QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ACL & QoS Configuration Commands

www.qtech.ru

Оглавление

1. ACL & QOS CONFIGURATION COMMANDS

ACL Commands

Command ID Table

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,AHP, ESP, PCP, PIM 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 and 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: 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.

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.
established	Match the RST or ACK bit of the TCP flag.
text	Remark text
In	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface
{rule mask offset}$^{+}$	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table "+" sign indicates at least one group
log	Output the matching syslog when the packet matches the ACL rule.

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 source 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
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			

access-list

Use this command to create an access list to filter data packets. Use the **no** form of this command to remove the specified access list.

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*] [**log**]

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*] | [**dscp**

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

3. Extended MAC access list (700 to 799)

access-list *id* {**deny** | **permit**} {**any** | **host** *source-mac-address* | *source-mac-address mask* } {**any** |

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

4. Extended expert access list (2700 to 2899)

Parameter	Description
Id	Access list number. 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)
dscp	Differentiated service code point
dscp	Code point value, ranging from 0 to 63
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name
host source-mac-address	Source physical address
host	Destination physical address

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

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

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

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

destination-mac-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.
established	Match the RST or ACK bits, not other bits of the TCP flag.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

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 layer-3 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

The UDF headers are as below:

- l2-head
- l3-head
- l4-head
- l5-head

Run **no** {**sn** | **permit** | **deny**} in ACL mode to delete ACEs.

Configuration Examples

1. Example of the standard IP ACL

The following basic IP ACL allows the packets whose source IP addresses are

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

192.168.1.64 - 192.168.1.127 to pass:

2. Example of the extended IP ACL

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

3. Example of the extended MAC ACL

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

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:

```
QTECH(config)#access-list 702 deny host 00d0f8000c0c any aarp QTECH(config)#
interface gigabitethernet 1/1
QTECH(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.

```
QTECH(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
QTECH(config)# access-list 2702 permit any any any any QTECH(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.

Platform Description

N/A

access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

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

no access-list ***id*** list-remark

Parameter	Description
id	Access list number. 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.
text	Comment that describes the access list.

Parameter	Description
Defaults	The access lists have no remarks by default.

Command Mode

Global configuration mode

❖ Usage Guide

You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.

Configuration Examples

```
QTECH(config)# ip access-list extended 100
QTECH(config)# access-list 100 list-remark this acl is to filter the host 192.168.4.12
```

The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL100.

Command	Description
show access- lists	Displays all access lists, including the remarks for the access lists.
show access-lists *id*	Displays the access list of a specified number, including the remarks for the access list.
show access-lists *name*	Displays the access list of a specified name, including the remarks for the access list.

Related Commands

Platform Description

access-list remark

Use this command to write a helpful comment (remark) for an entry in a numbered access list. Use the **no** form of this command to remove the remark.

access-list *id* **remark** *text***no access-list** *id* **remark** *text*

Parameter	Description
id	Access list number. 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.
text	Comment that describes the access list entry.

Defaults

The access list entries have no remarks by default.

Command Mode

Global configuration mode

Usage Guide

You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.

Configuration Examples

Related Commands

Platform Description

The following example writes a comment for an entry in ACL102.

```
QTECH(config)# access-list 102 remark deny-host-10.1.1.1
```

Command	Description
show access-lists	Displays all access lists, including the remarks for the access list entries.
show access-lists *id*	Displays the access list of a specified number, including the remarks for the access list entry.
show access-lists *name*	Displays the access list of a specified name, including the remarks for the access list entry.

clear counters access-list

Use this command to clear counters of packets matching ACLs.

clear counters access-list [*id* **|** *name*]

Parameter	Description
id	Access list number
name	Access list name

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the counters of packets matching the specified or all ACLs.

Configuration Examples

```
QTECH #show access-lists 2700 expert access-
list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any  (88 matches)
    20 deny tcp any any eq login any any (33455 matches)
    30 permit tcp any any host 192.168.6.9 any (10 matches)

QTECH# clear counters access-list 2700 QTECH #show
access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
    20 deny tcp any any eq login any any
    30 permit tcp any any host 192.168.6.9 any
```

The following example clears the packet matching counter of ACL No. 2700:

Command	Description
expert access-list	Defines an expert ACL.
deny	Defines a deny ACL entry.
permit	Defines a permits ACL entry.

Related Commands

Platform Description

N/A

clear access-list counters

Use this command to clear counters of packets matching the deny entries in ACLs.

clear access-list counters [*id* | *name*]

Parameter	Description
id	Access list number

name	Access list name

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the counters of packets matching the deny entries in ACLs.

Configuration Examples

The following example clears the packet matching counter of ACL No. 1: Before configuration:

```
QTECH #show access-lists ip access-list
standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches) (10 packets
    filtered)
```

After configuration:

```
QTECH# end
QTECH# clear access-list counters QTECH# show
access-lists
ip access-list standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches)
```

Command	Description
expert access-list	Defines an expert ACL.
deny	Defines a deny ACL entry.
permit	Defines a permits ACL entry.

Related Commands

Platform Description

N/A

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.

1. Standard IP ACL

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

2. Extended IP ACL

[*sn*] **deny** *protocol source source-wildcard destination destination-wildcard* [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*] [**ecn** *ecn*]] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

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 Protocol (TCP)

[*sn*] **deny tcp** { *source source-wildcard* **| host** *Source* **| any** } { *destination destination-wildcard* **| host** *destination* **| any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* **| established**]

- User Datagram Protocol (UDP)

[*sn*] **deny udp** { *source source –wildcard* **| host** *source* **| any** }] { *destination destination-wildcard* **| host** *destination* **| any** }] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**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*] | [**dscp** *dscp*]] [**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** } { *destinationdestination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**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*] | [**dscp** *dscp*]] [**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** }] { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **deny udp** [[**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*] | [**dscp** *dscp*]] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Parameter Description

Address Resolution Protocol (ARP)

[sn] **deny arp** {**vid** vlan-id}[**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**}

❖ 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** }

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

User Datagram Protocol **(UDP)**

[sn] **deny udp** { *source-ipv6-prefix/prefix-length* | **host** *source-ipv6-address* | **any** }

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

Parameter	Description
Sn	ACL entry sequence number
Deny	If not matched, access is denied.
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
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.
established	Match the RST or ACK bits, not other bits of the TCP flag.
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

Defaults

No entry

Command mode

ACL configuration mode.

Usage Guide

Use this command to configure the filtering entry of ACLs in ACL configuration mode.

Configuration Examples

```
QTECH(config)#expert access
list extended 2702 QTECH(config
exp
nacl)#deny tcp host 192.168.4.12
host 0013.0049.8272 any any
QTECH(config
exp
nacl)#permit any any any any
QTECH(config
exp
nacl)#show access
lists
```

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.

```
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 QTECH(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:

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

```
QTECH(config)#mac access-list extended mac1 QTECH(config-mac-nacl)#deny
host 0013.0049.8272 any aarp QTECH(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp QTECH(config-
mac-nacl)#exit
QTECH(config)# interface gigabitethernet 1/1
QTECH(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:

```
QTECH(config)#ip access-list standard 34 QTECH(config-ext-
nacl)# deny host 192.168.4.12 QTECH(config-ext-nacl)#show
access-lists
ip access-list standard 34 10 deny host
192.168.4.12 QTECH(config-ext-nacl)#exit
QTECH(config)# interface gigabitethernet 1/1
QTECH(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:

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

Command	Description
show access-lists	Displays all ACLs.
ipv6 traffic-filter	Applies the extended IPv6 ACL on the interface.
ip access-group	Applies the IP ACL on the interface.
mac access-group	Applies the extended MAC ACL on the interface.
ip access-list	Defines an IP ACL.
mac access-list	Defines an extended MAC ACL.
expert access-list	Defines an extended expert ACL.
ipv6 access-list	Defines an extended IPv6 ACL.
permit	Permits the access.

Related Commands

Platform Description

N/A

expert access-group

Use this command to apply the specified expert access list on the specified interface or globally. 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
id	Expert access list number: 2700 to 2899
name	Name of the expert access list
in	Specifies filtering on inbound packets.
out	Specifies filtering on outbound packets.

Parameter Description

Defaults

No expert access list is applied on the interface or globally.

Command mode

Global/Interface configuration mode.

Usage Guide

This command is used to apply the specified access list globally or on the interface to control the input and output data streams. Use the **show access-group** command to view the setting. Use the **expert access-group {** *id* | *name* **} { in | out } counter-only** command on the interface to only collect packet statistics and not filter packets.

Configuration Examples

The following example shows how to apply the **access-list** ***accept***_00d0f8xxxxxx only to Gigabit interface 0/1:

Related Commands

Platform Description

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

The following example applies the ACL numbered 2700 on interface fastEthernet0/1 to collect statistics on incoming packets:

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)#expert access-group 2700 in counter-only
```

Command	Description
show access-group	Displays the ACL configuration.

N/A

expert access-list advanced

Use this command to create an advanced expert access list and place the device in expert advanced access list configuration mode. Use the **no** form of this command to remove the advanced expert access list.

expert access-list advanced ***name***

no expert access-list advanced *name*

Parameter Description

Parameter	Description
name	Name of the advanced expert access list

Defaults

N/A

Command mode

Global configuration mode

Usage Guide

Use this command to create an advanced expert access list (namely, ACL80) to match your custom fields.

Configuration Examples

```
QTECH(config)# expert access-list advanced adv-acl
QTECH(config-exp-dacl)# show access-lists
```

The following example creates an advanced expert access list named adv-acl.

Related Commands

Platform Description

```
expert access-list advanced adv-acl
```

Command	Description

show access-lists	Displays all access lists.
show access-lists *name*	Displays the access list of a specified name.

N/A

expert access-list extended

Use this command to create an extended expert access list. 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	Extended expert access list number: 2700 to 2899
name	Name of the extended expert access list

Defaults

N/A

Command mode

Global configuration mode.

Usage Guide

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

Configuration Examples

Create an extended expert ACL named exp-acl:

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

Create an extended expert ACL numbered 2704:

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

Related Commands

Command	Description

show access-lists	Displays the extended expert ACLs

Platform Description

N/A

expert access-list counter

Parameter Description

Use this command to enable the counter of packets matching the specified expert access list. Use the

no form of this command to disable this function.

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

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

Parameter	Description
id	Expert access list number: 2700 to 2899.
name	Name of the access list.

Defaults

The counter of the packets matching the expert access list is disabled.

Command mode

Global configuration mode

Usage Guide

Use this command to enable the counter of packets matching the specified expert access list, so that you can analyze the counters to learn whether the network is attacked by the illegal packets.

Configuration Examples

```
QTECH(config)# expert access-list counter exp-acl
QTECH(config)# show access-lists
expert access-list extended exp-acl
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (16 matches)
 20 deny tcp any any eq login any any (78 matches)
```

The following example enables the counter of packets matching the extended expert access list named exp-acl:

The following example disables the counter of packets matching the extended expert access list named exp-acl.

```
QTECH(config)#no expert access-list counter exp-acl QTECH(config)#
show access-lists
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
 20 deny tcp any any eq login any any
```

Related Commands

Command	Description
show access-lists	Displays the extended expert ACL.

