expert access-group interface
gigabitethernet 0/2
expert access-group ee in
```

```
Applied On interface GigabitEthernet 0/2.
```

Related commands

Command	Description
expert access-list	Define the extended expert ACL.

1.2.4 show ip access-group

Use this command to show the IP ACL configured on the interface.

show ip access-group[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode

Privileged mode

Usage guidelines

Show the IP ACL configured of the interface. If no interface is specified, the associated IP ACLs of all the interfaces will be shown.

Examples

```
DES-7200# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

Related commands

Command	Description
ip access-list	Define the IP ACL.

1.2.5 show ipv6 traffic-filter

Use this command to show the configured IPv6 ACL of the interface.

show ipv6 traffic-filter[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode.
Usage guidelines	Show the IPv6 ACL associated with the interface. If no interface is specified, the associated IPv6 ACLs of all the interfaces will be shown.
Examples	DES-7200# **show ipv6 traffic-filter interface gigabitethernet** *0/4* ipv6 access-group v6 in Applied On interface GigabitEthernet 0/4.

Related commands

Command	Description
ipv6 access-list	Define the type of IPv6 ACL.

1.2.6 show mac access-group

Use this command to show the configured MAC ACL of the interface.

show mac access-group[**interface** <*interface*>]

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode.
Usage guidelines	Show the MAC ACL associated with the interface. If no interface is specified, the associated MAC ACLs of all associated interfaces will be shown.
Examples	DES-7200# **show mac access-group interface gigabitethernet** *0/3* mac access-group *mm* in Applied On interface GigabitEthernet 0/3.

Related

Command	Description

commands	**mac access-list**	Define the extended MAC ACL.

1.3 Security Channel

1.3.1 security global access-group

Use this command to configure the global security channel.

security global access-group { *id* | *name* **}**

no security global access-group

Parameter description

Parameter	Description
id	ACL ID
name	ACL name

Command mode Global configuration mode

Usage guidelines Use this command to configure the global security channel .

Examples

```
DES-7200# security global access-group 1
```

Platform description -

1.3.2 security access-group

Use this command to configure the security channel on the interface.

security access-group { *id* | *name* **}**

no security access-group

Parameter description

Parameter	Description
id	ACL ID

	name	ACL name

Command mode	Interface configuration mode.
Usage guidelines	Use this command to configure the security channel on the interface.
Examples	`DES-7200# security access-group 1`
Platform description	-

1.3.3 security uplink enable

Use this command to configure the uplink port of the security channel on the interface.

security uplink enable

no security uplink enable

Command mode	Interface configuration mode.
Usage guidelines	Use this command to configure the uplink port of the security channel on the interface.
Examples	`DES-7200# security uplink enable`
Platform description	-

1.3.4 show security

Use this command to show security channel configuration or the configuration of the security channel on the specified interface.

show secu-acl

Parameter	**Parameter**	**Description**

description	-	-

Default configuration N/A

Command mode Privileged mode

Usage guidelines This command is used to show all security channels.

Examples

```
DES-7200(config-if)#show secu-acl
Ports     Type      access-group
---------- ---------- ------------
Fa0/4     security   50
Global    security   60
Fa0/6     uplink     --
```

Related commands

Command	Description
security global access-group	Define the global security channel.
security access-group	Define the security channel on the interface.
security uplink enable	Define the uplink port of the security channel on the interface.

Platform description -

1.4 SVI Router ACLs Configuration Commands

1.4.1 svi router-acls enable

Use this command to enable the svi router-acls function to validate the SVI ACL on the routing packets only forwarded by Layer-3 devices. Use the **no** form of this command to disable this function

svi router-acls enable

[*no*] **svi router-acls enable**

Parameter description

Parameter	Description
no	Disable the svi router-acls function.

Default configuration Disabled.

Command mode Global configuration mode

Usage guidelines N/A

Examples

```
DES-7200#svi router-acls enable
```

Related commands

Command	Description
-	-

Platform description This command is supported by the DES-7200 series switches

2 QoS Configuration Command

2.1 Default Configuration

Before configuring QoS, you must have a full knowledge of these items related to QoS:

1. One interface can only be associated with one policy map at most.
2. One policy map may own many class maps
3. One class map can be associated with only one ACL, and all the ACEs of this ACL must have the same filter domain template.
4. The number of ACEs associated with an interface complies with the restriction given in "*Configuring Security ACLs*".

The QoS function is disabled by default. Namly the device processes all the packets in the same way. But if you associate a policy map with an interface and the trust mode on one interface, the QoS of this interface is enabled automatically. To disable the QoS function of the interface, simply resolve the policy map setting of the interface and set the information mode of the interface to Off. Below is the default QoS configuration:

Default CoS value	0
Queue Number	8
Queue Scheduling	WRR
QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:15
DRR Weight Range	1:15
Trust mode	No Trust

Default CoS to queue mapping table:

CoS Value	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Default CoS to DSCP mapping table

CoS Value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

Default IP Precedence to DSCP mapping table

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default DSCP to CoS mapping table

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

2.2 Related Configuration Commands

2.2.1 mls qos trust

Use this command to configure the trust mode on an interface. Use the no form of this command to restore it to the default.

mls qos trust [cos | dscp | ip-precedence]

no mls qos trust

Parameter description

Parameter	Description
cos	The QoS trust mode of the port is CoS.
dscp	The QoS trust mode of the port is DSCP.
ip-precedence	The QoS trust mode of the port is IP-PRE.
no	Restore it to the default value.

Default configuration N/A.

