DES-7200

CLI Reference Guide

Version 10.3(5)

D-Link®

DES-7200 CLI Reference Guide

Revision No.: Version 10.3(5)

Date: 2009/12/31

Preface

Version Description

This manual matches the firmware version 10.3(5).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

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

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

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

2. Command Line Format Convention

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

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

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

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

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

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

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

.

3. Signs

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

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

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

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

Contents

1 CLI Authorization Configuration Commands 1-1

1.1 alias 1-1

1.2 privilege 1-3

1.3 show aliases 1-5

2 Switch Management Configuration Commands 2-1

2.1 User Management Related Commands 2-1

2.1.1 disable 2-1

2.1.2 enable 2-2

2.1.3 enable password 2-2

2.1.4 enable secret 2-3

2.1.5 service password-encryption 2-4

2.1.6 password 2-5

2.1.7 login 2-6

2.1.8 login local 2-6

2.1.9 login authentication 2-7

2.1.10 username 2-8

2.1.11 lock 2-9

2.1.12 lockable 2-10

2.1.13 telnet 2-11

2.1.14 enable service 2-12

2.2 Basic System Management Related Commands 2-12

2.2.1 clock set 2-13

2.2.2 clock update-calendar 2-14

2.2.3 exec-timeout 2-14

2.2.4 hostname 2-15

2.2.5 session-timeout 2-16

2.2.6 show clock 2-16

2.2.7 show running-config 2-17

2.2.8 show startup-config 2-17

2.2.9 reload 2-18

2.2.10 show reload 2-18

2.2.11 prompt 2-19

2.2.12 banner motd 2-19

2.2.13 banner login 2-20

2.2.14 speed 2-20

2.2.15 show line 2-21

2.2.16 write 2-22

3 LINE Configuration Commands 3-1

3.1 Configuration Related Commands 3-1

3.1.1 line 3-1

3.1.2 line vty 3-2

3.1.3 transport input 3-2

3.1.4 access-class 3-4

4 Upgrade and Maintenance Configuration Commands 4-1

4.1 Configuration Related Commands 4-1

4.1.1 copy xmodem 4-1

4.1.2 copy tftp 4-2

5 Network Connectivity Test Tool Configuration Commands 5-1

5.1 Configuration Related Commands 5-1

5.1.1 ping 5-1

5.1.2 traceroute 5-2

5.1.3 line-detect 5-5

6 Interface Configuration Commands 6-1

6.1 Configuration Related Commands 6-1

6.1.1 interface aggregateport 6-1

6.1.2 interface fastEthernet 6-2

6.1.3 interface giagbitEthernet 6-3

6.1.4 interface tenGiagbitEthernet 6-3

6.1.5 interface vlan 6-4

6.1.6 medium-type 6-5

6.1.7 description 6-6

6.1.8 shutdown 6-6

6.1.9 speed 6-7

6.1.10 duplex 6-8

6.1.11 flowcontrol 6-9

6.1.12 mtu 6-10

6.1.13 carrier-delay 6-10

6.1.14 clear counters 6-11

6.1.15 clear interface 6-12

6.1.16 switchport 6-12

6.1.17 switchport mode 6-13

6.1.18 switchport access 6-14

6.1.19 switchport trunk 6-15

6.1.20 snmp trap link-status 6-16
6.2 Showing Related Command 6-17
6.2.1 show interfaces 6-17
7 Aggregate Port Configuration Commands 7-1
7.1 Configuration Related Commands 7-1
7.1.1 port-group 7-1
7.1.2 aggregateport load-balance 7-2
7.2 Showing Related Command 7-3
7.2.1 show aggregateport 7-3
8 LACP Configuration Commands 8-1
8.1 Configuration Related Commands 8-1
8.1.1 port-group mode 8-1
8.1.2 lacp port-priority 8-2
8.1.3 lacp system-priority 8-3
8.2 Showing Related Command 8-4
8.2.1 show lacp summary 8-4
9 VLAN Configuration Commands 9-1
9.1 Configuration Related Commands 9-1
9.1.1 vlan 9-1
9.1.2 name 9-2
9.1.3 switchport mode 9-2
9.1.4 switchport access 9-3
9.1.5 switchport trunk 9-4
9.2 Showing Related Command 9-6
9.2.1 show vlan 9-6
10 Super-VLAN Configuration Commands 10-1
10.1 Configuring Related Commands 10-1
10.1.1 supervlan 10-1
10.1.2 subvlan 10-1
10.1.3 subvlan-address-range 10-2
10.1.4 proxy-arp 10-3
10.2 Showing Related Command 10-3
10.2.1 show supervlan 10-3
11 Protocol VLAN Configuration Commands 11-1
11.1 Configuration Related Commands 11-1
11.1.1 protocol-vlan ipv4 *addr* mask *addr* vlan *id* 11-1

11.1.2 protocol-vlan profile *num* frame-type *type* ether-type *type* 11-2
11.1.3 protocol-vlan profile *num* vlan *id* 11-2
11.2 Showing Related Commands 11-3
11.2.1 show protocol-vlan 11-3

12 Private VLAN Configuration Commands 12-1
12.1 Configuration Related Commands 12-1
12.1.1 private-vlan *type* 12-1
12.1.2 private-vlan association 12-2
12.1.3 private-vlan mapping 12-3
12.1.4 switchport mode private-vlan 12-3
12.1.5 switchport private-vlan host-association 12-4
12.1.6 switchport private-vlan mapping 12-5
12.2 Showing Related Commands 12-5
12.2.1 show vlan private-vlan 12-5
12.3 Hybrid Commands 12-6
12.3.1 switchport mode hybrid 12-6
12.3.2 switchport hybrid native vlan 12-7
12.3.3 switchport hybrid allowed vlan 12-7

13 802.1Q Tunneling Configuration Commands 13-1
13.1 Configuration Related Commands 13-1
13.1.1 switchport mode dot1q-tunnel 13-1
13.1.2 switchport mode uplink 13-2
13.1.3 frame-tag tpid *tpid* 13-2
13.1.4 inner-priority-trust enable 13-3
13.2 Showing Command 13-4
13.2.1 show frame-tag tpid 13-4
13.2.2 show inner-priority-trust 13-4

14 MAC Address Configuration Commands 14-1
14.1 Configuration Related Commands 14-1
14.1.1 mac-address-table aging-time 14-1
14.1.2 clear mac-address-table dynamic 14-2
14.1.3 clear mac-address-table filtering 14-3
14.1.4 clear mac-address-table static 14-4
14.1.5 mac-address-table static 14-4
14.1.6 mac-address-table filtering 14-6
14.1.7 mac-address-table notification 14-6
14.1.8 snmp trap mac-notification 14-7