Platform

N/A

Description

expert access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

expert access-list new-fragment-mode { *id* **|** *name* }

no expert access-list new-fragment-mode { *id* **|** *name* }

Parameter Description

Parameter	Description
id	Expert access list number: 2700 to 2899.
name	Name of the expert access list.

Defaults

Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

Command mode

Global configuration mode

Usage Guide

Use this command to switch and control the matching mode of access rules to fragmentation packets.

Configuration Examples

Related Commands

Platform Description

The following example switches the matching mode of fragmentation packets for the ACL 2700 from the default mode to a new matching mode:

```
QTECH(config)#expert access-list new-fragment-mode 2700
```

Command	Description
-	-

N/A

expert access-list resequence

Use this command to resequence an expert access list. Use the no form of this command to restore the default order of access entries.

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

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

Parameter	Description
Id	Expert access list number: 2700 to 2899.
name	Name of the expert access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use this command to change the order of the access entries.

Configuration Examples

```
QTECH# show access-lists
expert access-list extended exp-acl
 10 permit ip any any any any
 20 deny ip any any any any
```

The following example resequences entries of expert access list “exp-acl”: Before the configuration:

```
QTECH# config
QTECH(config)# expert access-list resequence exp-acl 21 43 QTECH(config)#
exit
QTECH# show access-lists
expert access-list extended exp-acl
 21 permit ip any any any any
 64 deny ip any any any any
```

After the configuration:

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description

N/A

global access-group

Use this command to apply the global access list on the interface. Use the **no** form of this command to remove the global access list from the interface.

global access-group

no global access-group

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the global access list is applied on the interface.

Command mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# interface fastEthernet 0/0
QTECH(config-if-GigabitEthernet 0/0)#global access-group
```

The following example applies the global access list on interface fastEthernet0/0.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip access-group

Use this command to apply a specific access list globally or to an interface. Use the **no** form of this command to remove the access list from the interface.

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

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

Parameter Description

Parameter	Description
id	IP access list or extended IP access list number: 1 to 199, 1300 to 2699
name	Name of the IP ACL
in	Filters the incoming packets of the interface.
out	Filters the outgoing packets of the interface.

Defaults

No access list is applied globally or on the interface by default.

Command mode

Global, interface

Usage Guide

Use this command to control access to a specified interface, VXLAN or globally.

Configuration Examples

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

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

Related Commands

Command	Description
access-list	Defines an ACL.
show access-lists	Displays all ACLs.

Platform Description

N/A

ip access-list

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

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

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

Parameter Description

Parameter	Description
id	Access list number: Standard: 1 to 99, 1300 to 1999; Extended: 100 to 199, 2000 to 2699.
name	Name of the access list

Defaults

N/A

Command mode

Global configuration mode

Usage Guide

Configure a standard access list if you need to filter on source address only. If you want to filter on anything other than source address, you need to create an extended access list.

Refer to **deny** or **permit** in the two modes. Use the **show access-lists** command to display the ACL configurations**.**

Configuration Examples

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

The following example creates a standard access list named std-acl.

The following example creates an extended ACL numbered 123:

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

Related Commands

Command	Description
show access-lists	Displays all ACLs.

Platform Description

N/A

ip access-list log-update interval

Parameter Description

Use this command to configure the interval at which the IPv4 access list log is updated. Use the **no**

form of this command to restore the default interval.

ip access-list log-update interval ***time***

no ip access-list log-update interval

Defaults

The default interval at which the IPv4 access list log is updated is 5 minutes.

Parameter	Description
time	For the access rule with the log option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specified flow is output every 5 minutes. 0 indicates that no ACL logging is output.

Command mode

Global configuration mode

Usage Guide

Use this command to configure the interval at which the IPv4 access list log is updated.

Configuration Examples

```
QTECH# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# ip access-
list log-update interval 10
```

The following example configures the interval for the IPv4 access list log update to 10 minutes:

Related Commands

Command	Description
ip access-list	Defines an IPv4 access list.
deny	Defines the **deny** access entries.
permit	Defines the **permit** access entries.
show running	Displays running configurations of the device.

Platform Description

N/A

ip access-list counter

Use this command to enable the counter of packets matching the standard or extended IP access list. Use the **no** form of this command to disable the counter.

ip access-list counter { *id* | *name* }

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

Parameter Description

Parameter	Description
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the IP access list.

Defaults

The counter of packets matching the standard or extended IP access list is disabled by default.

Command mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# ip access-list counter std-acl QTECH(config-
std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255 (999 matches)
20 deny host 5.5.5.5 time-range tm (2000 matches)
```

The following example enables the counter of packets matching the standard access list:

```
QTECH(config)#no ip access-list counter std-acl QTECH(config-
std-nacl)# show access-lists
ip access-list standard std-acl 10 permit
 195.168.6.0 0.0.0.255
 20 deny host 5.5.5.5 time-range tm
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description

N/A

ip access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets of standard or extended IP access list. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

ip access-list new-fragment-mode { *id* **|** *name* }

no ip access-list new-fragment-mode { *id* **|** *name* }

Parameter Description

Parameter	Description
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the standard or extended IP access list

Defaults

Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

Command mode

Global configuration mode

Usage Guide

This command is used to switch and control the fragmentation packet matching mode of access rules.

Configuration Examples

Related Commands

Platform Description

The following example switches the fragmentation packet matching mode of the ACL 100 from the default mode to a new mode:

```
QTECH(config)#ip access-list new-fragment-mode 100
```

Command	Description
N/A	N/A

N/A

ip access-list resequence

Use this command to resequence a standard or extended IP access list. Use the **no** form of this

Parameter Description

Parameter	Description
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the standard or extended IP access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

command to restore the default order of access entries. **ip access-list resequence** { *id* | *name* } *start-sn inc-sn* **no ip access-list resequence** { *id* | *name* }

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use this command to change the order of the access entries.

Configuration Examples

```
QTECH# show access-lists ip access-list
standard 1 10 permit host 192.168.4.12
20 deny any any
```

The following example resequences entries of ACL1: Before the configuration:

After the configuration:

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

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description

N/A

ipv6 access-list

Use this command to create an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the **no** form of this command to remove the access list.

ipv6 access-list *name*

no ipv6 access-list *name*

Parameter Description

Parameter	Description
name	Name of the IPv6 access list.

Defaults

N/A

Command mode

Global configuration mode

Usage Guide

To filter the IPv6 packets through the access list, you need to define an IPv6 access list by using the

ipv6 access-list command.

Configuration Examples

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

QTECH(config-ipv6-nacl)#
```

The following example creates an IPv6 access list named v6-acl:

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description

N/A

ipv6 access-list counter

Use this command to enable the counter of packets matching the IPv6 access list. Use the **no** form of this command to disable the counter.

ipv6 access-list counter ***name***

no ipv6 access-list counter *name*

Parameter Description

Parameter	Description
name	Name of the IPv6 access list.

Defaults

-

Command mode

Global configuration mode

Usage Guide

Use this command to enable the counter of packets matching the IPv6 access list to monitor the IPv6 packets matching and filtering.

Configuration Examples

```
QTECH(config)# ipv6 access-list v6-acl QTECH(config-
ipv6-nacl)# show access-lists ipv6 access-list acl-v6
 10 permit icmp any any (7 matches)
20 deny tcp any any (7 matches)
```

The following example enables the counter of packets matching the IPv6 access list named v6-acl:

```
QTECH(config)#no ipv6 access-list v6-acl counter QTECH(config-
ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
 10 permit icmp any any
20 deny tcp any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description

N/A

ipv6 access-list log-update interval

Use this command to configure the interval at which the IPv6 access list log is updated. Use the no

form of this command to restore the default interval.

ipv6 access-list log-update interval *time*

no ipv6 access-list log-update interval

Parameter Description

Parameter	Description
time	For the access rule with the logging option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specific flow is output every 5 minutes. 0 indicates that no ACL logging is output.

Defaults

By default, the value is 5 minutes.

Command mode

Global configuration mode

Usage Guide

Use this command to configure the interval at which the IPv6 access list log is updated.

Configuration Examples

```
QTECH# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# ipv6
access-list log-update interval 9
```

The following example configures the interval for the IPv6 access list log update to 10 minutes:

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list.
deny	Defines the deny access entries.
permit	Defines the permit access entries.

show running	Displays the running configurations of the the device.

Platform Description

N/A

ipv6 access-list resequence

Use this command to resequence an IPv6 access list. Use the **no** form of this command to restore the default order of access entries.

ipv6 access-list resequence *name start-sn inc-sn*

no ipv6 access-list resequence ***name***

Parameter Description

Parameter	Description
name	Name of the IPv6 access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use this command to change the order of the access entries.

Configuration Examples

```
QTECH# show access-lists ipv6 access-
list v6-acl
 10 permit ipv6 any any
 20 deny ipv6 any any
```

The following example resequences entries of IPv6 access list “v6-acl”:

Before the configuration:

After the configuration:

```
QTECH# config
QTECH(config)# ipv6 access-list resequence v6-acl 21 43 QTECH(config)#
exit
QTECH# show access-lists ipv6 access-
list v6-acl
 21 permit ipv6 any any
 64 deny ipv6 any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description

N/A

ipv6 traffic-filter

Use this command to apply an IPV6 access list on the specified interface/VXLAN. Use the **no** form of the command to remove the IPv6 access list from the interface.

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

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

Parameter Description

Parameter	Description
name	Name of IPv6 access list
in	Specifies filtering on inbound packets
out	Specifies filtering on outbound packets

Defaults

N/ACommand mode

Interface configuration mode.

Usage Guide

Use this command to apply the IPv6 access list to a specified interface to filter the inbound or outbound packets.

Configuration Examples

The following example applies the IPv6 access list named **v6-acl** to interface GigabitEthernet 0/1:

```
QTECH(config)# interface GigaEthernet 0/1 QTECH(config-if)#
ipv6 traffic-filter v6-acl in
```

Related Commands

Command	Description
show access-group	Displays ACL configurations on the interface.

Platform Description

N/A

list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

list-remark *text*

no list-remark

Parameter Description

Parameter	Description
text	Comment that describes the access list.

Defaults

The access lists have no remarks by default.

Command mode

ACL configuration mode

Usage Guide

You can use this command to write a helpful comment for a specified access list.

Configuration Examples

```
QTECH(config)# ip access-list extended 102
QTECH(config-ext-nacl)# list-remark this acl is to filter the host 192.168.4.12
QTECH(config-ext-nacl)# show access-lists ip access-
list extended 102
deny ip host 192.168.4.12 any 1000 hits
this acl is to filter the host 192.168.4.12
QTECH(config-ext-nacl)#
```

The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL102.

Related Commands

Command	Description
show access-lists	Displays all access lists.
ip access-list	Defines an IPv4 access list.
access-list list remark	Adds a helpful comment for an access list in global configuration mode.

Platform Description

N/A

mac access-group

Use this command to apply the specified MAC access list globally or on the specified interface.. Use the **no** form of the command to remove the access list from the interface.

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

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

Parameter Description

Parameter	Description
id	MAC access list number. The range is from 700 to 799.
name	Name of the MAC access list
in	Specifies filtering on the inbound packets.

out	Specifies filtering on the outbound packets.

Defaults

No MAC access list is applied by default.Command mode

Global/Interface configuration mode.