Command mode	Interface configuration mode.
Examples	`DES-7200(config)# interface gigabitethernet 1/1` `DES-7200(config-if)# mls qos trust cos`
Related commands	**show mls qos interface** *interface-id*
Platform description	DES-7200 series support the parameter **cos dscp ip-precedence.**

2.2.2 mls qos cos

Use this command to configure the CoS value of an interface. Use the no form of this command to restore it to the default.

mls qos cos *default-cos*

no mls qos cos

Parameter description

Parameter	Description
default-cos	0~7
no	Restore it to the default value.

Default configuration	The CoS value is 0.
Command mode	Interface configuration mode.
Examples	`DES-7200(config)# interface gigabitethernet 1/1` `DES-7200(config-if)# mls qos cos 7`
Related commands	**show mls qos interface** *interface-id*

2.2.3 interface rate-limit

Use this command to set the rate limit on the port.

rate-limit { **input | output** } *bps burst-size*

no rate-limit

Parameter description

Parameter	Description
input	Input rate limit
ouput	Ouput rate limit
bps	Limited bandwidth per second
burst-size	The dscp-list range varies with products
no	Restore it to the default value.

Default configuration N/A

Command mode Interface configuration mode.

Examples

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# rate-limit input 1000000 4096
```

Related commands

Command	Description
show mls qos interface	-

2.2.4 class maps

Use the following command to creat an ACL:

ip access-list {**extended | standard**} { *acl-id* | a*cl-name* }

Or **mac access-list extended** {*acl-id* | a*cl-name*}

Or **expert access-list extended** {*acl-id* | a*cl-name*}

Or **ipv6 access-list extended** a*cl-name*

Or **access-list** *acl-id* series commands (refer to the related ACL chapters)

Use the following command to create a class map and enter the class map configuration mode:

[no] class-map *class-map-name*

Use the following command to create the matching standard of class map:

[**no**] **match access-group** a*cl-name*| *acl-id*

[**no**] **match ip dscp** dscp-value1 [dscp-value2 [dscp-valueN]]

[**no**] **match ip precedence** *ip-pre-value1* [*ip-pre-value2* [*ip-pre-valueN*]]

Parameter description

Parameter	Description
acl-name	Name of the created ACL
acl-id	ID of the created ACL
class-map-name	Name of the class map to be created
dscp-valueN	Ip dscp value to be created.
ip-pre-valueN	Ip precedence value to be created.
no class-map *class-map-name*	Delete the existed class map.
no match access-group a*cl-name*| *acl-id*	Delete the match.
no match ip dscp *dscp-value1* [*dscp-value2* [*dscp-valueN*]]	Delete the matched ip dscp value.
no match ip precedence *ip-pre-value1* [*ip-pre-value2* [*ip-pre-valueN*]]	Delete the matched ip precedence value.

Command mode

Global configuration mode.

Examples

Create an extended MAC ACL named me.

```
DES-7200(config)# mac access-list extended me
```

Set ACL rules.

```
DES-7200(config-ext-macl)# permit host 1111.2222.3333 any
```

Exit the ACL setting.

```
DES-7200(config-ext-macl)# exit
```

Create a class map named **cm.**

```
DES-7200(config)# class-map cm
```

Associate the class map and the ACL.

```
DES-7200(config-cmap)# match access-group me
```

Exit the class map setting.

	DES-7200(config-cmap)# **exit** Create the class-map naming cm-dscp and match the DSCP 8,16,24 and exit the setting DES-7200(config)# **class-map cm-dscp** DES-7200(config-cmap)# **match ip dscp** *8 16 24* DES-7200(config-cmap)# **exit**

Related commands	**Command**	**Description**
	show map access-lists	-
	show ip access-lists	-
	show class-map	-

Platform description	The none-tos function is supported on the DES-7200 series device.

2.2.5 policy maps

Use the following command to create a policy map and enter the policy map configuration mode

[no] policy-map *policy-map-name*

Use the following command to create the class map data classification used in the policy map and enter into the data classification configuration mode.

[no] class *class-map-name*

Use the following command to set the ip_dscp value of the IP packets, which does not take effect for non-IP packets.

set ip dscp *new-dscp*

no set ip dscp

Use the following command to set the cos value of the packets. With the **none-tos** configured, the DSCP value of the packets will not be modified.

set cos *new-cos* [none-tos]

no set cos

Use the following command to limit the bandwidth and specify the method of handling the excessive part.

police *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value* | **cos** *cos-value* [**none-tos**] }]

no police

Parameter description

Parameter	Description
policy-map-name	Name of the policy map to be created
no policy-map *policy-map-name*	Delete the existed policy map.
class-map-name	Name of the created class map
no class *class-map-name*	Delete the class map.
new-dscp	New DSCP value, whose range varies with products.
new-cos	New Cos value, in the range of 0 to 7.
rate-bps	The limitation of bandwidth per second, in kbps
burst-byte	The burst traffic limitation, in Kbyte
drop	Drop the packets exceeding the bandwidth.
dscp-value	Overwrite the DSCP value of the packets exceeding the bandwidth, whose range varies with products.
cos-value	Modify the Cos value of the packet of over-bandwidth, in the range of 0 to 7.

Command mode

Global configuration mode

Examples

Create a policy map and name it as **po**

```
DES-7200(config)# policy-map po
```

Associate class-map cm

```
DES-7200(config-pmap)# class cm
```

Set the DSCP value as 10

```
DES-7200(config-pmap-c)# set ip dscp 10
```

Set the bandwidth as 1M, the burst traffic as 4096k, and the method for handing the excessive part to assign the new DSCP value of 16**.**