14.1.9 address-bind 14-8
14.1.10 address-bind *ip-address* 14-9
14.1.11 address-bind uplink 14-10
14.1.12 address-bind install 14-11
14.1.13 address-bind ipv6-mode 14-11
14.1.14 mac-manage-learning uniform 14-13
14.1.15 mac-manage-learning uniform learning-synchronization 14-13
14.1.16 mac-manage-learning dispersive 14-14
14.2 Showing Related Command 14-14
14.2.1 show mac-address-table address 14-15
14.2.2 show mac-address-table aging-time 14-16
14.2.3 show mac-address-table count 14-16
14.2.4 show mac-address-table dynamic 14-17
14.2.5 show mac-address-table filtering 14-18
14.2.6 show mac-address-table interface 14-18
14.2.7 show mac-address-table notification 14-19
14.2.8 show mac-address-table static 14-20
14.2.9 show mac-address-table vlan 14-21
14.2.10 show address-bind 14-22
14.2.11 show mac-address-table mac-manage-learning 14-22
15 DHCP Snooping Configuration Commands 15-1
15.1 DHCP Snooping Global Commands 15-1
15.1.1 ip dhcp snooping 15-1
15.1.2 ip dhcp snooping vlan 15-2
15.1.3 ip dhcp snooping bootp-bind 15-3
15.1.4 ip dhcp snooping verify mac-address 15-4
15.1.5 ip dhcp snooping information option 15-5
15.1.6 ip dhcp snooping database write-delay 15-6
15.1.7 ip dhcp snooping database write-to-flash 15-7
15.2 DHCP snooping Interface Mode Commands 15-7
15.2.1 ip dhcp snooping suppression 15-8
15.2.2 ip dhcp snooping trust 15-8
15.2.3 ip dhcp snooping limit rate 15-9
15.3 Showing Related Commands 15-10
15.3.1 show ip dhcp snooping 15-10
15.3.2 show ip dhcp snooping binding 15-11
15.4 Other DHCP Snooping Configuration Commands 15-12
15.4.1 clear ip dhcp snooping binding 15-12

15.4.2 debug ip dhcp snooping 15-13

16 IGMP Snooping Configuration Commands 16-1

16.1 Configuration Related Commands 16-1

16.1.1 deny 16-2

16.1.2 permit 16-2

16.1.3 range 16-3

16.1.4 ip igmp profile 16-4

16.1.5 ip igmp snooping dyn-mr-aging-time 16-5

16.1.6 ip igmp snooping fast-leave enable 16-6

16.1.7 ip igmp snooping filter 16-6

16.1.8 ip igmp snooping ivgl 16-7

16.1.9 ip igmp snooping ivgl-svgl 16-8

16.1.10 ip igmp snooping limit-ipmc vlan server 16-9

16.1.11 ip igmp snooping max-groups 16-9

16.1.12 ip igmp snooping query-max-response-time 16-10

16.1.13 ip igmp snooping source-check default-server 16-11

16.1.14 ip igmp snooping source-check port 16-12

16.1.15 ip igmp snooping suppression enable 16-13

16.1.16 ip igmp snooping svgl 16-14

16.1.17 ip igmp snooping svgl profile 16-14

16.1.18 ip igmp snooping vlan mrouting interface 16-15

16.1.19 ip igmp snooping vlan mrouting interface profile 16-16

16.1.20 ip igmp snooping vlan mdevice learn pim-dvmrp 16-17

16.1.21 ip igmp snooping vlan static interface 16-18

16.2 Displaying and Monitoring Commands 16-19

16.2.1 show ip igmp snooping 16-19

16.2.2 show ip igmp profile [profile-number] 16-20

16.2.3 clear ip igmp snooping gda-table 16-20

16.2.4 clear ip igmp snooping statistics 16-21

16.2.5 debug igmp-snp 16-21

17 PIM Snooping Configuration Commands 17-1

17.1 Configuration Related Command 17-1

17.1.1 ip pim snooping (global configuration mode) 17-1

17.1.2 ip pim snooping dr-flood 17-2

17.1.3 ip pim snooping (interface configuration mode) 17-3

17.1.4 show ip pim snooping 17-4

17.1.5 show ip pim snooping mroute 17-5

17.1.6 show ip pim snooping neighbor 17-6

17.1.7 show ip pim snooping statistics 17-6
17.1.8 show ip pim snooping vlan 17-7
17.1.9 clear ip pim snooping statistics 17-9
17.1.10 clear ip pim snooping vlan 17-10
17.1.11 debug ip psnp event 17-11
17.1.12 debug ip psnp mst 17-11
17.1.13 debug ip psnp packet 17-11
17.1.14 debug ip psnp port 17-12
17.1.15 debug ip psnp timer 17-12

18 MSTP Configuration Commands 18-1
18.1 Configuration Related Commands 18-1
18.1.1 spanning-tree 18-1
18.1.2 spanning-tree bpdufilter 18-2
18.1.3 spanning-tree bpduguard 18-3
18.1.4 spanning-tree link-type 18-3
18.1.5 spanning-tree max-hops 18-4
18.1.6 spanning-tree mode 18-5
18.1.7 spanning-tree mst configure 18-6
18.1.8 spanning-tree mst cost 18-7
18.1.9 spanning-tree mst port-priority 18-8
18.1.10 spanning-tree mst priority 18-10
18.1.11 spanning-tree reset 18-11
18.1.12 spanning-tree tx-hold-count 18-11
18.1.13 spanning-tree pathcost method 18-12
18.1.14 spanning-tree portfast 18-12
18.1.15 spanning-tree portfast bpduguard default 18-13
18.1.16 spanning-tree portfast bpdufilter default 18-14
18.1.17 spanning-tree portfast default 18-14
18.1.18 spanning-tree tc- protection 18-15
18.1.19 spanning-tree tc-protection tc-guard 18-15
18.1.20 spanning-tree tc-guard 18-16
18.1.21 spanning-tree guard root 18-16
18.1.22 spanning-tree loopguard default 18-17
18.1.23 spanning-tree guard loop 18-17
18.1.24 spanning-tree guard none 18-18
18.1.25 spanning-tree autoedge 18-18
18.1.26 bpdu src-mac-check 18-19
18.1.27 clear spanning-tree detected-protocols 18-20

18.1.28 spanning-tree compatible enable 18-20
18.1.29 logging event status 18-21
18.2 Showing Related Command 18-21
18.2.1 show spanning-tree 18-21
18.2.2 show spanning-tree interface 18-22
18.2.3 show spanning-tree mst 18-23
19 SPAN Configuration Commands 19-1
19.1 monitor session 19-1
19.2 Show monitor 19-2
20 RSPAN Configuration Commands 20-1
20.1 Configuring related commands 20-1
20.1.1 monitor session 20-1
20.1.2 remote-span 20-2
21 IP Address Configuration Commands 21-1
21.1 Interface Address Configuration Commands 21-1
21.1.1 ip-address 21-1
21.1.2 ip unnumbered 21-3
21.2 Address Resolution Protocol (ARP) Configuration Commands 21-4
21.2.1 arp 21-5
21.2.2 arp retry interval 21-6
21.2.3 arp retry times 21-6
21.2.4 arp trusted num 21-7
21.2.5 arp trusted aging 21-8
21.2.6 arp unresolve 21-9
21.2.7 arp gratuitous-send interval 21-10
21.2.8 arp timeout 21-11
21.2.9 ip proxy-arp 21-11
21.2.10 service trustedarp 21-12
21.3 Broadcast Message Processing Configuration Commands 21-13
21.3.1 ip broadcast-addresss 21-13
21.3.2 ip directed-broadcast 21-14
21.4 IP Address Monitoring and Maintenance Commands 21-16
21.4.1 clear arp-cache 21-16
21.4.2 show arp 21-17
21.4.3 show arp counter 21-18
21.4.4 show arp timeout 21-19
21.4.5 clear ip route 21-20