Usage Guide

Use this command to apply the access list globally or to the interface to filter the inbound or outbound packets based on the MAC address.

Configuration Examples

The following example applies the MAC access-list **accept_00d0f8xxxxxx_only** to interface GigabitEthernet 1/1:

```
QTECH(config)# interface GigaEthernet 1/1 QTECH(config-
if-GigabitEthernet 1/1)# mac access-group
accept_00d0f8xxxxxx_only in
```

Related Commands

Command	Description
show access-group	Displays the ACL configuration on the interface.

Platform Description

N/A

mac access-list extended

Use this command to create an extended MAC access list. Use the no form of the command to remove the MAC access list.

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

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

Command	Description
how access-lists	Displays all access lists.

Parameter Description

Parameter	Description
id	Extended MAC access list number. The range is

	from 700 to 799.
name	Name of the extended MAC access list

Defaults

N/A

Command mode

Global configuration mode.

Usage Guide

To filter the packets based on the MAC address, you need to define a MAC access list by using the

mac access-list extended command.

Configuration Examples

The following command creates an extended MAC access list named mac-acl:

```
QTECH(config)# mac access-list extended mac-acl
QTECH(config-mac-nacl)# show access-lists mac access-list extended mac-acl
```

The following command creates an extended MAC access list numbered 704:

```
QTECH(config)# mac access-list extended 704
QTECH(config-mac-nacl)# show access-lists mac access-list extended 704
```

Related Commands

Platform Description

N/A

mac access-list counter

Use this command to enable the counter of packet matching the extended MAC access list. Use the

no form of this command to disable the counter.

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

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

Parameter	Description
name	Name of the extended MAC access list

id	Extended MAC access list number. The range is from 700 to 799.

Defaults

The counter is disabled by default.

Command mode

Global configuration mode

Usage Guide

Use this command to enable the counter of packets matching the MAC access list to monitor the packets matching and filtering.

Configuration Examples

```
QTECH(config)# mac access-list counter mac-acl
QTECH(config)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any (170 matches)
 20 deny any any etype-any cos 6 (239 matches)
```

The following example enables the counter of packet matching the extended MAC access list named mac-acl:

The following example disables the counter of packet matching the extended MAC access list named mac-acl:

```
QTECH(config)#no mac access-list counter mac-acl
QTECH(config)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any
 20 deny any any etype-any cos 6
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description

N/A

mac access-list resequence

Use this command to resequence an extended MAC access list. Use the no form of this command to restore the default order of access entries.

mac access-list resequence { *id* | *name* } *start-sn inc-sn* no mac access-list resequence { *id* | *name* }

Parameter	Description
id	Extended MAC access list number: 700 to 799.
name	Name of the extended MAC access list

start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use this command to change the order of the access entries.

Configuration Examples

```
QTECH# show access-lists
mac access-list extended mac-acl
 10 permit any any etype-any
 20 deny any any etype-any
```

The following example resequences entries of extended MAC access list “mac-acl”:

Before the configuration:

After the configuration:

```
QTECH# config
QTECH(config)# mac access-list resequence exp-acl 21 43 QTECH(config)#
exit
QTECH# show access-lists
mac access-list extended mac-acl
 21 permit any any etype-any
 64 deny any any etype-any
```

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description

N/A

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.

1. Standard IP ACL

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

2. Extended IP ACL

[*sn*] **permit protocol** *source source-wildcard destination destination-wildcard* [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

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

Transmission Control Protocol (TCP)

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

User Datagram Protocol (UDP)

[*sn*] **permit udp** { *source source –wildcard* **| host** *source* **| any** } { *destination destination-wildcard* **| host** *destination* **| any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

3. Extended MAC ACL

[sn] **permit** { **any | host** source-mac-address | source-mac-address mask} { **any | host** destination-mac-address | destination -mac-address mask } [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*] | [**dscp** *dscp*]] [**fragment**] [**range** *lower upper*] [**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] | [**dscp** dscp]] [**fragment**] [**range** lower upper] [**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] | [**dscp** dscp]] [**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** } { destination destination-wildcard **| host** destination | **any** } { **host** destination-mac-address **| any** }[[**precedence** precedence] [**tos** tos] | [**dscp** dscp]] [**fragment**] [**range** lower upper] [**time-range** time-range-name] [**match-all** tcp-flag **| established**]

Parameter Description

Parameter	Description
sn	ACL entry sequence number
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

User Datagram Protocol (UDP)

[*sn*] **permit udp** [**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*] | [**dscp** *dscp*]] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **permit arp** {**vid** *vlan-id***}** [**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] **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**] [**range** lower upper] [**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** }

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

User Datagram Protocol (UDP)

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

{ destination-ipv6-prefix / prefix-length **| host** destination-ipv6-address **| any** } [**dscp**

dscp][**flow-label** flow-label] [**fragment**] [**range** lower upper] [**time-range** time-range-name]

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
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.

established	Match the RST or ACK bits, not other bits of the TCP flag.
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

Defaults

N/A

Command mode

ACL configuration mode.

Usage Guide

Use this command to configure the permit conditions for the ACL in ACL configuration mode.

Configuration 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.

```
QTECH(config)#expert access-list extended exp-acl
QTECH(config-exp-nacl)#permit tcp host 192.168.4.12 host 0013.0049.8272 any any
QTECH(config-exp-nacl)#deny any any any any QTECH(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 QTECH(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:

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

```
QTECH(config)#mac access-list extended 702
QTECH(config-mac-nacl)#permit host 0013.0049.8272 any aarp QTECH(config-
mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702 QTECH(config-
mac-nacl)#exit QTECH(config)#interface gigabitethernet 1/1
QTECH(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:

```
QTECH(config)#ip access-list standard std-acl QTECH(config-
std-nacl)#permit host 192.168.4.12 QTECH(config-std-nacl)#show
access-lists
ip access-list standard std-acl 10 permit host
  192.168.4.12
QTECH(config-std-nacl)#exit
QTECH(config)# interface gigabitethernet 1/1 QTECH(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:

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

Related Commands

Command	Description
show access-lists	Displays all access lists.
ipv6 traffic-filter	Applies the extended IPv6 access list to the interface.
ip access-group	Applies the IP access list to the interface.
mac access-group	Applies the extended MAC access list to the interface.
ip access-list	Defines an IP access list.
mac access-list	Defines an extended MAC access list.
expert access-list	Define an extended expert access list.
ipv6 access-list	Defines an extended IPv6 access list.
deny	Defines the **deny** access entry.

Platform Description

N/A

redirect destination interface

Use this command to redirect the traffic matching the access list to the specified interface. Use the **no** form of this command to remove the redirection.

redirect destination interface *interface-name* **acl** { *id* | *name* } **in** **no redirect destination interface** *interface-name* **acl** { *id* | *name* } **in**

Parameter Description

Parameter	Description
interface-name	Redirect interface
id	Access list number
name	Access list name

Defaults

No redirection is configured.

Command mode

Interface configuration mode

Usage Guide

Use this command to configure access redirection, namely, to redirect the traffic matching the access list to the specified interface. You can monitor the operation of a specified access list by using this command.

Configuration Examples

```
 QTECH(config)# interface gigabitEthernet 0/3
QTECH(config-if-GigabitEthernet 0/3)# redirect destination interface gigabitEthernet 0/2
acl1 in
```

The following example configures access redirection.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

remark

Use this command to write a helpful comment (remark) for an entry in the access list. Use the **no** form of this command to remove the remark.

[*sn*] **remark** *text*

no [*sn*] **remark**

Parameter Description

Parameter	Description
text	Comment that describes the access entry.
sn	The sequence number of the ACE.

Defaults

The access entries have no remarks.

Command mode

ACL configuration mode.

Usage Guide

Use this command to write a helpful comment for an access entry.

Up to 100 characters are allowed in the remark.

Two access entry remarks in one access list entry are not allowed. Removing an access entry may delete the remark for it as well.

If sn is specified, the remark is applied to the specified ACE; otherwise, the remark is applied to the last ACE.

Configuration Examples

```
QTECH(config)# ip access-list extended 102 QTECH(config-
ext-nacl)# remark first_remark
QTECH(config-ext-nacl)# 10 permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0 QTECH(config-
ext-nacl)# 10 remark second_remark
QTECH(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0 QTECH(config-
ext-nacl)# end
QTECH#
```

The following example writes remarks for the entry in extended IP access list 102.

Related Commands

Command	Description
show access-lists	Displays all access lists.
ip access-list	Defines an IP access list.

Platform Description

N/A

security access-group

Use this command to configure an interface secure channel. Use the **no** form of this command to restore to default settings.

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

no security access-group

Parameter Description

Parameter	Description
id	Access list number.
name	Name of the access list.

Defaults

N/A

Command mode

Interface configuration mode

Usage Guide

If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a secure channel for the users on the specified interface to access the external network without authentication.

Configuration Examples

```
QTECH(config)# interface GigaEthernet 1/1
QTECH(config-if-GigabitEthernet 1/1)# security access-group 1
```

The following example configures a secure channel on interface GigaEthernet 1/1:

Related Commands

Command	Description
show secu-acl	Displays the secure channel configuration.

Platform Description

N/A

security global access-group

Use this command to configure the global secure channel.

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

no security global access-group

Parameter Description

Parameter	Description
id	Access list number.
name	Name of the access list.

Defaults **-**

Command mode

Global configuration mode

Usage Guide

If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a global secure channel for some users to access the external network without authentication.

Configuration Examples

```
 The following example configures a global secure channel.
QTECH(config)#security global access-group 1
```

Related Commands

Command	Description
show secu-acl	Displays the secure channel configuration..

Platform Description

N/A

security uplink enable

Use this command to configure an exceptional interface of the global secure channel.

security uplink enable

no security uplink enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The global secure channel takes effect on all interfaces by default.

Command mode

Interface configuration mode.

Usage Guide

The global secure channel takes effect on all interfaces by default. To disable the secure channel function on some interfaces, you can used this command to configure the interface as exceptional

Configuration Examples

```
QTECH(config)# interface GigaEthernet 1/1
QTECH(config-if-GigabitEthernet 1/1)# security uplink enable
```

The following example configures interface GigaEthernet 1/1 as an exceptional interface of the secure channel.

Related Commands

Command	Description
show secu-acl	Displays the secure channel

	configuration.

Platform Description

N/A

show access-group

Use this command to display the access list applied to the interface.

show access-group [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface	Interface name

Defaults -

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the access list configuration on the specified interface. If no interface is specified, access list configuration on all interfaces is displayed.