```
DES-7200(config-pmap-c)# police 1000000 4096
exceed-action dscp 16
```

Related commands	**show policy-map**
Platform description	This command is supported on the DES-7200 series devices. The DES-7200 series support the Cos modifying.

2.2.6 service-policy

Use this command to apply the policy map on the interface or the virtual-group.

service-policy {**input | output**} *policy-map-name*

no service-policy {**input | output**}

Parameter description

Parameter	Description
policy-map-name	Name of the created policy map
no	Cancel the application of the policy map on the interface or the virtual-group.

Command mode	Interface configuration mode, and virtual-group configuration mode.

Examples

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# service-policy input po
DES-7200(config)# virtual-group 3
DES-7200(config-if)# service-policy input po
```

Related commands	**show mls qos interface.**
Platform description	DES-7200 series support the parameter **input** and **output.** The parameter **output** is not supported in the virtual-group.

2.2.7 priority-queue

Use this command to configure the output queue scheduling algorithm.

priority-queue

[no] priority-queue

Parameter description

Parameter	Description
priority-queue	Set the output queue scheduling algorithm to SP (for DES-7200).
no priority-queue	Set the output queue scheduling algorithm to WRR.

Default configuration The output queue scheduling algorithm is WRR.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# no priority-queue
```

Related commands **show mls qos queuing**

53.2.8 priority-queue cos-map

Use this command to configure the associated CoS value of output queue:

priority-queue cos-map *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]

no priority-queue cos-map

Parameter description

Parameter	Description
qid	Specified queue id.
cos0 ... cos7	Associated CoS value.
no	Restore to the default value.

Default configuration See default configuration.

Command mode Global configuration mode.

Examples	`DES-7200(config)#priority-queue cos-map 1 0 1`
Related commands	**show mls qos queuing**

2.2.8 wrr-queue bandwidth

Use this command to set the weight ratio for the WRR algorithm. Use the **no** form of the command to restore it to the default.

wrr-queue bandwidth *weight1 ... weightn*

no war-queue bandwidth

Parameter description

Parameter	Description
weight1...weightn	Weight value specified for the output queues. For the number of weights and its range, see the default settings.
no	Restore to the default value.

Default configuration	weight1: ...: weightn = 1:..:1
Command mode	Global configuration mode
Examples	`DES-7200(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8`
Related commands	**show mls qos queuing**

2.2.9 mls qos map cos-dscp

Use this command to map the CoS value to the DSCP value. Use the **no** form of the command to disable the mapping.

mls qos map cos-dscp *dscp1...dscp8*

no mls qos map cos-dscp

Parameter description

Parameter	Description
dscp	Specify the DSCP value.
no	Restore to the default value.

Default configuration See the default configuration.

Command mode Global configuration mode

Examples

```
DES-7200(config)# mls qo map cos-dscp 8 10 16 18 24 26 32 34
```

Related commands

Command	Description
show mls qos maps	Show DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

2.2.10 mls qos map dscp-cos

Use this command to map the DSCP value to the COS value. Use the **no** form of the command to disable the mapping.

mls qos map dscp-cos *dscp-list* to *cos*

no mls qos map dscp-cos

Parameter description

Parameter	Description
dscp-list	DSCP list. Its range varies with products.
cos	COS value ranging 0 to 7
no	Restore to the default value.

Default configuration See the default configuration.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

Related commands	Command	Description
	show mls qos maps	Show DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

2.2.11 interface rate-limit

Use this command to configure rate limitation on the interface. Use the **no** form of the command to restore it to the default.

rate-limit {**input** | **output**} *bps burst-size*

no rate-limit

Parameter description	Parameter	Description
	input	Specify the input speed limit.
	output	Specify the output speed limit.
	bps	Bandwidth limitation per second
	burst-size	Burst traffic limit (Kbyte). Its range varies with products.
	no	Restore to the default value.

Command mode Interface configuration mode.

Examples

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# rate-limit input 1000000 4096
```

Related commands **show mls qos interface.**

2.2.12 mls qos scheduler

Use this command to configure the queue scheduling algorithm. Use the **no** form of the command to restore it to the default.

mls qos scheduler [**sp | rr | wrr | drr**]

no mls qos scheduler

Parameter description	Parameter	Description
	sp	Absolute priority scheduling
	rr	Round-robin scheduling

	wrr	Frame count weighted round-robin scheduling
	drr	Frame length weighted round-robin scheduling
	no	Restore to the default value.

Default configuration The queue scheduling algorithm is wrr by default.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# mls qos scheduler sp
```

Related commands **show mls qos scheduler.**

2.2.13 drr-queue bandwidth

Use this command to set the queue weight in the DRR scheduling mode. Use the **no** form of the command to restore it to the default.

drr-queue bandwidth *weight1...weight8*

no drr-queue bandwidth

Parameter description	**Parameter**	**Description**
	weight1...weight8	Queue weight. For the value range, see the default configuration.
	no	Restore to the default value.

Default configuration See the default configuration.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# drr-queue bandwidth 1 2 3 4 5 6 7 8
```

Related commands	**show mls qos queuing**

2.2.14 mls qos map ip-prec-dscp

Use this command to map the IP-precedence to the DSCP value. Use the **no** form of this command to disable the mapping.

mls qos map ip-prec-dscp dscp1...dscp8

no mls qos map ip-prec-dscp

Parameter description

Parameter	Description
dscp	Specify the DSCP value.
no	Restore to the default value.