21.4.6 show ip arp 21-20
21.4.7 show ip interface 21-21
21.4.8 show ip redirects 21-23

22 IP Service Configuration Commands 22-1
22.1 IP Service Configuration Commands 22-1
22.1.1 ip default-gateway 22-1
22.1.2 ip mask-reply 22-2
22.1.3 ip mtu 22-3
22.1.4 ip redirects 22-4
22.1.5 ip source-route 22-5
22.1.6 ip unreachables 22-5

23 DHCP Configuration Commands 23-1
23.1 DHCP Configuration Related Command 23-1
23.1.1 bootfile 23-2
23.1.2 client-identifier 23-2
23.1.3 client-name 23-4
23.1.4 default-device 23-5
23.1.5 dns-server 23-5
23.1.6 domain-name 23-7
23.1.7 hardware-address 23-7
23.1.8 host 23-9
23.1.9 ip address dhcp 23-10
23.1.10 ip dhcp excluded-address 23-10
23.1.11 ip dhcp ping packet 23-11
23.1.12 ip dhcp ping timeout 23-12
23.1.13 ip dhcp pool 23-13
23.1.14 lease 23-14
23.1.15 netbios-name-server 23-15
23.1.16 netbios-node-type 23-16
23.1.17 network (DHCP) 23-17
23.1.18 next-server 23-18
23.1.19 option 23-19
23.1.20 service dhcp 23-21
23.2 Showing and Monitoring Commands 23-21
23.2.1 clear ip dhcp binding 23-22
23.2.2 clear ip dhcp conflict 23-22
23.2.3 clear ip dhcp server statistics 23-23
23.2.4 debug ip dhcp client 23-24

23.2.5 debug ip dhcp server 23-24
23.2.6 show dhcp lease 23-25
23.2.7 show ip dhcp binding 23-26
23.2.8 show ip dhcp conflict 23-27
23.2.9 show ip dhcp server statistics 23-28

24 DHCP Relay Configuration Commands 24-1
24.1 DHCP Relay Configuration Command 24-1
24.1.1 service dhcp 24-1
24.1.2 ip helper-address 24-2
24.1.3 ip dhcp relay information option dot1x 24-2
24.1.4 ip dhcp relay information option dot1x access-group 24-3
24.1.5 ip dhcp relay information option82 24-4
24.1.6 ip dhcp relay check server-id 24-4
24.1.7 ip dhcp relay suppression 24-5

25 DNS Module Configuration Commands 25-1
25.1 Configuring Related Commands 25-1
25.1.1 ip domain-lookup 25-1
25.1.2 ip name-server 25-2
25.1.3 ip host 25-2
25.1.4 clear host 25-3
25.1.5 show hosts 25-4

26 SNTP Configuration Commands 26-1
26.1 Configuring Related Commands 26-1
26.1.1 sntp enable 26-1
26.1.2 sntp server 26-2
26.1.3 sntp interval 26-2
26.2 Showing Related Command 26-3
26.2.1 show sntp 26-3

27 NTP Configuration Commands 27-1
27.1 NTP Configuring Related Commands 27-1
27.1.1 no ntp 27-1
27.1.2 ntp access-group 27-2
27.1.3 ntp authenticate 27-3
27.1.4 ntp authentication-key 27-4
27.1.5 ntp disable 27-5
27.1.6 ntp master 27-6
27.1.7 ntp server 27-7

27.1.8 ntp synchronize 27-8
27.1.9 ntp trusted-key 27-9
27.1.10 ntp update-calendar 27-10
27.2 Showing and Monitoring Commands 27-10
27.2.1 debug ntp 27-10
27.2.2 show ntp status 27-11
28 UDP-Helper Module Configuration Commands 28-1
28.1 Configuration Related Commands 28-1
28.1.1 udp-helper enable 28-1
28.1.2 ip helper-address 28-2
28.1.3 ip forward-protocol 28-3
29 SNMP Configuration Command 29-1
29.1 Configuration Related Commands 29-1
29.1.1 no snmp-server 29-1
29.1.2 snmp-server chassis-id 29-2
29.1.3 snmp-server community 29-3
29.1.4 snmp-server contact 29-4
29.1.5 snmp-server enable traps 29-4
29.1.6 snmp-server host 29-5
29.1.7 snmp-server location 29-6
29.1.8 snmp-server packetsize 29-7
29.1.9 snmp-server queue-length 29-8
29.1.10 snmp-server system-shutdown 29-8
29.1.11 snmp-server trap-source 29-9
29.1.12 snmp-server trap-timeout 29-10
29.1.13 snmp-server user 29-10
29.1.14 snmp-server group 29-12
29.1.15 snmp-server view 29-13
29.1.16 snmp-server if-index persist 29-13
29.2 Showing Related Command 29-14
29.2.1 show snmp 29-14
30 RMON Configuration Commands 30-1
30.1 Configuration Related Commands 30-1
30.1.1 rmon collection stats 30-1
30.1.2 rmon collection history 30-2
30.1.3 rmon alarm 30-3
30.1.4 rmon event 30-3

30.2 Showing Related Commands 30-4
30.2.1 show rmon statistics 30-4
30.2.2 show rmon history 30-5
30.2.3 show rmon alarm 30-6
30.2.4 show rmon event 30-7
31 RIP Configuration Commands 31-1
31.1 Configuration Related Commands 31-1
31.1.1 address-family (RIP) 31-1
31.1.2 auto-summary (RIP) 31-2
31.1.3 default-metric (RIP) 31-4
31.1.4 default-information originate(RIP) 31-5
31.1.5 distance 31-7
31.1.6 distribute-list in (RIP) 31-7
31.1.7 distribute-list out (RIP) 31-9
31.1.8 exit-address-family 31-10
31.1.9 ip rip authentication key-chain 31-11
31.1.10 ip rip authentication mode 31-12
31.1.11 ip rip authentication text-password 31-13
31.1.12 ip rip default-information 31-14
31.1.13 ip rip receive enable 31-16
31.1.14 ip rip receive version 31-17
31.1.15 ip rip send enable 31-18
31.1.16 ip rip send version 31-19
31.1.17 ip rip v2-broadcast 31-20
31.1.18 ip split-horizon (RIP) 31-21
31.1.19 ip summary-address rip 31-22
31.1.20 network (RIP) 31-23
31.1.21 neighbor (RIP) 31-24
31.1.22 offset-list(RIP) 31-25
31.1.23 output-delay 31-26
31.1.24 passive-interface 31-27
31.1.25 redistribute (RIP) 31-29
31.1.26 router rip 31-30
31.1.27 timers basic 31-31
31.1.28 validate-update-source 31-32
31.1.29 version (RIP) 31-34
31.2 Showing Related Command 31-35
31.2.1 show ip rip 31-35