Configuration

```
QTECH# show access-group
```

Examples

```
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	Applies the IP access list to the interface.
mac access-group	Applies the MAC access list to the interface.
expert access-group	Applies the expert access list to the interface.
ipv6 traffic-filter	Applies the IPv6 access list to the interface.

Platform Description

N/A

show access-lists

Use this command to display all access lists or the specified access list.

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

Parameter Description

Parameter	Description
id	Access list number
name	Name of the IP access list
summary	Access list summary

Defaults

N/A

Command mode

Global configuration mode

Usage Guide

Use this command to display the specified access list. If no access list number or name is specified, all the access lists are displayed.

Configuration Examples

```
QTECH# show access-lists n_acl ip access-list
standard n_acl QTECH# show access-lists 102
ip access-list extended 102
QTECH# show access-lists
ip access-list standard n_acl ip access-list
extended 101
permit icmp host 192.168.1.1 any log (1080 matches) permit tcp
  host 1.1.1.1 any established
  deny ip any any (80021 matches) mac access-list
extended mac-acl expert access-list extended exp-
acl ipv6 access-list extended v6-acl
petmit ipv6 ::192.168.4.12 any (100 matches)
deny any any (9 matches)
```

Related Commands

Command	Description
ip access-list	Defines an IP access list.
mac access-list	Defines an extended MAC access list.
expert access-list	Defines an extended expert access list.
ipv6 access-list	Defines an extended IPv6 access list.

Platform Description

N/A

show expert access-group

Use this command to display the expert access list applied to the interface.

show expert access-group [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults -

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the expert access list configured on the interface. If no interface is specified, the expert access lists on all interfaces are displayed.

Configuration Examples

```
QTECH# show expert access-group interface gigabitethernet 0/2 expert access-group
ee in
Applied On interface GigabitEthernet 0/2.
```

Related

Command	Description
xpert access-list	Defines an extended expert access list.

Platform Description

N/A

show ip access-group

Use this command to display the standard and extended IP access lists on the interface.

show ip access-group [**interface** *interface-name*]

Parameter Description

Parameter	Description
Interface Interface-name	Interface name

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the standard and extended IP access lists configured on the interface. If no interface is specified, the standard and extended IP access lists on all interfaces are displayed.

Configuration Examples

```
QTECH# 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	Defines an IP access list.

Platform Description

N/A

show ipv6 traffic-filter

Use this command to display the IPv6 access list on the interface.

show ipv6 traffic-filter [interface *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults -

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the IPv6 access list configured on the interface. If no interface is specified, the IPv6 access lists on all interfaces are displayed.

Configuration Examples

```
QTECH# 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	Defines an IPv6 access list.

Platform Description

N/A

show mac access-group

Use this command to display the MAC access list on the interface.

show mac access-group [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the MAC access list configured on the interface. If no interface is specified, the MAC access lists on all interfaces are displayed.

Configuration Examples

```
QTECH# show mac access-group interface gigabitethernet 0/3 mac access-
group mm in
Applied On interface GigabitEthernet 0/3.
```

Related Commands

Command	Description
mac access-list	Defines a MAC access list.

Platform Description

N/A

show redirect interface

Use this command to display the access redirection configuration.

show redirect [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface *interface-name*	Interface name

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the access redirection configuration on the interface. If no interface is specified, the access redirection configuration on all interfaces is displayed.

Configuration Examples

```
QTECH #show redirect interface gigabitEthernet 0/3
acl redirect configuration on interface gigabitEthernet 0/3 redirect
destination interface gigabitEthernet 0/3 acl 1 in
```

The following example displays the access redirection configuration on interface GigabitEthernet 0/3.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

svi router-acls enable

Use this command to enable the SVI filter only for the Layer3 packets. Use the **no** form of this command to disable this function.

svi router-acls enable

no svi router-acls enable

Parameter Description

Parameter	Description
N/A	N/A.

Defaults

The SVI filter takes effect for both Layer2 and Layer3 packets by default.

Command mode

Global configuration mode

Usage Guide

Use this command to make the SVI filter take effect only for the Layer3 packets,

Configuration Examples

Related Commands

Platform Description

The following example enables the SVI filter only for the Layer3 packets.

```
QTECH(config)#svi router-acls enable
```

Command	Description
N/A	N/A

N/A

2. QOS COMMANDS

class

Use this command to add reference to an existing class map. Use the no form of this command to remove the class from the policy map.

class *class-map-name*

no class *class-map-name*

Parameter Description

Parameter	Description
class-map-name	Reference to a class map.

Defaults

The function is disabled by default.

Command Mode

Policy configuration mode

Usage Guide

N/A

Configuration Examples

The following example adds reference to the class map named cmap1.

```
QTECH(config)# class-map cmap1 QTECH(config-cmap)#

match ip dscp 5 QTECH(config-cmap)# exit



QTECH(config)#  policy-map  pmap1  QTECH(config-

pmap)# class cmap1 QTECH(config-pmap-c)# end
```

Related Commands

Command	Description
show policy-map [*policy-map-name* **[class** *class-map-name*]]	Displays the policy map.

Platform Description

N/A

class map

Use this command to create a class map and enter class-map configuration mode. Use the **no** or

default form of this command to remove a class map.

class-map *class-map-name*

no class-map class-map-name

default class-map class-map-name

Parameter Description

Parameter	Description
class-map-name	Class map name. The class map name can be a maximum of 31 characters.

Defaults

None

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# mac access-list extended me QTECH(config-ext-macl)#

permit host 1111.2222.3333 any QTECH(config-ext-macl)# exit


QTECH(config)# class-map cm_acl QTECH(config-cmap)#

match access-group me QTECH(config-cmap)# exit
```

The following example creates a class map named cm_acl to match an access list named me.

The following example creates a class map named cm_dscp to match DHCP 8, 16 and 24.

```
QTECH(config)# class-map cm_dscp QTECH(config-cmap)#

match ip dscp 8 16 24

QTECH(config-cmap)# exit
```

Related Commands

Command	Description

show class-map [*class-map-name*]	Displays the class map.

Platform Description

N/A

drr-queue bandwidth

Use this command to set the DRR queue weight ratio. Use the **no** or **default** form of this command to restore the default setting.

drr-queue bandwidth *weight1...weight8*

no drr-queue bandwidth default drr-queue bandwidth

Parameter Description

Parameter	Description
weight1...weight8	8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. For the products supporting the SP scheduling policy, the weight range is from 0 to 15. For the products not supporting the SP scheduling policy, the weight range is from 1 to 15.

Defaults

The default queue weight ratio is 1:1:1:1:1:1:1:1.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example configures the DRR queue weight ratio to 1:1:1:2:2:4:6:8.

```
QTECH(config)# drr-queue bandwidth 1:1:1:2:2:4:6:8
```

Command	Description
show mls qos queuing	Displays information about the queue.

N/A

match

Use this command to define a match criteria in class map configuration mode. Use the **no** form of this command to remove the match criteria.

match { **access-group** *access_list* **|** **ip** { **dscp** *dscp-vlaue-list* **|** **precedence** *pre-vlaue-list* } }

no match { **access-group** *access_list* **|** **ip** { **dscp** *dscp-vlaue-list* **|** **precedence** *pre-vlaue-list* } }

Parameter Description

Parameter	Description
access-group *access_list*	Identifies a numbered or named access list as the match criteria.
ip dscp *dscp-vlaue-list*	Identifies DSCP values as the match criteria. Multiple DSCP can be configured. The range is from 0 to 63.

Defaults

None

Command Mode

Class map configuration mode

Usage Guide N/A

Configuration Examples

The following example creates a class map named cmap1 to match DSCP 20, 22, 24 and 30.

Related Commands

```
QTECH(config)# class-map cmap1
QTECH(config-cmap)# match ip dscp 20 22 24 30
```

Platform Description

Command	Description
show class-map [*class-map-name*]	Displays the class map.

N/A

mls qos cos

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

mls qos cos *default-cos*

no mls qos cos

Parameter Description

Parameter	Description
default-cos	CoS value of the interface. The range is from 0 to 7.

Defaults

The default CoS value is 0.

Command Mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# interface gigabitethernet 1/1

QTECH(config-if)# mls qos cos 7
```

The following example configures the default CoS value to 7.

Related Commands

Command	Description
show mls qos interface *interface-id*	Displays information of the specified interface.

Platform Description

N/A

mls qos map cos-dscp

Use this command to map the CoS value to the DSCP value. Use the no or default form of this command to restore the default CoS-DSCP mapping.

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

no mls qos map cos-dscp default mls qos map cos-dscp

Parameter Description

Parameter	Description
dscp1...dscp8	Specifies the DSCP value. The range is from 0 to 63.

Defaults

By default, the CoS 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

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

Command	Description
show mls qos maps **cos-dscp**	Displays the CoS-DSCP mapping.

N/A

mls qos map dscp-cos

Use this command to map the DSCP value to the CoS value. Use the **no** or **default** form of this command to restore the default DSCP-CoS mapping.

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

no mls qos map dscp-cos default mls qos map dscp-cos

Parameter Description

Parameter	Description
dscp-list	DSCP list. The range is from 0 to 63.
cos	CoS value. The range is from 0 to 7.

Defaults

The default DSCP-CoS mapping is listed below:

DSCP 0-7	DSCP 8-15	DSCP 16-23	DSCP 24-31	DSCP 32-39	DSCP 40-47	DSCP 48-55	DSCP 56-63
CoS 0	CoS 1	CoS 2	CoS 3	CoS 4	CoS 5	CoS 6	CoS 7

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

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

Command	Description
show mls qos maps dscp-cos	Displays the DSCP-CoS mapping.

N/A

mls qos map ip-precedence-dscp

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

mls qos map ip-precedence-dscp *dscp1* ... *dscp8*

no mls qos map ip-precedence-dscp default mls qos map ip-precedence-dscp

Parameter Description

Parameter	Description
dscp1...dscp8	DSCP list. The range is from 0 to 63.

Defaults

By default, the IP precedence 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

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

Related Commands

Command	Description
show mls qos maps **ip-pre-dscp**	Displays the IP-precedence to DSCP mapping.

Platform Description

N/A

mls qos scheduler

Use this command to configure the output queue scheduling. Use the **no** or **default** form of this command to restore the default scheduler.

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

no mls qos scheduler

Parameter Description

Parameter	Description
sp	Specifies the absolute priority scheduling.
rr	Specifies the round-robin scheduling.
wrr	Specifies the frame count weighted round-robin scheduling.
drr	Specifies the frame length weighted round-robin scheduling.

Defaults

The default queue scheduling is wrr globally, no queue scheduling is configured on the interface.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example specifies the sp scheduling.

```
QTECH(config)# mls qos scheduler sp
```

Command	Description
show mls qos scheduler	Displays the output queue scheduling.

N/A

mls qos trust

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

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

no mls qos trust default mls qos trust

Parameter Description

Parameter	Description
cos	Specifies the CoS trust mode.
dscp	Specifies the DSCP trust mode.
ip-precedence	Specifies the IP-PRE trust mode.

Defaults

No trust mode is configured by default.

Command Mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# interface gigabitethernet 1/1

QTECH(config-if)# mls qos trust cos
```

The following example configures the CoS trust mode.

Related Commands

Command	Description
show mls qos interface *interface-id*	Displays the specified interface configuration.

Platform Description

N/A

police

Use this command to configure traffic policing for a class map in a policy map. Use the **no** form of this command to remove traffic policing for the class map.

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

no police

Parameter Description

Parameter	Description
rate-bps	Bandwidth limit value per second (The unit is KBits). This value depends on the specific product.
burst-byte	Burst traffic limit value (The unit is KBytes). This value depends on the specific product.
drop	Drops the packet. This is available only when the packet exceeds the bandwidth limit.
dscp *new-dscp*	Modifies the DSCP value of the packet. This is available only when the packet exceeds bandwidth limit. The DSCP value range is from 0 to 63.
cos *new-cos*	Modifies the CoS value of the packet. This is available only when the packet exceeds bandwidth limit. The CoS value range is from 0 to 7.
none-tos	Modifies the CoS value only.