Default configuration See the default configuration.

Command mode Global configuration mode.

Examples

```
DES-7200(config)# mls qo map ip-prec -dscp 8 10 16 18 24 26 32 34
```

Related commands

Command	Description
show mls qos maps	Show the DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

2.2.15 virtual-group

Use this command to configure a physical port or Aggregate port as the member port of a virtual group. Use the **no** form of this command to remove the member attribute of a virtual group on the port.

virtual-group *virtual-group-number*

no virtual-group *virtual-group-number*

Parameter description

Parameter	Description
virtual-group-number	Virtual group number, up to 128.

Default configuration	By default, the physical port belongs to no virtual-group.
Command mode	Interface configuration mode.
Usage guidelines	The member port joined the virtual group must be physical port or Aggregate Port. The virtual group member ports must be in the same line card(for the chassis-shaped switch) or in the same switch(for the box-shaped switch). If the line card or switch has 48 ports, then all member ports shall be distributed on the former 24 ports or the latter 24 ports.

Examples	The following example sets the interface gigabitEthernet 1/3 as the member of virtual group 3:
	`DES-7200(config)# interface gigabitethernet 1/3`
	`DES-7200(config-if)# virtual-group 3`

Related commands

Command	Description
show virtual-group	Show the virtual-group settings.

2.3 Showing Related Command

2.3.1 show class-map

Use this command to show the information of class maps.

show class-map [*class -name*]

Parameter description

Parameter	Description
class-name	Name of the class map

Default configuration	All class maps are shown by default.

Command mode	Privileged EXEC mode.
Examples	`DES-7200# show class-map`

2.3.2 show policy-map

Use this command to show the information of the policy map.

show policy-map [*policy-name* [**class** *class-name*]]

Parameter description

Parameter	Description
policy-name	Name of the policy name
class-name	Name of the class map

Default configuration	All policy maps are shown by default.
Command mode	Privileged EXEC mode.
Examples	`DES-7200# show policy-map`

2.3.3 show mls qos interface

Use this command to display the QoS configuration on the interface.

show mls qos interface [*interface-id*] [**policers**]

Parameter description

Parameter	Description
interface-id	Interface ID
policers	Show the police associated with the interface

Default configuration	The QoS information of all ports is shown.

Command mode	Privileged EXEC mode.
Examples	`DES-7200# show mls qos interface fastEthernet 0/1`

2.3.4 show mls qos queuing

Use this command to show the QoS queuing information.

show mls qos queueing

Command mode	Privileged EXEC mode.
Examples	`DES-7200# show mls qos queueing`
Platform description	DES-7200 series show cos-to-queue map, wrr weight, and drr weight.

2.3.5 show mls qos scheduler

Use this command to show the information on queue scheduling algorithm.

show mls qos scheduler

Command mode	Privileged EXEC mode.
Examples	`DES-7200# show mls qos scheduler`
Platform description	This command is supported on DES-7200 series.

2.3.6 show mls qos maps

Use this command to show QoS maps.

show mls qos maps [**cos-dscp | dscp-cos | ip-prec-dscp**]

Parameter description

Parameter	Description
cos-dscp	Show the cos-dscp maps.
dscp-cos	Show the dscp-cos maps.

	ip-prec-dscp	Show the ip-prec-dscp maps.

Default configuration All QoS maps are shown by default.

Command mode Privileged EXEC mode.

Examples

```
DES-7200# show mls qos maps
```

2.3.7 show mls qos rate-limit

Use this command to show the information about rate limit on the interface.

show mls qos rate-limit [**interface** *interface-id*]

Parameter description

Parameter	Description
interface	Interface ID

Command mode Privileged EXEC mode.

Examples

```
DES-7200# show mls qos rate-limit
```

2.3.8 show virtual-group

Use this command to show the virtual group information.

show virtual-group [*virtual-group-number* | **summary**]

Parameter description

Parameter	Description
virtual-group-number	Virtual group number, up to 128.
summary	Show the information on all virtual groups.

Command mode Privileged EXEC mode.

Examples

```
DES-7200# show virtual-group 1

DES-7200# show virtual-group summary
```

Related commands

Command	Description
virtual-group	Enable the virtual group.

3 MPLS QOS Configuration Commands

3.1 Default Configurations

MPLS QoS allows the differentiation of MPLS packets. Since MPLS QoS is a subset of QoS, the previous section (QoS Configuration commands) is called IP QoS to facilitate description.

Before proceeding with MPLS QoS configuration, the following information related to MPLS QoS shall be clarified:

- All configurations of IP QoS are applicable to MPLS QoS;
- MPLS QoS allows the differentiation of MPLS packets;
- When one or multiple label is inserted into an IP packet, the default action is the map internal CoS to all EXP bits added into the label as per cos-exp mapping relation.
- Support one group of exp-cos maps and 8 groups of cos-exp maps.

By default, MPLS QoS function is disabled, namely the device will treat all packets equally. The following tables show the default configurations of MPLS QoS:

Default EXP-to-CoS map

	EXP value	CoS value
EXP to CoS	0	0
	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7

Default CoS-EXP map

CoS to EXP

CoS	EXP
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Usage guidelines

Caution The contents in 8 groups of default cos-exp maps are the same.

Note Currently, MPLS QoS is supported by DES-7200 series products based on EC line card.