31.2.2 show ip rip database 31-36
31.2.3 show ip rip external 31-37
31.2.4 show ip rip interface 31-38

32 OSPFv2 Configuration Commands 32-1
32.1 Configuration Related Commands 32-1
32.1.1 area 32-1
32.1.2 area authentication 32-2
32.1.3 area default-cost 32-3
32.1.4 area filter-list 32-4
32.1.5 area nssa 32-5
32.1.6 area range 32-6
32.1.7 area stub 32-8
32.1.8 area virtual-link 32-9
32.1.9 auto-cost 32-11
32.1.10 clear ip ospf process 32-12
32.1.11 compatible rfc1583 32-13
32.1.12 default-information originate (OSPF) 32-13
32.1.13 default-metric 32-15
32.1.14 distance ospf 32-16
32.1.15 distribute-list in 32-17
32.1.16 distribute-list out 32-18
32.1.17 enable mib-binding 32-19
32.1.18 enable traps 32-19
32.1.19 ip ospf authentication 32-22
32.1.20 ip ospf authentication-key 32-23
32.1.21 ip ospf cost 32-24
32.1.22 ip ospf database-filter all out 32-25
32.1.23 ip ospf dead-interval 32-26
32.1.24 ip ospf disable all 32-27
32.1.25 ip ospf hello-interval 32-27
32.1.26 ip ospf message-digest-key 32-28
32.1.27 ip ospf mtu-ignore 32-30
32.1.28 ip ospf network 32-30
32.1.29 ip ospf priority 32-33
32.1.30 ip ospf retransmit-interval 32-34
32.1.31 ip ospf transmit-delay 32-35
32.1.32 log-adj-changes 32-36
32.1.33 max-concurrent-dd 32-37

32.1.34 neighbor 32-37
32.1.35 network area 32-39
32.1.36 overflow database 32-40
32.1.37 overflow database external 32-41
32.1.38 overflow memory-lack 32-41
32.1.39 passive-interface 32-43
32.1.40 redistribute 32-43
32.1.41 router ospf 32-45
32.1.42 router-id 32-46
32.1.43 summary-address 32-47
32.1.44 timers lsa-group-pacing 32-48
32.1.45 timers spf 32-49
32.2 Showing Related Command 32-50
32.2.1 show ip ospf 32-50
32.2.2 show ip ospf border-devices 32-53
32.2.3 show ip ospf database 32-54
32.2.4 show ip ospf interface 32-66
32.2.5 show ip ospf neighbor 32-68
32.2.6 show ip ospf route 32-71
32.2.7 show ip ospf summary-address 32-72
32.2.8 show ip ospf virtual-link 32-72
33 BGP4 Configuration Commands 33-1
33.1 Configuration Related Commands 33-1
33.1.1 address-family ipv4 33-1
33.1.2 address-family ipv4 vrf 33-2
33.1.3 address-family vpnv4 33-2
33.1.4 aggregate-address (IPv4) 33-3
33.1.5 auto-summary 33-4
33.1.6 bgp always-compare-med 33-5
33.1.7 bgp bestpath as-path ignore 33-6
33.1.8 bgp bestpath compare-confed-aspath 33-7
33.1.9 bgp bestpath compare-routerid 33-7
33.1.10 bgp bestpath med confed 33-8
33.1.11 bgp bestpath med missing-as-worst 33-9
33.1.12 bgp client-to-client reflection 33-10
33.1.13 bgp cluster-id 33-11
33.1.14 bgp confederation identifier 33-12
33.1.15 bgp confederation peers 33-13

33.1.16 bgp default ipv4-unicast 33-14
33.1.17 bgp default local-preference 33-15
33.1.18 bgp deterministic-med 33-16
33.1.19 bgp enforce-first-as 33-17
33.1.20 bgp fast-external-fallover 33-18
33.1.21 bgp log-neighbor-changes 33-19
33.1.22 bgp router-id 33-19
33.1.23 clear bgp ipv4 unicast 33-20
33.1.24 clear bgp ipv4 unicast dampening 33-22
33.1.25 clear bgp ipv4 unicast external 33-22
33.1.26 clear bgp ipv4 unicast flap-statistics 33-23
33.1.27 clear bgp ipv4 unicast peer-group 33-24
33.1.28 clear ip bgp 33-25
33.1.29 clear ip bgp dampening 33-27
33.1.30 clear ip bgp external 33-27
33.1.31 clear ip bgp flap-statistics 33-28
33.1.32 clear ip bgp peer-group 33-29
33.1.33 clear ip bgp vrf 33-30
33.1.34 default-information originate 33-31
33.1.35 default-metric 33-32
33.1.36 distance bgp 33-33
33.1.37 exit-address-family 33-34
33.1.38 ip as-path access-list 33-35
33.1.39 maximum-prefix 33-36
33.1.40 neighbor activate 33-37
33.1.41 neighbor advertisement-interval 33-38
33.1.42 neighbor allowas-in 33-39
33.1.43 neighbor as-override 33-40
33.1.44 neighbor default-originate 33-41
33.1.45 neighbor description 33-42
33.1.46 neighbor distribute-list 33-43
33.1.47 neighbor ebgp-multihop 33-44
33.1.48 neighbor filter-list 33-45
33.1.49 neighbor maximum-prefix 33-46
33.1.50 neighbor next-hop-self 33-47
33.1.51 neighbor password 33-48
33.1.52 neighbor peer-group (assigning members) 33-50
33.1.53 neighbor peer-group (creating) 33-51
33.1.54 neighbor prefix-list 33-52

33.1.55 neighbor remote-as 33-53
33.1.56 neighbor remove-private-as 33-54
33.1.57 neighbor route-map 33-55
33.1.58 neighbor route-reflector-client 33-56
33.1.59 neighbor send-community 33-57
33.1.60 neighbor shutdown 33-58
33.1.61 neighbor soft-reconfiguration inbound 33-59
33.1.62 neighbor soo 33-60
33.1.63 neighbor timers 33-61
33.1.64 neighbor unsuppress-map 33-63
33.1.65 neighbor update-source 33-64
33.1.66 neighbor version 33-65
33.1.67 neighbor weight 33-66
33.1.68 network(BGP) 33-67
33.1.69 network synchronization 33-68
33.1.70 overflow memory-lack 33-68
33.1.71 redistribute 33-70
33.1.72 redistribute (OSPF) 33-71
33.1.73 redistribute (ISIS) 33-72
33.1.74 router bgp 33-73
33.1.75 synchronization 33-74
33.1.76 timers bgp 33-75
33.2 Showing Related Command 33-76
33.2.1 show ip bgp 33-76
33.2.2 show ip bgp cidr-only 33-77
33.2.3 show ip bgp community 33-78
33.2.4 show ip bgp community-list 33-79
33.2.5 show ip bgp dampening dampened-paths 33-79
33.2.6 show ip bgp dampening flap-statistics 33-80
33.2.7 show ip bgp dampening parameters 33-81
33.2.8 show ip bgp filter-list 33-82
33.2.9 show ip bgp inconsistent-as 33-82
33.2.10 show ip bgp neighbors 33-83
33.2.11 show ip bgp paths 33-85
33.2.12 show ip bgp quote-regexp 33-85
33.2.13 show ip bgp regexp 33-86
33.2.14 show ip bgp summary 33-87
33.2.15 show ip bgp vpnv4 33-88
33.2.16 show ip community-list 33-89