Defaults

No traffic policing is configured for the class map by default.

Command Mode

Policy map class configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures traffic policing which modifies the DSCP value of the packet to 16 for class map “cm-acl” in policy map “pmap1”.

```
QTECH(config)# policy-map pmap1 QTECH(config-

pmap)# class cm-acl



QTECH(config-pmap-c)# police 102400 4096 exceed-action dscp 16
```

Related Commands

Command	Description
show policy-map [*policy-map-name* [**class** *class-map-name*]]	Displays the policy map configuration.

Platform Description

N/A

policy map

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

no or **default** form of this command to remove the specified policy map.

policy-map *policy-map-name*

no policy-map *policy-map-name*

default policy-map *policy-map-name*

Parameter Description

Parameter	Description
policy-map-name	Policy map name. The policy map name can be a maximum of 31 characters.

Defaults

No policy map is configured by default.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example creates policy map “po”, and then adds a reference to class map “cmap1”. Sets the rate limit value to 10 Mbps, the burst traffic limit value to 256 Kbps, and discard packets which exceed the limit.

```
QTECH(config)# policy-map po QTECH(config-
pmap)# class cmapl

QTECH(config-pmap-c)# police 10240 256 exceed-action drop
```

Related Commands

Command	Description
show policy-map [*policy-map-name* [**class** *class-map-name*]]	Displays the policy map configuration.

Platform Description

N/A

priority-queue

Use this command to configure the output queue scheduling policy to SP. Use the **no** or **default** form of this command to restore the default queue scheduling policy.

priority-queue

no priority-queue

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The default output queue scheduling policy is WRR.

Command Mode

Global configuration mode.

Usage Guide

This command shares the same configuration with the mls qos scheduler sp. The show run command displays this configuration in the mls qos scheduler sp item instead of priority-queue.

Configuration Examples

The following example configures the output queue scheduling policy to SP.

```
QTECH(config)# priority-queue
```

Related Commands

Command	Description

show mls qos scheduler	Displays the output queue scheduling policy.

Platform Description

N/A

priority-queue cos-map

Use this command to configure the mapping between the CoS value and the queue ID. Use the **no** or

default form of this command to restore the default CoS mapping to the queue.

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

no priority-queue cos-map default priority-queue cos-map

Parameter Description

Parameter	Description
qid	Queue ID. The range is from 1 to 8.
cos0 ... cos7	CoS value. The range is from 0 to 7.

Defaults

The default mapping between the CoS value and the queue ID is listed below:

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

Command Mode

Global configuration mode.

Usage Guide **N/A**

Configuration Examples

The following example maps the CoS 3, 5 to the output queue 1.

```
QTECH(config)#priority-queue cos-map 1 3 5
```

Related Commands

Command	Description
show mls qos queuing	Displays the output queues.

Platform Description

N/A

qos mc-queue cos-maparameter Description

This command is used to configure the mapping between CoS values of multicast queues.

qos mc-queue cos-map *cos0-qid cos1-qid cos2-qid cos3-qid cos4-qid cos5-qid cos6-qid cos7-qid*

no qos mc-queue cos-map

Parameter	Description
cosN-qid	Queue ID mapped by the packet whose CoS is N. The value of N ranges from 0 to 7, and queue ID ranges from 1 to 3.

Defaults

The default value is different from products.

Command

Global configuration mode

Mode

Usage Guide

In the case of default configuration, the relevant trust mode must be enabled. For example, packets can enter the default mapped queue only when CoS is trusted.

Configuration Examples

The following example sets the CoS 0, 1, 2, 3, 4, 5, 6, 7 to be mapped to the multicast queues 1 1 1 2 2 2 2 3 respectively.

```
QTECH(config)# qos mc-queue cos-map 1 1 1 2 2 2 2 3
```

Related Commands

Command	Description
show qos mc-queue cos-map	This command is used to view the queue mapping.

Platform Description

N/A

qos queue

Use this command to configure a minimum or maximum of the interface bandwidth to a queue. Use the **no** or **default** form of this command to remove the minimum or maximum of the interface bandwidth.

qos queue *queue-id* **bandwidth** { **minimum** | **maximum** } *bandwidth* **no qos queue** *queue-id* **bandwidth** { **minimum** | **maximum** } **default qos queue** *queue-id* **bandwidth** { **minimum** | **maximum** }

Parameter Description

Parameter	Description
queue	Configure the minimum or maximum of the interface bandwidth to the queue on the device supporting both unicast and multicast queue bandwidth configuration.
queue-id	Queue ID. The range is from 1 to 8.
bandwidth { **minimum** | **maximum** } *bandwidth*	Bandwidth value. The value range depends on the specific product.

Defaults

No minimum or maximum of interface bandwidth to a queue is configured by default.

Command Mode

Interface configuration mode

Usage Guide

Support global configuration mode and interface configuration mode. Function that these two modes support is different.

Configuration Examples

The following example configures the minimum interface bandwidth of queue 1 to 5 Mbps and the maximum to 10 Mbps; the minimum interface bandwidth of queue 2 to 1 Mbps and the maximum to 5

Mbps;

```
 QTECH(config)# interface gigabitEthernet 0/1
QTECH(config-if-GigabitEthernet 0/1)# qos queue 1 bandwidth maximum 10240
QTECH(config-if-GigabitEthernet 0/1)# qos queue 1 bandwidth minimum 5120
QTECH(config-if-GigabitEthernet 0/1)# qos queue 2 bandwidth minimum 2048
```

Related Commands

Command	Description
show qos bandwidth [**interfaces** *interface-id*]	Displays the interface bandwidth of the queue.

Platform Description

N/A

queueing wred

Use this command to enable the WRED (Weighted Random Early Detection) function. Use the **no** or **default** form of this command to disable the WRED function.

queueing wred

no queueing wred default queueing wred

Parameter Description

Parameter	Description
N/A	N/A

Defaults

WRED is disabled by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables WRED.

```
QTECH(config)# queueing wred
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

rate-limit

Use this command to configure rate limiting on the interface. Use the **no** or **default** form of this command to remove rate limiting from the interface.

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

no rate-limit **{** input | output **}**

default rate-limit { **input | output** }

Parameter Description

Parameter	Description
input	Configures input rate limiting.
output	Configures output rate limiting.
bps	Bandwidth limit value per second (The unit is KBits). This value depends on the specific product.
burst-size	Burst traffic limit value (The unit is KBytes). This value depends on the specific product.

Defaults

Rate limiting is not configured by default.

Command Mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

The following example configures the rate limit value to 10 Mbps, and the burst traffic limit value to 256 Kbps.

```
QTECH(config)# interface gigabitethernet 1/3

QTECH(config-if-GigabitEthernet 1/3)# rate-limit input 10240 256
```

Related Commands

Command	Description
show mls qos rate-limit [**interface** *interface-id*]	Displays the rate limiting configuration of the interface.

Platform Description

N/A

service-policy

Use this command to apply the policy map to the interface, the virtual group or globally. Use the **no** or

default form of this command to remove the policy map.

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

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

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

Parameter Description

Parameter	Description
policy-map-name	Policy map name
input	Applies the policy map to the input direction.
output	Applies the policy map to the output direction.

Defaults

No policy map is configured on the interface or virtual group by default.

Command Mode

Interface configuration mode, and virtual group configuration mode.

Usage Guide

N/A

Configuration Examples

The following example applies policy map “po” to the input direction of interface GigabitEthernet 1/3.

```
QTECH(config)# interface gigabitethernet 1/3

QTECH(config-if-GigabitEthernet 1/3)# service-policy input po
```

The following example applies policy map “po” to the output direction of virtual group 3.

```
QTECH(config)# virtual-group 3

QTECH(config-VirtualGroup)# service-policy output po
QTECH(config)# virtual-group 3

QTECH(config-VirtualGroup)# service-policy output po
```

Related Commands

Command	Description
show mls qos interface policers	Displays the policy map configuration on the interface.
show mls qos virtual-group policers	Displays the policy map configuration on the virtual group.

Platform Description

N/A

set

Parameter Description

Parameter	Description
ip dscp *new-dscp*	Configures the DSCP value for the traffic. The range is from 0 to 63.
cos *new-cos*	Configures the CoS value for the traffic. The range is from 0 to 7.
none-tos	Configures the CoS value only.
vid *new-vid*	Configures the VID value for the traffic. The range is from 1 to 4094.

Use this command to configure the CoS, DSCP or VID value for the traffic. Use the **no** form of this command to remove the CoS, DSCP or VID value from the traffic.

set { **ip dscp** *new-dscp* **| cos** *new-cos* | [**none-tos**] **vid** *new-vid* }

no set { **ip dscp** | **cos** | **vid** }

Defaults

No CoS, DSCP or VID value is configured for the traffic in policy map class mode.

Command Mode

Policy map class configuration mode

Usage Guide

N/A

Configuration Examples

The following example creates policy map “pmap1”, and adds a reference to class map “cmap1”.

```
QTECH(config)# policy-map pmap1 QTECH(config-

pmap)# class cmap1
```

The following example modifies the CoS value of the traffic to 3.

```
QTECH(config-pmap-c)# set cos 3
```

Related Commands

Command	Description
show **policy-map**[*policy-map-name* [**class** *class-map-name*]]	Displays the policy map configuration on the interface.

Platform Description

N/A

show class-map

Use this command to display the class map.

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

Parameter Description

Parameter	Description
class-map-name	Class map name.

Defaults

None

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show class-map
```

The following example displays all class maps.

```
Class Map cmap1 Match ip dscp 20 40

Class Map cmap2

  Match access-group 110
```

Related Commands

Platform Description

The fields in the output of this command are described in the following table.

Field	Description
Class Map	Indicates the class map name.
Match	Indicates the matched rule.

Command	Description
N/A	N/A

N/A

show mls qos interface

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

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

Parameter Description

Parameter	Description
interface-id	Interface name
policers	Displays the traffic policing configured on the interface.

Defaults

None

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show mls qos interface gigabitethernet 1/3

Interface: GigabitEthernet 1/3

Ratelimit input: 10240 256

Ratelimit output: 51200 4096 Attached input policy-map: pmap1
```

The following example displays the QoS configuration of interface GigabitEthernt 1/3.

```
Default cos: 3
```

The fields in the output of this command are described in the following table.

Field	Description
Interface	Indicates the interface name.
Ratelimit input	Indicates the input rate limit value .
Ratelimit output	Indicates the output rate limit value .
Attached input policy-map	Indicates the input policy map .
Attached output policy-map	Indicates the output policy map.
Default trust	Indicates the trust mode of the interface.
Default cos	Indicates the default CoS value.

The following example displays the QoS configuration of all interfaces.

```
QTECH#  show  mls  qos  interface  policers  Interface:

GigabitEthernet 0/1

Attached   input   policy-map:   pmap1   Attached

output     policy-map:     pmap1     Interface:

GigabitEthernet 0/2
```

```
Attached input  policy-map: p1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show mls qos maps

Use this command to display DSCP-CoS mapping, CoS-DSCP mapping and IP-PRE-DSCP mapping.