3.2 Configuration Related Commands

3.2.1 match mpls experimental topmost

Match one or multiple EXPs. Use this command in class-map configuration mode. Use **no** form of this command to remove matched EXP values from one class map.

match mpls experimental topmost *exp-value1* [*exp-value2* [*exp-valueN*]]

no match mpls experimental topmost *exp-value1* [*exp-value2* [*exp-valueN*]]

Parameter description

Parameter	Description
exp-valueN	EXP value to be matched; up to 8 different values can be matched at one time.

Default No matching rule.

Command mode	Class-map configuration mode.
Usage guidelines	The range of EXP value is 0-7.

Examples	The following example shows how to match multiple EXP values. 3 EXP values are matched in this example.
	`DES-7200(config)# class-map map1`
	`DES-7200(config-cmap)# match mpls experimental topmost 1 2 3`
	`DES-7200(config-cmap)# exit`

Related commands

Command	Description
class-map	Create one class map in order to identify objects and classify traffic as per certain matching rules.
match ip dscp	Match the DSCP value of packet (only applies to IPv4 packets).
policy-map	Create or modify a policy map, which can be associated to one or multiple interfaces as QoS service policy.
service-policy	Associate one policy map to the specified interface.
set cos	Mark the CoS value of packet
show class-map	Display the specific contents of all class maps or the specified class map.

Platform description	This command is supported by DES-7200 series devices based on EC line card.

3.2.2 mls qos map exp-cos

Use this command to set mapping the EXP value to the packet CoS value. Use **no** form of this command to the restore to the default exp-cos mapping relation.

mls qos map exp-cos *cos1 cos2 cos3 cos4 cos5 cos6 cos7 cos8*

no mls qos map exp-cos

Parameter description

Parameter	Description
cos1...cos8	Define EXP-to-CoS mapping. These 8 values (cos1-cos8) correspond to EXP values of 0-7.

Default	See the default EXP-CoS map given in the section of "Default Configurations".
Command mode	Global configuration mode.
Usage guidelines	NA.

Examples

```
DES-7200# configure terminal
DES-7200(config)# mls qos exp-cos 1 1 2 2 5 6 7 8
```

Related commands

Command	Description
show mls qos maps	Display configurations of QoS mapping relation.

Platform description	This command is supported by DES-7200 series devices based on EC line card.

3.2.3 mls qos map cos-exp

Use this command to set mapping the CoS value to the EXP value. Use **no** form of this command to the restore to the default cos-exp mapping relation.

mls qos map cos-exp *group-number exp1 exp2 exp3 exp4 exp5 exp6 exp7 exp8*

no mls qos map cos-exp *group-number*

Parameter description

Parameter	Description
group-number	Number of cos-exp mapping group (1-8).
exp1...exp8	Define CoS-to-EXP mapping. These 8 values (exp1-exp8) correspond to CoS values of 0-7.

Default	See the default CoS-EXP map given in the section of "Default Configurations".
Command mode	Global configuration mode.
Usage guidelines	If the user doesn't to map which cos-exp mapping group to a specific interface, then all cos-exp mapping groups applied to this interface will be the first group by default.

Examples	Example: Configure the first group of cos-exp map.
	`DES-7200# configure terminal`
	`DES-7200(config)# mls qos map cos-exp 1 0 2 1 3 3 5 6 7`

Related commands

Command	Description
show mls qos maps	Display configurations of QoS mapping relation.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.2.4 mls qos service cos-exp

Associate a cos-exp mapping group to the interface. Use **no** form of this command to restore to the first group.

mls qos service cos-exp *group-number*

no mls qos service cos-exp

Parameter description

Parameter	Description
group-number	Number of cos-exp mapping group (1-8).

Default

By default, the first group of cos-exp map is associated to the interface.

Command mode

Interface configuration mode.

Usage guidelines

Caution

Cos-exp mapping relation only applies to egress packets.

Note

By default, the contents in 8 groups of default cos-exp maps are the same.

Usage guidelines

NA

Examples

Example: Associate the third group of cos-exp map to interface Gi 1/1.

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mls qos service cos-exp 3
```

Related commands

Command	Description
mls qos map cos-exp	Map CoS value to the EXP value.
show mls qos interface *interface-id*	Display QoS information related to the interface.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.2.5 mls qos trust

Configure QoS trust mode on the interface. Use **no** form of this command to restore the interface to the default trust mode.

mls qos trust {cos | dscp | ip-precedence | experimental}

no mls qos trust

Parameter description

Parameter	Description
cos	QoS trust mode of the interface is trust CoS.
dscp	QoS trust mode of the interface is trust DSCP.
ip-precedence	QoS trust mode of the interface is trust IP-PRE.
experimental	QoS trust mode of the interface is trust MPLS EXP.

Default

Untrusted.

Command mode	Interface configuration mode.
Usage guidelines	NA.

Examples	Example: Configure the trust mode of port Gi 1/1 to trust MPLS EXP.
	`DES-7200(config)# interface gigabitethernet 1/1`
	`DES-7200(config-if)# mls qos trust experimental`

Related commands

Command	Description
show mls qos interface *interface-id*	Display QoS information related to the interface.

Platform description	The QoS trust mode as trust MPLS EXP is supported by DES-7200 series products based on EC line card.

3.2.6 mpls copy experimental

Enable the MPLS EXP copying. The EXP bits in the incoming topmost label will be copied to the outgoing label to be exchanged. When the ingress label is removed, the EXP bits in the original incoming topmost label will be copied to the second topmost label. Use **no** form of this command to disable MPLS EXP copying.

[no] mpls copy experimental

Parameter description

Parameter	Description
-	-

Default	MPLS EXP copying is disabled.
Command mode	Global configuration mode.

Usage guidelines	NA

Examples	Example: Enable the MPLS EXP copying.
	`DES-7200# configure terminal`
	`DES-7200(config)# mpls copy experimental`

Related commands

Command	Description
show mls qos mpls	Display MPLS QoS information.

Platform description	This command is supported by DES-7200 series devices based on EC line card.

3.2.7 mpls propagate-experimental none

When configuring to remove the label, the EXP bits in the original incoming topmost label won't be copied to the second topmost label. Use **no** form of this command to restore the copying of EXP bits in the incoming topmost label to the second topmost label.

[no] mpls propagate-experimental none

Parameter description

Parameter	Description
-	-

Default	This function is disabled.
Command mode	Global configuration mode.
Usage guidelines	Before configuring "**mpls propagate-experimental none**", you must configure "**mpls copy experimental**" command first.

Examples

Example: When configuring to remove the label, the EXP bits in the original incoming topmost label won't be copied to the second topmost label.