33.2.17 show ip as-path-access-list 33-89

34 Protocol-independent Configuration Commands 34-1

34.1 Configuration Related Commands 34-1

34.1.1 distribute-list in 34-1

34.1.2 distribute-list out 34-2

34.1.3 ip community-list 34-3

34.1.4 ip default-network 34-5

34.1.5 ip prefix-list 34-6

34.1.6 ip prefix-list description 34-7

34.1.7 ip prefix-list sequence-number 34-8

34.1.8 ip route 34-9

34.1.9 ip routing 34-11

34.1.10 ip static route-limit 34-11

34.1.11 ipv6 prefix-list 34-12

34.1.12 ipv6 prefix-list description 34-14

34.1.13 ipv6 prefix-list sequence-number 34-15

34.1.14 match as-path 34-16

34.1.15 match community 34-17

34.1.16 match interface 34-18

34.1.17 match ip address 34-19

34.1.18 match ip next-hop 34-21

34.1.19 match ip route-source 34-23

34.1.20 match ipv6 address 34-24

34.1.21 match ipv6 next-hop 34-26

34.1.22 match ipv6 route-source 34-28

34.1.23 match length 34-30

34.1.24 match metric 34-32

34.1.25 match origin 34-33

34.1.26 match route-type 34-34

34.1.27 match tag 34-36

34.1.28 maximum-paths 34-38

34.1.29 route-map 34-38

34.1.30 set aggregator as 34-41

34.1.31 set as-path prepend 34-42

34.1.32 set comm-list delete 34-43

34.1.33 set community 34-44

34.1.34 set dampening 34-46

34.1.35 set default interface 34-47

34.1.36 set extcommunity 34-49
34.1.37 set interface 34-50
34.1.38 set ip default next-hop 34-52
34.1.39 set ip dscp 34-54
34.1.40 set ip next-hop 34-55
34.1.41 set ip next-hop verify-availability 34-57
34.1.42 set ip precedence 34-59
34.1.43 set ip tos 34-60
34.1.44 set level 34-62
34.1.45 set local-preference 34-63
34.1.46 set metric 34-64
34.1.47 set metric-type 34-66
34.1.48 set next-hop 34-67
34.1.49 set origin 34-69
34.1.50 set originator-id 34-70
34.1.51 set tag 34-71
34.1.52 set weight 34-72
34.1.53 ip ref ecmp load-balance source 34-74
34.2 Show Related Command 34-75
34.2.1 show route-map 34-75
34.2.2 show ip community-list 34-76
34.2.3 show ip prefix-list 34-76
34.2.4 show ip route 34-77
34.2.5 show ipv6 prefix-list 34-79
34.2.6 show ip ref 34-80
35 PBR Configuration Commands 35-1
35.1 Configuration Related Commands 35-1
35.1.1 ip policy route-map 35-1
35.1.2 ip policy 35-3
36 IPv6 Configuration Commands 36-1
36.1 Configuration Related Commands 36-1
36.1.1 ping ipv6 36-2
36.1.2 ipv6 address 36-2
36.1.3 ipv6 enable 36-3
36.1.4 ipv6 hop-limit 36-4
36.1.5 ipv6 neighbor 36-4
36.1.6 ipv6 source-route 36-5
36.1.7 ipv6 route 36-6

36.1.8 ipv6 ns-linklocal-src 36-7
36.1.9 ipv6 nd ns-interval 36-8
36.1.10 ipv6 nd reachable-time 36-9
36.1.11 ipv6 nd prefix 36-10
36.1.12 ipv6 nd ra-lifetime 36-11
36.1.13 ipv6 nd ra-interval 36-12
36.1.14 ipv6 nd ra-hoplimit 36-13
36.1.15 ipv6 nd ra-mtu 36-14
36.1.16 ipv6 nd managed-config-flag 36-15
36.1.17 ipv6 nd dad attempts 36-16
36.1.18 ipv6 nd suppress-ra 36-17
36.1.19 ipv6 redirects 36-17
36.1.20 clear ipv6 neighbors 36-18
36.1.21 tunnel mode ipv6ip 36-18
36.1.22 tunnel destination 36-19
36.1.23 tunnel source 36-20
36.1.24 tunnel ttl 36-21
36.2 Show Related Command 36-22
36.2.1 show ipv6 route 36-22
36.2.2 show ipv6 neighbors 36-23
36.2.3 show ipv6 interface 36-25
37 OSPFv3 Configuration Commands 37-1
37.1 Configuration Related Commands 37-1
37.1.1 area default-cost 37-1
37.1.2 area-range 37-2
37.1.3 area stub 37-3
37.1.4 area virtual-link 37-4
37.1.5 auto-cost 37-5
37.1.6 clear ipv6 ospf process 37-6
37.1.7 default-information originate 37-7
37.1.8 default-metric 37-8
37.1.9 ipv6 ospf area 37-9
37.1.10 ipv6 ospf cost 37-10
37.1.11 ipv6 ospf dead-interval 37-11
37.1.12 ipv6 ospf hello-interval 37-12
37.1.13 ipv6 ospf neighbor 37-13
37.1.14 ipv6 ospf network 37-14
37.1.15 ipv6 ospf priority 37-15

37.1.16 ipv6 ospf retransmit-interval 37-16
37.1.17 ipv6 ospf transmit-delay 37-17
37.1.18 ipv6 router ospf 37-18
37.1.19 log-adj-changes 37-19
37.1.20 max-concurrent-dd 37-20
37.1.21 passive-interface 37-20
37.1.22 redistribute 37-21
37.1.23 router-id 37-23
37.1.24 timers spf 37-24
37.2 Show Related Command 37-25
37.2.1 show ipv6 ospf 37-25
37.2.2 show ipv6 ospf database 37-26
37.2.3 show ipv6 ospf interface 37-28
37.2.4 show ipv6 ospf neighbor 37-29
37.2.5 show ipv6 ospf route 37-30
37.2.6 show ipv6 ospf topology 37-31
37.2.7 show ipv6 ospf virtual-links 37-32
38 IGMP Configuration Commands 38-1
38.1 IGMP Configuration Task List 38-1
38.1.1 clear ip igmp group 38-2
38.1.2 clear ip igmp interface 38-2
38.1.3 ip igmp access-group 38-3
38.1.4 ip igmp join-group 38-4
38.1.5 ip igmp static-group 38-4
38.1.6 ip igmp immediate-leave group-list 38-5
38.1.7 ip igmp last-member-query-count 38-6
38.1.8 ip igmp last-member-query-interval 38-7
38.1.9 ip igmp limit (interface configuration) 38-8
38.1.10 ip igmp query-interval 38-9
38.1.11 ip igmp query-max-response-time 38-9
38.1.12 ip igmp query-timeout 38-10
38.1.13 ip igmp robustness-variable 38-11
38.1.14 ip igmp version 38-11
38.1.15 ip igmp limit (global configuration) 38-12
38.1.16 ip igmp proxy-service 38-13
38.1.17 ip igmp mroute-proxy 38-14
38.1.18 ip igmp ssm-map enable 38-14
38.1.19 ip igmp ssm-map static 38-15