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

Parameter Description

Command	Description
N/A	N/A

Defaults

None

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

The following example displays the CoS-DSCP mapping.

```
QTECH# show mls qos maps cos-dscp

cos dscp

-----

0   0

1   8

2   16

3   24

4   32
```

```
5   40

6   48

7   56
```

The fields in the output of this command are described in the following table.

Field	Description
cos	Indicates the CoS value.
dscp	Indicates the DSCP value mapped .

The following example displays the DSCP- CoS mapping.

```
QTECH# show mls qos maps dscp-cos

dscp cos    dscp cos    dscp cos    dscp cos

--------

 0   0   1      0       2   0      3   0

 4   0      5   0       6   0      7   0

 8   1      9   1      10   1     11   1

12   1     13   1      14   1     15   1

16   2     17   2      18   2     19   2

20   2     21   2      22   2     23   2

24   3     25   3      26   3     27   3

28   3     29   3      30   3     31   3

32   4     33   4      34   4     35   4

36   4     37   4      38   4     39   4

40   5     41   5      42   5     43   5
```

```
44   5     45   5      46   5     47   5

48   6     49   6      50   6     51   6

52   6     53   6      54   6     55   6

56   7     57   7      58   7     59   7

60   7     61   7      62   7     63   7
```

The fields in the output of this command are described in the following table.

Field	Description

dscp	Indicates the DSCP value.
cos	Indicates the CoS value mapped .

The following example displays the IP-PRE-DSCP mapping.

```
QTECH# show mls qos maps ip-prec-dscp
0 0
1 8
2 16
3 24
4 32
5 40
6 48
7 56
```

Related Commands

Platform Description

The fields in the output of this command are described in the following table.

Field	Description
ip-precedence	Indicates the IP-PRE value.
dscp	Indicates the DSCP value mapped .

Command	Description
N/A	N/A

N/A

show mls qos queueing

Use this command to display the QoS queuing configuration.

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

Parameter Description

Parameter	Description
interface *interface-id*	ID of interface.

Defaults

N/A

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show mls qos queueing Cos-queue map:

cos qid

--- --- 0     1

1   2

2   3

3   4

4   5

5   6

6   7

7   8
wrr bandwidth weights:
qid weights
```

The following example displays the QoS queuing configuration.

```


drr bandwidth weights: weights

qid

------ -----------

1   3

2   3

3   3

4   3

5   3

6   3

7   3

8   3


wfq bandwidth weights:

qid weights

------
```

```
1   3

2   4

3   5

4   6

5   7

6   8

7   9

8   10


Interface: GigabitEthernet 0/1
 Wrr queue bandwidth: 1 1 1 1 2 2 2 2
 Drr queue bandwidth: 1 1 2 2 2 2 4 4
 Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

The fields in the output of this command are described in the following table.

Field	Description
Cos-queue map	Indicates the mapping between the CoS value and the queue ID.
wrr bandwidth weights	Indicates the WRR queue weight.
drr bandwidth weights	Indicates the DRR queue weight.
wfq bandwidth weights	Indicates the WFQ queue weight.
cos	Indicates the CoS value.
qid	Indicates the queue ID.
Weights	Indicates the weight value
Interface	Interface name
wrr bandwidth weights	Indicates the WRR queue weight.
drr bandwidth weights	Indicates the DRR queue weight.
wfq bandwidth weights	Indicates the WFQ queue weight.

```
QTECH# show mls qos queueing interface gigabitEthernet 0/1

Interface: GigabitEthernet 0/1
```

```
Wrr queue bandwidth: 1 1 1 1 2 2 2 2

Drr queue bandwidth: 1 1 2 2 2 2 4 4

Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

Interface	Interface name
wrr bandwidth weights	Indicates the WRR queue weight.
drr bandwidth weights	Indicates the DRR queue weight.
wfq bandwidth weights	Indicates the WFQ queue weight.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show mls qos rate-limit

Use this command to display the rate limiting configuration of the interface.

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

Parameter Description

Parameter	Description
interface-id	Interface name

Defaults

N/A

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show mls qos rate-limit Interface:
```

```
GigabitEthernet 0/1

  rate limit input Kbps = 10240 burst = 256
```

The following example displays the rate limiting configuration of all interfaces.

```
Interface: GigabitEthernet 0/3

  rate limit output Kbps = 102400 burst = 4096
```

Related Commands

Platform Description

The fields in the output of this command are described in the following table.

Field	Description
Interface	Indicates the interface name.
rate limit input Kbps = x burst = y	Indicates the input rate limit value, and the input burst traffic limit value.
rate limit output Kbps = x burst = y	Indicates the output rate limit value, and the output burst traffic limit value.

Command	Description
N/A	N/A

N/A

show mls qos scheduler

Use this command to display the queue scheduling policy.

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

Parameter Description

Parameter	Description
interface *interface-id*	Interface name

Defaults

None

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

The following example displays the queue scheduling policy.

```
QTECH# show mls qos scheduler

Global Multi-Layer Switching scheduling Weighted Round

 Robin

Interface GigabitEthernet 0/1 Multi-Layer Switching scheduling:

 Deficit Round Robin
```

The fields in the output of this command are described in the following table.

Field	Description
Weighted Round Robin	Indicates that the queue scheduling policy is
	WRR. The other queue scheduling policies are listed as follows: SP: Strict Priority RR: Round Robin DRR: Deficit Round Robin WFQ: Weighted Fair Queue
Interface	Interface name
Deficit Round Robin	The queue scheduling is DRR

Related Commands

Command	Description
N/A	N/A

latform Description

N/A

show mls qos virtual-group

Use this command to display the policy map configuration on the virtual group.

show mls qos virtual-group [*virtual-group-number* | **policers**]

Parameter Description

Parameter	Description
virtual-group-number	Virtual group number. The range is from 1 to 128.
policers	Displays the policy map configuration on all virtual groups.

Defaults

None

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show mls qos virtual-group policers Virtual-

group: 1

Attached input policy-map: pmap1 Virtual-

group: 20

Attached output policy-map: pmap2
```

The following example displays the policy map configuration on all virtual groups.

The fields in the output of this command are described in the following table.

Field	Description
Virtual-group	Indicates the virtual group number.
Attached input policy-map	Indicates the policy map applied on the input virtual group.
Attached output policy-map	Indicates the policy map applied on the output virtual group.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show policy-map

Use this command to display policy maps.

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

Parameter Description

Parameter	Description
policy-map-name	Policy map name
class-map-name	Class map name

Defaults

None

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
 QTECH# show policy-map pmap1

  Policy Map pmap1 Class cmap1

      set ip dscp 16 Class cmap2

      police 10240 256 exceed-action dscp 8 Class cmap3

police 512000 4096 exceed-action drop
```

The following example displays configuration of policy map “pmap1”.

The fields in the output of this command are described in the following table.

Field	Description

Policy Map	Indicates the policy map name.
Class	Indicates the class map name.
set	Indicates that the DSCP value is modified in this example.
police	Indicates bandwidth limit configuration and the action policy for the violated packets.

The following example displays the action policy for the traffic of class map “cmap1” in policy map “pmap1” .

```
QTECH#show policy-map pmap1 class cmap1 Class cmap1

set ip dscp 16
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show qos bandwidth

Use this command to display the bandwidth configuration.

show qos bandwidth [**interfaces** *interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface name

Defaults

None

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

The following example displays the bandwidth configuration of interface GigabitEthernet 0/1. (Taking the device supporting the bandwidth configuration of the unicast queue or the multicast queue for example.)

```
QTECH# show qos bandwidth interface gigabitEthernet 0/1
```

```
1          5120          10240

2             0              0

3             0              0

4             0              0

5             0              0

6             0              0

7             0              0

8             0              0
```

The fields in the output of this command are described in the following table.

```
Interface: GigabitEnternet 0/1
........................................................................
Uc-queue-id I  minimum-bandwidth I maximum-bandwidth
```

Related Commands

Field	Description
Interface	Indicates the interface name.
queue-id	Indicates the queue ID.
uc-queue-id	Indicates the unicast queue ID.
mc-queue-id	Indicates the multicast queue ID.
minimum-bandwidth	Indicates the minimum bandwidth configuration.

	The unit is Kbps.
maximum-bandwidth	Indicates the maximum bandwidth configuration. The unit is Kbps.
Total queue minimum-bandwidth Total queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when both unicast and multicast queues are displayed.
Total ucast-queue minimum-bandwidth Total ucast-queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when only unicast queue is displayed.
Total mcast-queue minimum-bandwidth Total mcast-queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when only multicast queue is displayed.

Command	Description
N/A	N/A

Platform Description

N/A

show qos mc-queue cos-map

This command is used to display the mapping between multicast queues and priorities.

show qos mc-queue cos-map

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide

-

Configuration Examples

```
QTECH# show qos mc-queue cos-map Cos to multicast
queue map:
Cos Queue id
0    1
1    1
```

The following example displays the mapping between multicast queues and priorities

```
2         1
3         1
4         2
5         2
6         2
7         3
```

Related Commands

Command	Description
Cos	Cos value
Queue id	Queue ID of Cos

Platform Description

N/A

show qos mc-queue scheduler

This command is used to display the scheduling algorithm for multicast queues.

show qos mc-queue scheduler [**interfaces** *interface-id*]

Parameter Description

Parameter	Description
interfaces *interface-id*	Interface to be displayed.

Defaults

-

Command Mode

Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide

-

Configuration Examples

```
QTECH# show qos mc-queue scheduler Multicast

queue scheduler: Interface GigabitEthernet 0/0 :

Strict Priority


Interface GigabitEthernet 0/1 : Strict

 Priority


Interface GigabitEthernet 0/2 :
```

The following example displays the scheduling algorithm for multicast queues.

```
Weighted Round Robin
Queue id    Weight
1           1
2           2
3           3
```

Related Commands

Command	Description
qos mc-queue scheduler mode {sp | wrr}	This command is used to configure the scheduling algorithm for multicast queues.
qos mc-queue scheduler weight *weight1* *weight2 weight3*	This command is used to configure the WRR algorithm weight for multicast queues.

Platform Description

N/A

show queueing wred interface

Use this command to display WRED settings on the interface.

show queueing wred interface *interface-id*

Parameter Description

Parameter	Description
interface-id	Interface name

Defaults

None

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

The following example displays the WRED settings on interface GigabitEthernet 0/1.

```
QTECH#show queueing wred interface gigabitEthernet 0/1

qid min_1 prob_1 min_2 prob_2

1    100   60       80    80
2    100   60       80    80
3    100   60       80    80
4    100   60       80    80
5    100   60       80    80
```

```
6    100   60       80    80
7    100   60       80    80
8    100   60       80    80



cos qid  threshold_id

0    1    1
1    2    1
2    3    1
3    4    1
4    5    1
5    6    1
6    7    1
7    8    1
```

Related Commands

Platform Description

The fields in the output of this command are described in the following table.

Field	Description
qid	Indicates the queue ID.
cos qid threshold_id	Indicates the mapping of CoS value, queue ID and threshold number.

Command	Description
N/A.	N/A.

N/A.

show virtual-group

Use this command to display the member port in the virtual group.

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

Parameter Description

Parameter	Description
virtual-group-number	Virtual group number. The range is from 1 to 128.
summary	Displays the member port in all virtual groups.

Defaults

N/A

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show virtual-group summary
virtual-group   member
.................   ................
1               Gi0/1 Gi0/2
2               Gi0/0
```

The following example displays the member port in all virtual groups.