```
DES-7200# configure terminal
DES-7200(config)# mpls copy experimental
DES-7200(config)# mpls propagate-experimental none
```

Related commands

Command	Description
mpls copy experimental	Enable the MPLS EXP copying.
show mls qos mpls	Display the MPLS QoS information.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.2.8 police

Limit the bandwidth for the specified traffic and specify the action for handling excessive traffic. Use **no** form of this command to disable traffic limit.

police *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value* | **cos** *cos-value* [**none-tos**]}]

no police

Parameter description

Parameter	Description
rate-bps	Limit the bandwidth per second (unit: kbps).
burst-byte	Limit the burst traffic (unit: kbyte).
drop	Discard excessive packets.
dscp-value	Change the DSCP value of excessive packets.
cos-value	Change the CoS value of excessive packets (range: 0-7).

	none-tos	The DSCP value of excessive packets won't be modified while changing the CoS value of excessive packets.

Default

Drop excessive packets.

Command mode

Data classification configuration mode.

Usage guidelines

This command is used to mark the CoS value of packets. Use this command to modify the CoS value of packets, and the use the cos-exp map attached to the interface to indirectly modify the MPLS EXP value of egress packets.

Examples

Example: Match MPLS packets with MPLS EXP being 2 and classify these packets into the class of exp-2. Configure policy to rate limit the incoming packets and mark the CoS value of excessive packets as 0 (assuming that the input interface of MPLS packets is gigabitethernet 2/2).

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# class-map exp-2
DES-7200(config-cmap)# match mpls experimental topmost 2
DES-7200(config-cmap)# exit
DES-7200(config)# policy-map policy-for-exp2
DES-7200(config-pmap)# class exp-2
DES-7200(config-pmap-c)# police 1000000 4096 exceed-action cos 0
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
DES-7200(config)# interface gigabitethernet 2/2
DES-7200(config-if)# service-policy input
```

```
policy-for-exp2
DES-7200(config-if)# exit
DES-7200(config)#
```

Related commands

Command	Description
class-map	Create one class map in order to identify objects and classify traffic as per certain matching rules.
policy-map	Create or modify a policy map, which can be associated to one or multiple interfaces as QoS service policy.
service-policy	Associate one policy map to the specified interface.
mls qos map cos-exp	Map CoS value to the EXP value.
mls qos map exp-cos	Map CoS value to the EXP value.
show class-map	Display the specific contents of all class maps or the specified class map.
show policy-map	Display the specific contents of all policy maps or the specified policy map.

Platform description This command is supported by DES-7200 series devices based on EC line card.

3.2.9 set cos

Re-mark the CoS value of packets. Use **no** form of this command to disable re-marking.

set cos *new-cos* [**none-tos**]

no set cos

Parameter

Parameter	Description

description	*new-cos*	The new CoS value to be re-marked.
	none-tos	The DSCP value of packets is not modified while re-marking the CoS value of packets.

Default	NA
Command mode	Data classification configuration mode.
Usage guidelines	This command is used to re-mark the EXP value of topmost label of MPLS packets. When using this command, make sure the exp-cos and cos-exp maps use the default settings. Please refer to the configuration guidelines for detailed reasons.

Examples	Example: Configure all incoming MPLS packets on port Gi 1/1 with EXP value of topmost label being 2, so that the EXP value of topmost label will be re-marked to 1 after output.
	`DES-7200# configure terminal`
	`DES-7200(config)# class-map map1`
	`DES-7200(config-cmap)# match mpls experimental topmost 2`
	`DES-7200(config-cmap)# exit`
	`DES-7200(config)# policy-map policy1`
	`DES-7200(config-pmap)# class map1`
	`DES-7200(config-pmap-c)# set cos 1`
	`DES-7200(config-pmap-c)# exit`
	`DES-7200(config-pmap)# exit`
	`DES-7200(config)#`
	`DES-7200(config)# interface gigabitethernet 1/1`
	`DES-7200(config-if)# service-policy input policy1`
	`DES-7200(config-if)# exit`
	`DES-7200(config)#`

Related commands

Command	Description
class-map	Create a class map to identify objects and classify traffic as per certain matching rules.
policy-map	Create or modify a policy map, which can be associated to one or multiple interfaces as QoS service policy.
service-policy	Associate one policy map to the specified interface.
mls qos map cos-exp	Map CoS value to the EXP value.
mls qos map exp-cos	Map CoS value to the EXP value.
show class-map	Display the specific contents of all class maps or the specified class map.
show policy-map	Display the specific contents of all policy maps or the specified policy map.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.3 Showing Related Commands

3.3.1 show class-map

Display the contents of class map.

show class-map [*class-name*]

Parameter description

Parameter	Description
class-name	Name of class map.