38.2 Show Related Commands 38-16
38.2.1 show ip igmp groups 38-16
38.2.2 show ip igmp interface 38-17
38.2.3 show ip igmp ssm-mapping 38-18

39 PIM-DM Configuration Commands 39-1
39.1 PIM-DM Related Configuration Commands 39-1
39.1.1 ip pim dense-mode 39-1
39.1.2 ip pim neighbor-filter 39-2
39.1.3 ip pim query-interval 39-3
39.1.4 ip pim state-refresh disable 39-4
39.1.5 ip pim state-refresh origination-interval 39-5
39.2 Show Related Commands 39-5
39.2.1 show ip pim dense-mode interface 39-5
39.2.2 show ip pim dense-mode neighbor 39-6
39.2.3 show ip pim dense-mode nexthop 39-7
39.2.4 show ip pim dense-mode mroute 39-8

40 PIM-SM Configuraiton Commands 40-1
40.1 PIM-SM Configuration Commands 40-1
40.1.1 clear ip mroute 40-2
40.1.2 clear ip mroute statistics 40-2
40.1.3 clear ip pim sparse-mode bsr rp-set 40-3
40.1.4 ip multicast-routing 40-3
40.1.5 ip pim accept-register list 40-4
40.1.6 ip pim bsr-candidate 40-4
40.1.7 ip pim cisco-register-checksum 40-6
40.1.8 ip pim dr-priority 40-6
40.1.9 ip pim ignore-rp-set-priority 40-7
40.1.10 ip pim jp-timer 40-8
40.1.11 ip pim mib 40-8
40.1.12 ip pim neighbor-filter 40-9
40.1.13 ip pim query-interval 40-9
40.1.14 ip pim register-rate-limit 40-10
40.1.15 ip pim register-rp-reachability 40-10
40.1.16 ip pim register-source 40-11
40.1.17 ip pim register-suppression 40-12
40.1.18 ip pim rp-address 40-12
40.1.19 ip pim rp-candidate 40-13
40.1.20 ip pim rp-register-kat 40-14

40.1.21 ip pim sparse-mode 40-15
40.1.22 ip pim spt-threshold 40-16
40.1.23 ip pim ssm 40-17
40.2 Show Related Commands 40-18
40.2.1 show debugging 40-18
40.2.2 show ip pim sparse-mode bsr-router 40-18
40.2.3 show ip pim sparse-mode interface 40-19
40.2.4 show ip pim sparse-mode local-members 40-19
40.2.5 show ip pim sparse-mode mroute 40-20
40.2.6 show ip pim sparse-mode neighbor 40-20
40.2.7 show ip pim sparse-mode nexthop 40-21
40.2.8 show ip pim sparse-mode rp mapping 40-21
40.2.9 show ip pim sparse-mode rp-hash 40-22

41 Multicast Routing Configuration Commands 41-1
41.1 Configuration Related Commands: 41-1
41.1.1 clear ip mroute 41-1
41.1.2 clear ip mroute statistics 41-2
41.1.3 ip mroute 41-3
41.1.4 ip multicast route-limit 41-4
41.1.5 ip multicast ttl-threshold 41-4
41.1.6 ip multicast-routing 41-5
41.1.7 ip multicast-rpf 41-6
41.1.8 ip multicast boundary 41-7
41.1.9 ip multicast static 41-7
41.2 Show Related Commands 41-8
41.2.1 show ip mroute 41-8
41.2.2 show ip rpf 41-11
41.2.3 show ip mvif 41-12
41.3 Debugging Related Commands 41-12
41.3.1 debug nsm mcast all 41-12
41.3.2 debug nsm mcast fib-msg 41-13
41.3.3 debug nsm mcast vrf 41-13
41.3.4 debug nsm mcast register 41-14
41.3.5 debug nsm mcast stats 41-14

42 MPLS Configuration Commands 42-1
42.1 Basic MPLS Commands 42-1
42.1.1 advertise-labels for 42-1
42.1.2 discovery targeted-hello 42-2

42.1.3 label-merge 42-3
42.1.4 label-retention-mode 42-4
42.1.5 label-switching 42-5
42.1.6 ldp router-id 42-6
42.1.7 loop-detection 42-7
42.1.8 lsp-control-mode 42-8
42.1.9 mpls ip (Global configuration mode) 42-9
42.1.10 mpls ip (Interface configuration mode) 42-9
42.1.11 mpls ip fragment 42-10
42.1.12 mpls ip icmp forward 42-11
42.1.13 mpls ip ttl expiration 42-12
42.1.14 mpls ip ttl propagate 42-13
42.1.15 mpls ldp distribution-mode 42-14
42.1.16 mpls ldp hello-holdtime 42-15
42.1.17 mpls ldp hello-interval 42-16
42.1.18 mpls ldp keepalive-holdtime 42-17
42.1.19 mpls ldp max-hop-count 42-18
42.1.20 mpls ldp max-label-requests 42-19
42.1.21 mpls ldp max-path-vector 42-20
42.1.22 mpls ldp max-pdu 42-21
42.1.23 transport-address 42-22
42.1.24 mpls mtu 42-23
42.1.25 mpls router ldp 42-24
42.1.26 mpls static ftn 42-25
42.1.27 mpls static l3vpn-ftn 42-26
42.1.28 mpls static l2vc-ftn 42-27
42.1.29 mpls static ilm in-label 42-28
42.1.30 neighbor 42-30
42.1.31 propagate-release 42-31
42.1.32 show mpls forwarding-table 42-31
42.1.33 show mpls label-pool 42-34
42.1.34 show mpls ldp bindings 42-35
42.1.35 show mpls ldp discovery 42-36
42.1.36 show mpls ldp neighbor 42-37
42.1.37 show mpls ldp parameters 42-38
42.1.38 show mpls ldp session 42-39
42.1.39 show mpls summary 42-40
42.1.40 target-session holdtime 42-41
42.2 BGP/MPLS L3 VPN Commands 42-42