Related Commands

Platform Description

The fields in the output of this command are described in the following table.

Field	Description
virtual-group	Indicates the virtual group number.
member	Indicates the member port in the virtual group.

Command	Description
N/A	N/A

N/A

virtual-group

Use this command to create a virtual group in global configuration mode.

Use this command to configure add an interface to a virtual group in interface configuration mode. Use the **no** or **default** form of this command to remove a virtual group in global configuration mode. Use the **no** or **default** form of this command to remove an interface from a virtual group in interface configuration mode.

virtual-group *virtual-group-number*

no virtual-group *virtual-group-number*

default virtual-group *virtual-group-number*

Parameter Description

Parameter	**Description**
virtual-group-number	Virtual group number. The range is from 1 to 128.

Defaults

No virtual group is configured, or no interface is added to a virtual group, by default.

Command Mode

Interface configuration mode, global configuration mode.

Usage Guide

The member port added to the virtual group must be a physical port or an aggregate port member.

The member ports of a virtual group must be on the same module of a chassis switch or on the same box switch.

Configuration Examples

```
QTECH(config)# interface gigabitethernet 1/3

QTECH(config-if)# virtual-group 3
```

The following example sets the interface gigabitEthernet 1/3 as the member of virtual group 3:

Related Commands

Command	Description
show virtual-group [*virtual-group-number* | **summary**]	Displays the virtual group configuration.

Platform Description

N/A

wrr-queue bandwidth

Use this command to set the WRR weight ratio. Use the no or default form of this command to restore the default setting.

wrr-queue bandwidth *weight1 ... weight8*

no wrr-queue bandwidth default wrr-queue bandwidth

Parameter Description

Parameter	Description

weight1...weight8	8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. For the products supporting the SP scheduling policy, the weight range is from 0 to 15. For the products not supporting the SP scheduling policy, the weight range is from 1 to 15.

Defaults

The default queue weight ratio is 1:1:1:1:1:1:1:1.

Command Mode

Global/Interface configuration mode

Usage Guide

If the weight value is 0, the SP scheduling policy is applied.

Configuration Examples

The following example configures the WRR queue weight ratio to 1:1:1:1:2:2:4:8.

```
QTECH(config)# wrr-queue bandwidth 1 1 1 1 2 2 4 8
```

Related Commands

Command	Description
show mls qos queuing	Displays the QoS queuing configuration.

Platform Description

N/A

wrr-queue cos-map

Use this command to map the CoS value to a threshold for a specified queue. Use the **no** or **default**

form of this command to restore the default settings

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

no wrr-queue cos-map *threshold_id*

default wrr-queue cos-map *threshold_id*

Parameter Description

Parameter	Description
threshold_id	Threshold number. The range is from 1 to 2. Up to two threshold values can be configured.
cos_N	CoS value. The range is from 0 to 7. Up to 8 CoS values can be configured.

Defaults

All CoS values are mapped to the threshold 1.

Command mode

Interface configuration mode.

Usage Guide

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.

Configuration Examples

```
QTECH(config)# interface gigabitethernet 1/3

QTECH(config-if-GigabitEthernet 1/3)#wrr-queue cos-map 2 1 6
```

The following example enters the interface GigabitEthernet 1/3 to map CoS 1, 2 to threshold 2.

Related Commands

Command	Description
show queueing wred interface *interface-id*	Displays the WRED configuration on the interface.

Platform Description

N/A.

wrr-queue random-detect min-threshold

Use this command to configure the minimum WRED drop threshold. Use the **no** or **default** form of this command to restore the default WRED drop threshold.

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

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

default wrr-queue random-detect min-threshold *queue_id*

Parameter Description

Parameter	Description
queue_id	Queue ID.
thrN	Up to two threshold values can be configured. The threshold value range is from 1 to 100.

Defaults

Two threshold values are configured, and the default threshold values are 100 and 80.

Command mode

Interface configuration mode.

Usage Guide

Because the maximum value of the configuration range is equal to the current higher threshold, you need to pay attention to the setting of the higher threshold when configuring the lower threshold.

onfiguration Examples

```
QTECH(config)# interface gigabitethernet 1/3

QTECH(config-if-GigabitEthernet 1/3)# wrr-queue random-detect min-threshold 1 60 70
```

The following example configures the low WRED drop thresholds to 60 and 70 for queue 1.

Related Commands

Command	Description
show queueing wred interface *interface-id*	Displays the WRED configuration on the interface.

Platform Description

N/A.

wrr-queue random-detect probability

Use this command to configure the WRED packet drop probability. Use the **no** or **default** form of this command to restore the WRED packet drop probability.

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

no wrr-queue random-detect probability ***queue_id***

default wrr-queue random-detect probability *queue_id*

Parameter Description

Parameter	Description
queue_id	Queue ID.
proN	Up to two probability values can be configured. The threshold value range is from 1 to 100.

Defaults

Two packet drop probability values are configured, and the default probability values are 100 and 80.

Command mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# interface gigabitethernet 1/3

QTECH(config-if-GigabitEthernet 1/3)# wrr-queue random-detect probability 1 50 70
```

The following example configures the WRED packet drop values to 50 and 70 for queue 1.

Related Commands

Command	Description

show queueing wred interface *interface-id*	Displays the WRED configuration on the interface.

Platform Description

N/A.

3. MMU COMMANDS

3.1. *mmu buffer-mode*

Use this command to configure global buffer mode.

mmu buffer-mode **{** normal | burst-enhance |qos-enhance | flowctrl-enhance **}**

Use the **no** form of this command to restore the default setting.

no mmu buffer-mode

Parameter Description

Parameter	Description
normal	Normal buffer mode
burst-enhance	Burst enhancement
qos-enhance	QoS enhancement
flowctrl-enhance	Flow control enhancement

Defaults

The default buffer mode varies from product.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example configures the normal buffer mode.

```
QTECH# mmu buffer-mode normal
```

Platform Description

N/A

3.2 clear queue-buffer peaked

Use this command to clear the historical peak value of the queue buffer.

clear queue-buffer peaked

Parameter

Parameter	Description
N/A	

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Examples

```
QTECH# clear queue-buffer peaked
QTECH#
```

The following example clears the historical peak value of the buffer.

Platform Description

N/A

3.3. clear queue-counters

Use this command to clear queue statistics.

clear queue-counter [interface *interface _id*]

Parameter Description

Parameter	Description
interface_id	Port Number

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Examples

```
QTECH# clear queue-counter
QTECH#
```

The following example clears all queue statistics.

The following example clears queue statistics of an interface.

```
QTECH# clear queue-counter Interface TenGigabitEthernet 1/9
QTECH#
```

Platform

N/A

3.4. mmu usage-warn-limit

Use this command to configure the usage warning threshold.

mmu usage-warn-limit [{ unicast } {*queue-id1* [*queue-id2* [*queue-idN*]}**] set** *value*

Use the **no** form of this command to restore the default setting.

no mmu usage-warn-limit

Parameter Description

Parameter	Description
unicast	Performs buffer management on the output unicast queue.
queue-idN	Queue ID
priority-idN	Priority group ID
value	Usage warning threshold.

Defaults

The default threshold is 0.

Command Mode

Global configuration mode/Interface configuration mode

Default Level

14

Usage Guide

If the buffer usage for the port group exceeds the global threshold, a warning log is printed. If the buffer usage for the queue exceeds the queue threshold, a warning log is printed. To avoid producing excessive logs, the warning log for a port group/queue is printed only once within 30 seconds.

Configuration Examples

```
QTECH#config
QTECH(config)# mmu usage-warn-limit set 90
```

The following example sets the usage warning threshold globally.

```
QTECH#config
QTECH(config)# int te1/1
QTECH(config-if)# mmu usage-warn-limit unicast 3 8 set 80
```

The following example sets the usage warning threshold for unicast queue 3 and 8 to 80%.

Platform Description

N/A

3.5. mmu queue-guarantee

Use this command to configure the guaranteed buffer.

mmu queue-guarantee output { unicast } {*queue-id1* [*queue-id2* [*queue-idN*] { **set** *value*

Parameter Description

Parameter	Description
output	Performs buffer management on the output queue.
unicast	Performs buffer management on the output unicast queue.
queue-idN	Queue ID
value	Sets the number of guaranteed buffer, in the unit of cells.

Use the **no** form of this command to restore the default setting.

no mmu queue-guarantee output { unicast }

Defaults

The default varies with different products.

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

This command is executed in different ways on different devices.

Configuration Examples

```
QTECH#config
QTECH(config)# interface tenGigabitEthernet 1/9
QTECH(config-if)#mmu queue-guarantee ouput unicast 1 3 7 8 set 15
QTECH(config-if)#exit
QTECH(config)#exit QTECH#
```

The following example configures guaranteed buffer for unicast queue.

Platform Description

N/A

3.6. mmu queue-thredshold

Use this command to configure the shared buffer.

mmu queue-thredshold output { unicast } { *queue-id1* [*queue-id2* [*queue-idN*]] } **set** *th%*

Use the **no** form of this command to restore the default setting.

no mmu queue-thredshold output { unicast }

Parameter Description

Parameter	Description
output	Performs buffer management on the output queue.
unicast	Performs buffer management on the output unicast queue.

queue-idN	Queue ID
th%	Total shared buffer * threshold = Available buffer

Defaults

The default varies with different products.

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

```
QTECH#config
QTECH(config)# interface tenGigabitEthernet 1/9
QTECH(config-if)#mmu queue-threshold ouput unicast 1 3 7 8 set 80
QTECH(config-if)#exit
```

The following example configures shared buffer for unicast queue.

Platform Description

N/A

3.7. mmu fc-threshold

Use this command to configure the inbound buffer threshold.

mmu fc-threshold set ***th%***

Use the **no** form of this command to restore the default setting.

no mmu fc-threshold

Parameter Description

Parameter	Description
th%	Indicates the percentage of inbound buffer threshold.

Defaults

The default varies with different products.

Command Mode

Interface configuration mode

Usage Guide

This command is executed in different ways on different devices. This command only takes effect when flow control/PFC is enabled.

Configuration

The following example configures inbound buffer threshold of priority group.

Examples

```
QTECH#config
QTECH(config)# interface tenGigabitEthernet 0/9
QTECH(config-if)#mmu fc-threshold set 80 QTECH(config-
if)#exit
```

Platform Description

N/A

3.8. show queue-buffer interface

Use this command to display buffer usage of interfaces.

show queue-buffer interface { *interface-id*}

Parameter Description

Parameter	Description
interface-id	Interface

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

```
Qtech(config)#show queue-buffer interface hundredGigabitEthernet 0/1
Interface HundredGigabitEthernet 0/1:
Slice 1:
Type   Queue Used cells Available cells Usage Usage warn limit Usage warn count Peaked
cells
Unicast      1        42288         0                 100%     0%                 0
42288
Unicast     2       0            42280             0%      0%               0                0
Unicast     3       0            42280             0%      0%               0                0
Unicast     4       0            42280             0%      0%               0                0
Unicast     5       0            42280             0%      0%               0                0
Unicast     6       0            42280             0%      0%               0                0
Unicast     7       0            42280             0%      0%               0                0
Unicast     8        0            42280             0%      0%               0               0
Multicast  1 0 668 0% 0%  0
3442
Multicast   2       0           668              0%      0%              0              0
Multicast  3 0 668  0%  0% 0  0
```

The following example displays buffer usage of the specified interface based on output queue.