Default	Display all class maps.
Command mode	Privileged mode.
Usage guidelines	If the *class-name* is not specified, all class maps will be displayed. Enter the specific class-name to display contents of the specified class map.

Examples	Example: Configure one class-map to match multiple EXP values and display contents of this class-map.
	`DES-7200(config)# class-map map1`
	`DES-7200(config-cmap)# match mpls experimental topmost 1 2 3`
	`DES-7200(config-cmap)# exit`
	`DES-7200(config)# exit`
	`DES-7200# show class-map map1`
	
	`Class Map class1`
	`Match mpls experimental topmost 1 2 3`
	`DES-7200#`

Related commands

Command	Description
class-map	Create one class map in order to identify objects and classify traffic as per certain matching rules.

Platform description	Supported by DES-7200 series devices.

3.3.2 show mls qos interface

Display QoS information related to the interface.

show mls qos interface *interface-id* [**policers**]

Parameter description

Parameter	Description
interface-id	The interface to be displayed.
policers	Police associated to the interface.

Default

Display QoS information of all interfaces.

Command mode

Privileged mode.

Usage guidelines

If the *interface-id* is not specified, QoS information of all interfaces will be displayed; enter the specific interface-id to display the QoS information of the specified interface.

Examples

Example: Configure one policy map and associate to Gi 1/1 and display the QoS information of interface Gi 1/1.

```
DES-7200# configure terminal
DES-7200(config)# class-map map1
DES-7200(config-cmap)# match mpls experimental topmost 2
DES-7200(config-cmap)# exit
DES-7200(config)# policy-map policy1
DES-7200(config-pmap)# class map1
DES-7200(config-pmap-c)# set cos 1 none-tos
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
DES-7200(config)#
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# service-policy input policy1
DES-7200(config-if)# exit
DES-7200(config)# exit
DES-7200# show mls qos interface gigabitethernet 1/1
Interface: GigabitEthernet 1/1
```

```
Attached input  policy-map: policy1
Attached output policy-map:
Default trust: none
Default cos: 0
Attached mpls cos-exp group: 1
DES-7200#
```

Related commands

Command	Description
-	-

Platform description

Supported by DES-7200 series devices.

3.3.3 show mls qos maps

Display the cos-dscp maps, dscp-cos maps, ip-prec-dscp maps, cos-exp maps and exp-cos maps.

show mls qos maps [cos-dscp | dscp-cos | ip-prec-dscp | cos-exp | exp-cos]

Parameter description

Parameter	Description
cos-dscp	Display the cos-dscp maps.
dscp-cos	Display the dscp-cos maps.
ip-prec-dscp	Display the ip-prec-dscp maps.
cos-exp	Display the cos-exp maps.
exp-cos	Display the exp-cos maps.

Default

Display the cos-dscp maps, dscp-cos maps, ip-prec-dscp maps, cos-exp maps and exp-cos maps.

Command mode

Privileged mode.

Usage

If no map type is specified, all maps will be displayed.

guidelines

Examples

```
DES-7200# show mls qos maps exp-cos
exp cos
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
DES-7200#
DES-7200# show mls qos maps cos-exp
CoS-to-EXP Map group number: 1
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
   7  7
CoS-to-EXP Map group number: 2
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number: 3
```

```
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number：4
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number：5
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number：6
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
```

```
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number: 7
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
CoS-to-EXP Map group number: 8
cos exp
--- ---
  0  0
  1  1
  2  2
  3  3
  4  4
  5  5
  6  6
  7  7
```

Related commands

Command	Description
-	-

Platform description

Displaying cos-exp maps and exp-cos maps is supported by DES-7200 series products based on EC line card.

3.3.4 show mls qos mpls

Display the MPLS QoS information.

show mls qos mpls

Parameter description

Parameter	Description
-	-

Default

NA

Command mode

Privileged mode.

Usage guidelines

NA

Examples

```
DES-7200# show mls qos mpls
Default mpls copy exp: disable
Default mpls propagate-exp none: disable
DES-7200#
```

Related commands

Command	Description
mpls copy experimental	Enable the MPLS EXP copying.
mpls propagate-experimental none	The EXP bits in the topmost label won't be copied to the second topmost label while removing the label stack.

Platform description

This command is supported by DES-7200 series devices based on EC line card.

3.3.5 show policy-map

Display the contents of policy map (the specified class *class-name*).

show policy-map [*policy-name* [**class** *class-name*]]

Parameter description

Parameter	Description
policy-name	Name of policy name.
class-name	Name of class map.

Default

Display all policy names.

Command mode

Privileged mode.

Usage guidelines

If the policy-name is not specified, all policy maps will be displayed; enter the specific policy-name to display contents of the specified policy map. If the class-name is not specified, all class maps under the specified policy map will be displayed; if the specific class-name is specified, contents of this class map under the specified policy map will be displayed.

Examples

Example: Configure a policy map to configure all incoming MPLS packets with EXP value of topmost label being 2, so that the EXP value of topmost label will be marked to 1 after output. After configuring policy map, display the contents of this policy map.

```
DES-7200# configure terminal
DES-7200(config)# class-map map1
DES-7200(config-cmap)# match mpls experimental topmost 2
DES-7200(config-cmap)# exit
DES-7200(config)# policy-map policy1
DES-7200(config-pmap)# class map1
DES-7200(config-pmap-c)# set cos 1 none-tos
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
DES-7200(config)# exit
```

```
DES-7200# show policy-map policy1


 Policy Map policy1
     Class map1
       set cos 1 none-tos
DES-7200#
```

Related commands

Command	Description
class-map	Create one class map in order to identify objects and classify traffic as per certain matching rules.
policy-map	Create or modify a policy map, which can be associated to one or multiple interfaces as QoS service policy.
set cos	Re-mark the CoS value of packet.
show class-map	Display the specific contents of all class maps or the specified class map.