42.2.1 address-family ipv4 vrf 42-42
42.2.2 address-family vpnv4 42-43
42.2.3 clear ip bgp vrf 42-44
42.2.4 exit address-family 42-45
42.2.5 ip route static inter-vrf 42-45
42.2.6 ip route vrf 42-46
42.2.7 ip vrf 42-47
42.2.8 ip vrf forwarding 42-48
42.2.9 maximum routes 42-49
42.2.10 neighbor activate 42-50
42.2.11 neighbor allowas-in 42-51
42.2.12 neighbor as-override 42-52
42.2.13 neighbor description 42-53
42.2.14 neighbor remote-as 42-55
42.2.15 neighbor shutdown 42-56
42.2.16 neighbor soo 42-57
42.2.17 rd 42-58
42.2.18 redistribute 42-59
42.2.19 redistribute OSPF 42-61
42.2.20 route-target 42-63
42.2.21 show ip bgp vpnv4 42-64
42.2.22 show ip route vrf 42-66
42.2.23 show ip vrf 42-67
42.3 L2 VPN Commands 42-68
42.3.1 show mpls l2transport vc 42-68
42.3.2 show mpls l2vc ftn-table 42-71
42.3.3 show mpls ldp vc 42-71
42.3.4 vc-withdraw-expect-release 42-74
42.3.5 xconnect 42-75
43 Port-based Flow Control Configuration Commands 43-1
43.1 Configuration Related Commands 43-1
43.1.1 storm-control 43-1
43.1.2 switchport protected 43-3
43.1.3 protected-ports route-deny 43-3
43.1.4 switchport port-security 43-4
43.1.5 switchport port-security aging 43-5
43.1.6 switchport port-security mac-address 43-6
43.1.7 arp-check 43-7

43.2 Show Related Command 43-8
43.2.1 show storm-control 43-8
43.2.2 show port-security 43-9

44 802.1X Configuration Commands 44-1
44.1 dot1x Active Authentication Command 44-1
44.1.1 dot1x auto-req 44-1
44.1.2 dot1x auto-req packet-num 44-2
44.1.3 dot1x auto-req req-interval 44-3
44.1.4 dot1x auto-req user-detect 44-4
44.2 dot1x Timeout Parameter Setting Commands 44-4
44.2.1 dot1x timeout quiet-period 44-5
44.2.2 dot1x timeout re-authperiod 44-6
44.2.3 dot1x timeout server-timeout 44-7
44.2.4 dot1x timeout supp-timeout 44-8
44.2.5 dot1x timeout tx-period 44-9
44.3 dot1x Re-authentication Commands 44-10
44.3.1 dot1x re-authentication 44-10
44.3.2 dot1x reauth-max 44-11
44.4 dot1x Detection Function Commands 44-12
44.4.1 dot1x probe-timer 44-12
44.4.2 dot1x client-probe enable 44-13
44.5 Other dot1x Configuration Commands 44-14
44.5.1 dot1x authentication 44-15
44.5.2 dot1x auth-address-table 44-16
44.5.3 dot1x auth-mode 44-16
44.5.4 dot1x default 44-17
44.5.5 dot1x dynamic-vlan enable 44-18
44.5.6 dot1x guest-vlan 44-19
44.5.7 dot1x eapol-tag 44-20
44.5.8 dot1x max-req 44-20
44.5.9 dot1x private-supplicant-only 44-21
44.5.10 dot1x port-control auto 44-22
44.5.11 dot1x port-control-mode 44-23
44.5.12 dot1x stationarity enable 44-24
44.6 Show Related Commands 44-25
44.6.1 show dot1x 44-26
44.6.2 show dot1x auth-address-table 44-27
44.6.3 show dot1x auto-req 44-28

44.6.4 show dot1x private-supplicant-only 44-29
44.6.5 show dot1x max-req 44-31
44.6.6 show dot1x port-control 44-32
44.6.7 show dot1x probe-timer 44-33
44.6.8 show dot1x re-authentication 44-34
44.6.9 show dot1x reauth-max 44-35
44.6.10 show dot1x summary 44-36
44.6.11 show dot1x user id 44-37
44.6.12 show dot1x timeout 44-39

45 AAA Configuration Commands 45-1
45.1 ID Authentication Related Command 45-1
45.1.1 aaa authentication dot1x 45-1
45.1.2 aaa authentication enable 45-2
45.1.3 aaa authentication login 45-3
45.1.4 aaa authentication ppp 45-5
45.1.5 login authentication 45-6
45.2 Authorization Related Commands 45-7
45.2.1 aaa authorization commands 45-7
45.2.2 aaa authorization config-commands 45-9
45.2.3 aaa authorization console 45-9
45.2.4 aaa authorization exec 45-10
45.2.5 aaa authorization network 45-12
45.2.6 authorization commands 45-13
45.2.7 aaa authorization exec 45-14
45.3 Accounting Related commands 45-15
45.3.1 aaa accounting commands 45-15
45.3.2 aaa accounting exec 45-17
45.3.3 aaa accounting network 45-18
45.3.4 aaa accounting update 45-19
45.3.5 aaa accounting update periodic 45-20
45.3.6 accounting commands 45-21
45.3.7 accounting exec 45-22
45.4 AAA Server Group Commands 45-23
45.4.1 aaa group server 45-23
45.4.2 ip vrf forwarding 45-24
45.4.3 server 45-24
45.4.4 show aaa group 45-25
45.5 Other AAA Commands 45-26

45.5.1 aaa local authentication attempts 45-26
45.5.2 aaa local authentication lockout-time 45-27
45.5.3 aaa new-model 45-28
45.5.4 clear aaa local user lockout 45-28
45.5.5 debug aaa 45-29
45.5.6 show aaa method-list 45-29
45.5.7 show aaa user lockout 45-30

46 RADIUS Configuration Commands 46-1
46.1 Configuration Related Commands 46-1
46.1.1 ip radius source-interface 46-1
46.1.2 radius-server host 46-2
46.1.3 radius-server key 46-3
46.1.4 radius-server retransmit 46-4
46.1.5 radius-server timeout 46-5
46.1.6 radius-server deadtime 46-6
46.1.7 radius attribute 46-7
46.1.8 radius set qos cos 46-9
46.1.9 radius vendor-specific extend 46-10
46.2 Show Related Commands 46-10
46.2.1 debug radius 46-11
46.2.2 show radius server 46-11
46.2.3 show radius parameter 46-12
46.2.4 show radius vendor-specific 46-13

47 TACACS+ Configuration Commands 47-1
47.1 Related Commands of TACACS+ Configuration 47-1
47.1.1 aaa group server tacacs+ 47-1
47.1.2 server(TACACS+) 47-2
47.1.3 ip vrf forwarding(TACACS+) 47-3
47.1.4 ip tacacs source-interface 47-4
47.1.5 tacacs-server host 47-5
47.1.6 tacacs-server key 47-6
47.1.7 tacacs-server timeout 47-7
47.2 TACACS+ Privileged Command 47-8
47.2.1 debug tacacs+ 47-8
47.2.2 show tacacs 47-8