```
Slot Slice PortGroup Total cells Total usage Usage warn limit Static used cells Global  shared cells Available shared cells
0 1 1 53248 79% 90% 8 47564
5284
0 2 1 53248 79% 90% 8 47564
5284
0 3 1 53248 0% 90% 0 47564
47564
0      4      1         53248       0%         90%             0
47564   47564
```

Field	Description
Slice	No. of the module on the chip for buffer division
Type	Queue type, including unicast queue and multicast queue
Queue	Queue No., ranging from 1 to 8 by default and can be switched to 0 to 7 through configuration

Used cells	Size of the occupied buffer in a queue, in the unit of cell
Available cells	Size of the available buffer in a queue, in the unit of cell
Usage	Percentage of the occupied buffer in a queue
Usage warn limit	Buffer usage warning threshold of a specific port group or queue
Usage warn count	Number of times that the occupied buffer exceeds the warning threshold
Peaked cells	Historical peak value of the used buffer
Slot	Slot No. of the line card
PortGroup	Port group No., starting from 1
Total cells	Total buffer on a specified slice
Total usage	Percentage of the occupied buffer on a specified slice
Static used cells	Size of the occupied guarantee buffer on a specified slice
Global sha red cells	Total shared buffer on a specified slice
Available shared cells	Size of the available shared buffer on a specified slice

The following example displays the buffer queue information of all interfaces.

```
QTECH#show queue-buffer

Interface HundredGigabitEthernet 0/1:

Slice 1:

Type    Queue Used cells Available cells Usage Usage warn limit Usage warn count Peaked

cells

Unicast       1         22383          1                  99%       50%                    686

42288

Unicast    2       0            22384              0%      0%                0              0
Unicast    3      0            22384             0%     0%                0                0

Unicast       4          22391           0                  100%       0%                  0

22416

Unicast    5      0            22384             0%     0%                0                0

Unicast    6      0            22384             0%     0%                0                0

Unicast    7      0            22384             0%     0%                0                0

Unicast    8      0            22384             0%     0%               0               0

Multicast  1  0  357  0%  0%  0

3442

Multicast  2      0            357               0%     0%               0               0

Multicast  3      0            357               0%     0%               0               0

Multicast  4      0            357               0%     0%               0               0

Multicast  5      0            357               0%     0%               0               0

Multicast  6      0            357               0%     0%               0               0

Multicast  7      0            357               0%     0%               0               0

Multicast  8  0  357  0%  0%  0  0


Slice  3:

Type  Queue  Used  cells  Available  cells  Usage  Usage  warn  limit  Usage  warn  count  Peaked

cells

Unicast  1  0  42287  0%  0%  0

42288

Unicast    2      0            42287             0%     0%                0                0

Unicast    3      0            42287             0%     0%                0                0

Unicast    4      0            42287             0%     0%                0                0

Unicast    5      0            42287             0%     0%                0                0

Unicast    6      0            42287             0%     0%                0                0

Unicast    7      0            42287             0%     0%                0                0

Unicast    8      0            42287             0%     0%                0                0
Multicast  1  0  5292  0%  0%  0
Multicast  2      0            5292              0%     0%                0                0

Multicast  3      0            5292              0%     0%                0                0

Multicast  4      0            5292              0%     0%                0                0

Multicast  5      0            5292              0%     0%                0                0

Multicast  6      0            5292              0%     0%                0                0

Multicast  7      0            5292              0%     0%                0                0

Multicast  8      0            5292              0%     0%                0                0


Slice  4:

Type  Queue  Used  cells  Available  cells  Usage  Usage  warn  limit  Usage  warn  count   Peaked

cells

Unicast    1      0            42287             0%     0%                0                0

Unicast    2      0            42287             0%     0%                0                0

Unicast    3      0            42287             0%     0%                0                0
Unicast    4    0        42287        0%    0%         0        0
Unicast    5    0        42287        0%    0%         0        0
Unicast    6    0        42287        0%    0%         0        0
Unicast    7    0        42287        0%    0%         0        0
Unicast    8    0        42287        0%    0%         0        0
Multicast  1    0        5292         0%    0%         0        0
Multicast  2    0        5292         0%    0%         0        0
Multicast  3    0        5292         0%    0%         0        0
Multicast  4    0        5292         0%    0%         0        0
Multicast  5    0        5292         0%    0%         0        0
Multicast  6    0        5292         0%    0%         0        0
Multicast  7    0        5292         0%    0%         0        0
Multicast  8    0        5292         0%    0%         0        0
Slot Slice PortGroup Total cells Total usage Usage warn limit Static used cells Global
shared cells Available shared cells
0 1 1 53248 84% 90% 16 47564
2797
0 2 1 53248 0% 90% 0 47564
47564
0 3 1 53248 0% 90% 0 47564
47564
3442
0 4 1                     53248         0%   90%         0
47564                     47564
```

Platform Description

N/A

3.9. show queue-counter interface

Use this command to display buffer queue statistics of interfaces.

show queue-counter interface *interface-id*

Parameter Description

Parameter	Description
interface-id	Interface

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Default Level

Usage Guide

N/A

Configuration Examples

The following example displays buffer queue statistics of the specified interface based on output queue.

QTECH#show queue-counter interface gigabitEthernet 0/9 Interface HundredGigabitEthernet 4/1:

```
Unicast
  Queue     Transmitted Bytes        Dropped Bytes    Frame Loss Rate(%)    Transmit  Rate(bps)
      1                     0                    0                     0                    0
      2                     0                    0                     0                    0
      3                     0                    0                     0                    0
      4                     0                    0                     0                    0
      5                     0                    0                     0                    0
      6                     0                    0                     0                    0
      7                     0                    0                     0                    0
      8                 62797                    0                     0                  656
  Multicast
  Queue     Transmitted Bytes        Dropped Bytes    Frame Loss Rate(%)    Transmit  Rate(bps)
      1                     0                    0                     0                    0
      2                     0                    0                     0                    0
      3                     0                    0                     0                    0
      4                     0                    0                     0                    0
      5                     0                    0                     0                    0
      6                     0                    0                     0                    0
      7                     0                    0                     0                    0
      8                     0                    0                     0                    0
  Unicast
  Queue   Transmitted Packets      Dropped Packets    Frame Loss Rate(%)    Transmit  Rate(pps)
      1                     0                    0                     0                    0
      2                     0                    0                     0                    0
      3                     0                    0                     0                    0
      4                     0                    0                     0                    0
      5                     0                    0                     0                    0
      6                     0                    0                     0                    0
      7                     0                    0                     0                    0
      8                   472                    0                     0                    0
  Multicast
  Queue   Transmitted Packets      Dropped Packets    Frame Loss Rate(%)    Transmit  Rate(pps)
```

```
      1                 0                 0                 0                0
      2                 0                 0                 0                0
      3                 0                 0                 0                0
      4                 0                 0                 0                0
      5                 0                 0                 0                0
      6                 0                 0                 0                0
      7                 0                 0                 0                0
      8                 0                 0                 0                0
```

The following example displays buffer queue statistics of all interfaces.

```
QTECH#show queue-counter
Interface HundredGigabitEthernet 0/1:
  Unicast
QTECH#show queue-counter
Interface HundredGigabitEthernet 0/1:
  Unicast
  Queue   Transmitted Bytes   Dropped Bytes    Frame Loss Rate(%)
Transmit Rate(bps)
      1            117380835776           1056130216960
89.99 50525032
      2                           0                            0
0 0
      3                           0                            0
0 0
      4              2736178496             24624019520
89.99 50525056
      5                           0                            0
0 0
      6                           0                            0
0 0
      7                           0                            0
0 0
      8                     1200887                           0
0 664
  Multicast
  Queue   Transmitted Bytes   Dropped Bytes    Frame Loss Rate(%)
Transmit Rate(bps)
      1                     24098176                  233925440
90.66 0
      2 0 0  0
QTECH#show queue-counter
Interface HundredGigabitEthernet 0/1:
  Unicast
  Queue   Transmitted Bytes   Dropped Bytes    Frame Loss Rate(%)
Transmit Rate(bps)
      1            117380835776           1056130216960
89.99 50525032
      2                           0                       0
0 0
      3                           0                       0
0 0
      4              2736178496             24624019520
89.99 50525056
      5                           0                       0

0
      3                           0                       0
0  0
      4                           0                       0
0 0
      5                           0                       0
0 0
      6                           0                       0
0 0
      7                           0                       0
0 0
      8                           0                       0
0 0
  Unicast
  Queue  Transmitted Packets  Dropped Packets   Frame Loss Rate(%)
Transmit Rate(pps)
      1                1834075559               16502034640
89.99 75183
      2                           0                       0
0 0
      3                           0                       0
0 0
      4                  42752789                 384750305
89.99 75183
      5                           0                       0
0 0
      6                           0                       0
0 0
      7                           0                       0
0 0
```

```
      8                         9306                          0
0 0
  Multicast
  Queue  Transmitted Packets  Dropped Packets   Frame Loss Rate(%)
Transmit Rate(pps)
      1                       376534                     3655085
90.66 0
      2                         0                           0
0 0
      3                         0                           0
0  0
      4                         0                           0
0 0
      5 0 0  0
                  0
      6                         0                           0
0  0
      7                         0                           0
0 0
      8                       0                         0
0 0Gi0/24 0 0 0  0.000
……
Interface HundredGigabitEthernet 0/64:
  Unicast
  Queue   Transmitted Bytes   Dropped Bytes    Frame Loss Rate(%)
Transmit Rate(bps)
      1                  83892643136                754894738496
89.99 0
      2                         0                           0
0 0
      3                         0                           0
0  0
      4                         0                           0
0 0
      5                         0                           0
0 0
      6                         0                           0
0 0
      7                         0                           0
0 0
      8                    1203321                        0
0 664
  Multicast
  Queue  Transmitted Bytes   Dropped Bytes    Frame Loss Rate(%)
Transmit Rate(bps)
      1                    126178880                   1208592000
90.54 0
      2                           0                           0
0   0
      3                           0                           0
0 0
      4                           0                           0
0 0
      5                           0                           0
0   0
      6                           0                           0
0 0
      7 0 0  0

0
      8                           0                           0
0 0
  Unicast
  Queue  Transmitted Packets  Dropped Packets   Frame Loss Rate(%)
Transmit Rate(pps)
      1                  1310822549                 11795230289
89.99  0
      2                           0                           0
0 0
      3                           0                           0
0 0
      4                           0                           0
0   0
      5                           0                           0
0 0
      6                           0                           0
0 0
      7                           0                           0
0 0
      8                        9317                            0
0 0
  Multicast
  Queue  Transmitted Packets  Dropped Packets   Frame Loss Rate(%)
Transmit Rate(pps)
      1                      1971545                   18884250
90.54 0
```

```
          2                                             0                                             0
0  0
          3                                             0                                             0
0  0
          4                                             0                                             0
0  0
          5                                             0                                             0
0    0
          6                                             0                                             0
0  0
          7                                             0                                             0
0  0
          8                                             0                                             0
0  0
```

Platform Description