Platform description

Supported by DES-7200 series devices.

4 WRED Configuration Commands

4.1 Default Confiiugrations

	Parameter		Default Value	
Default configuration	Queue1	Threshold1	CoS	0，1，2，3，4，5，6，7
			WRED-drop	100%low，100%high
			random-detectprobability	60%
		Threshold2	CoS	NONE
			WRED-drop	80% low，100%high
			random-detectprobability	80%

Usage guidelines	By default, all wrr-queues are mapped to the threshold 1 of queue 1; the min-threshold value equals to the max-threshold and is 100%, representing the WRED function is disabled.

4.2 Related Configuration Commands

4.2.1 wrr-queue cos-map

Use this command to map the CoS value to a threshold for a specified queue in the interface configuration mode. Use the **no** form of this command to return to the default settings.

wrr-queue cos-map *threshold_id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]

Parameter description

Parameter	Description
queue_id	Interface queue id.

	cos_value	CoS value, in the range of 0-7

Default The cos value is the threshold for queue1.

Command mode Interface configuration mode.

Usage guidelines DSCP-threshold mapping can be enabled by mapping DSCP-CoS to CoS-threshold.

When all CoS values are mapped to one threshold on the interface, it changes the enabled WRED to RED.

Examples The following example shows how to set the cos1 and cos6 for queue2 (For the configuration of cos-queue mapping, use the **priority-queue cos-map** command in the global configuration mode.)

```
DES-7200(config-if)# wrr-queue cos-map 2 1 6
```

4.2.2 wrr-queue random-detect min-threshold

Use this command to set the minimum WRED threshold for the specified queue on the interface. Use the **no** form of this command to remove the minimum WRED threshold. The min-threshold value must be less than the max-threshold in the same group.

wrr-queue random-detect min-threshold *queue_id thr1* [*thr2 thr3*]

no wrr-queue random-detect min-threshold *queue_id*

Parameter description

Parameter	Description
queue_id	The interface queue id.
thr1	The min-threshold value for queue1.
thr2	The min-threshold value for queue2.
thr3	The min-threshold value for queue3.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines	Several physical ports could be in a WRED interface group, which requires for the completely-consistent WRED settings for those physical member ports. The related WRED parameters configured for one physical port are valid for other member ports in the same interface group. For DES-7200 series, each physical port corresponds to one interface group. DES-7200 series switches support to set the threshold for 2 queues only.
Examples	The following example shows how to set the min-threshold for queue1 on an interface: `DES-7200(config-if)# wrr-queuerandom-detect min-threshold 1 68 69 70`

4.2.3 wrr-queue random-detect probability

Use this command to set all maximum drop probability for the specified queue on the interface. Use the **no** form of this command to remove the maximum drop probability.

wrr-queue random-detect probability *queue_id prob1 [prob2 prob3]*

no wrr-queue random-detect probability *queue_id*

Parameter description

Parameter	Description
queue_id	The interface queue id.
prob1	The maximum drop probability for queue1.
prob2	The maximum drop probability for queue2.
prob3	The maximum drop probability for queue3.

Default	N/A.
Command mode	Interface configuration mode.
Usage guidelines	Several physical ports could be in a WRED interface group, which requires for the completely-consistent WRED settings for those physical member ports. The related WRED parameters configured for one physical port are valid for other member ports in the same interface group.

For DES-7200 series, each physical port corresponds to one interface group.

DES-7200 series support to set the maximum drop probability for 2 queues only.

Examples

The following example shows how to set the maximum drop probability for queue1 on an interface:

```
DES-7200(config-if)# wrr-queuerandom-detect probability
1 61 62 63
```

4.3 Showing Commands

4.3.1 show queueing wred interface

Use this command to show all WRED settings on an interface in the privileged user mode.

show queueing wred interface<*interface*>

Parameter description

Parameter	Description
interface	The physical interface number.

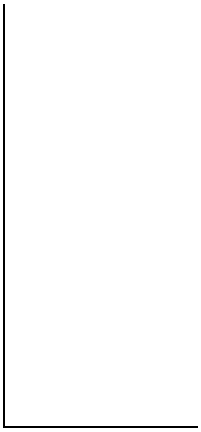
Command mode

Privileged user mode.

Examples

The following example shows the result of the command **show queueing wred interface g0/1**:

```
-----   -----   -----   ------   -----   -----   ------
qid max_1 min_1 prob_1 max_2 min_2 prob_2 max_3 min_3
prob_3
-----   -----   -----   ------   -----   -----   ------
1    0    0    90     0     0     91      0     0     92
2    88   66   90     87    55    91      86    66    92
3    0    0    0      0     0     0       0     0     0
4    0    0    0      0     0     0       0     0     0
5    88   66    0     89    67    0       90    68    0
6    0    0    0      0     0     0       0     0     0
7    0    0    0      0     0     0       0     0     0
8    0    0    0      0     0     0       0     0     0
cos  qid  threshold_id
```



| --- | --- | --- |
0	1	1
1	2	1
2	3	1
3	4	2
4	5	1
5	6	3
6	7	2
7	8	1