48 SSH Configuration Commands 48-1
48.1 Related Configuration Commands 48-1

48.1.1 crypto key generate 48-1
48.1.2 crypto key zeroize 48-2
48.1.3 ip ssh version 48-3
48.1.4 ip ssh time-out 48-4
48.1.5 ip ssh authentication-retries 48-5
48.2 Showing Related Commands 48-5
48.2.1 show ip ssh 48-6
48.2.2 show ssh 48-7
48.2.3 show crypto key mypubkey 48-7
48.2.4 disconnect ssh 48-8

49 CPU Protection Configuration Commands 49-1
49.1 Related Configuration Commands 49-1
49.1.1 cpu-protect type packet-type pps pps_value 49-1
49.1.2 cpu-protect type packet-type pri *pri_num* 49-2
49.2 Showing Related Command 49-2
49.2.1 show cpu-protect mboard 49-2
49.2.2 show cpu-protect slot 49-3
49.2.3 show cpu-protect type 49-4

50 Anti-attack System Guard Configuration Commands 50-1
50.1 Configuration Related Commands 50-1
50.1.1 system-guard enable 50-1
50.1.2 system-guard isolate-time seconds 50-2
50.1.3 system-guard same-dest-ip-attack-packets number 50-3
50.1.4 system-guard scan-dest-ip-attack-packets number 50-3
50.1.5 system-guard detect-maxnum number 50-4
50.1.6 system-guard exception-ip ip mask 50-5
50.1.7 clear system-guard [interface interface-id [ip-address]] 50-6
50.2 Showing Related Command 50-7
50.2.1 show system-guard [interface *interface-id*] 50-7
50.2.2 show system-guard isolate-ip [interface *interface-id*] 50-8
50.2.3 show system-guard detect-ip [interface *interface-id*] 50-8
50.2.4 show system-guard exception-ip [interface *interface-id*] 50-9

51 DAI Configuration Commands 51-1
51.1 Commands for Enabling and Disabling the DAI Inspection Function of the Specified VLAN 51-1
51.1.1 ip arp inspection vlan *vlan-id* 51-1
51.2 Commands for Configuring the L2 Port to a Trusted Port 51-2
51.2.1 ip arp inspection trust 51-2

51.3 DHCP Snooping Database Related Configuration 51-3

52 IP Source Guard Configuration Commands 52-1

52.1 IP Source Guard Global Command 52-1

52.1.1 ip source binding 52-1

52.2 IP Source Guard Command in the Interface Mode 52-2

52.2.1 ip verify source 52-2

52.3 Other IP Source Guard Commands 52-3

52.3.1 show ip source binding 52-3

52.3.2 show ip verify source 52-4

52.3.3 debug ip source bind 52-5

53 NFPP Configuration Commands 53-1

53.1 Related Configuration Commands 53-1

53.1.1 cpu-protect sub-interface {manage | protocol | route} pps 53-1

53.1.2 cpu-protect sub-interface {manage | protocol | route} percent 53-2

53.1.3 arp-guard isolate timeout 53-3

53.1.4 arp-guard rate-limit 53-4

53.1.5 arp-guard attack-threshold 53-4

53.1.6 arp-guard scan-threshold 53-6

53.1.7 clear arp-guard users 53-8

53.1.8 clear arp-guard scan 53-9

53.2 Showing and Monitoring Commands 53-9

53.2.1 show arp-guard configuration 53-9

53.2.2 show arp-guard users 53-10

53.2.3 show arp-guard scan 53-11

54 ACL Configuration Commands 54-1

54.1 Configuration Related Commands 54-3

54.1.1 access-list 54-4

54.1.2 ip access-list 54-12

54.1.3 mac access-list 54-13

54.1.4 expert access-list 54-14

54.1.5 ipv6 access-list 54-15

54.1.6 ip access-list resequence 54-16

54.1.7 deny 54-17

54.1.8 permit 54-23

54.1.9 list-remark text 54-28

54.1.10 no sn 54-28

54.1.11 ip access-group 54-29

54.1.12 mac access-group 54-30
54.1.13 expert access-group 54-31
54.1.14 ipv6 traffic-filter 54-32
54.2 Showing Related Commands 54-33
54.2.1 show access-lists 54-34
54.2.2 show ip access-group 54-35
54.2.3 show expert access-group 54-35
54.2.4 show mac access-group 54-36
54.2.5 show ipv6 traffic-filter 54-37
54.2.6 show access-group 54-37
54.3 Security Channel 54-38
54.3.1 security global access-group 54-39
54.3.2 security access-group 54-39
54.3.3 security uplink enable 54-40

55 VACL Configuration Commands 55-1
55.1 Configuring Related Commands 55-1
55.1.1 vlan access-map 55-1
55.1.2 match ip/mac address 55-2
55.1.3 action forward/drop/redirect 55-3
55.1.4 vlan filter 55-4
55.2 Showing Related Commands 55-4
55.2.1 show vlan access-map 55-4
55.2.2 show vlan filter 55-5

56 QoS Configuration Command 56-1
56.1 Default Configuration 56-1
56.2 Related Configuration Commands 56-2
56.2.1 mls qos trust 56-2
56.2.2 mls qos cos 56-3
56.2.3 class maps 56-3
56.2.4 policy maps 56-5
56.2.5 service-policy 56-6
56.2.6 priority-queue 56-7
56.2.7 wrr-queue bandwidth 56-8
56.2.8 mls qos map cos-dscp 56-9
56.2.9 mls qos map dscp-cos 56-9
56.2.10 interface rate-limit 56-10
56.2.11 mls qos scheduler 56-11
56.2.12 drr-queue bandwidth 56-11

56.2.13 mls qos map ip-prec-dscp 56-12
56.2.14 wrr-queue bandwidth 56-13
56.2.15 wrf-queue-sp 56-14
56.2.16 virtual-group 56-15
56.3 Showing Related Command 56-16
56.3.1 show class-map 56-16
56.3.2 show policy-map 56-16
56.3.3 show mls qos interface 56-17
56.3.4 show mls qos virtual-group 56-17
56.3.5 show mls qos queuing 56-18
56.3.6 show mls qos scheduler 56-18
56.3.7 show mls qos maps 56-18
56.3.8 show mls qos rate-limit 56-19
56.3.9 show virtual-group 56-19
57 VRRP Configuration Commands 57-20
57.1 Configuration Related Commands 57-20
57.1.1 vrrp authentication 57-20
57.1.2 vrrp delay 57-21
57.1.3 vrrp description 57-22
57.1.4 vrrp ip 57-23
57.1.5 vrrp preempt 57-24
57.1.6 vrrp priority 57-25
57.1.7 vrrp timers advertise 57-26
57.1.8 vrrp timers learn 57-27
57.1.9 vrrp track 57-28
57.2 VRRP Monitoring and Maintenance Commands 57-30
57.2.1 debug vrrp 57-30
57.2.2 debug vrrp errors 57-31
57.2.3 debug vrrp events 57-32
57.2.4 debug vrrp packets 57-32
57.2.5 debug vrrp state 57-33
57.3 Showing Related Command 57-33
57.3.1 show vrrp 57-33
57.3.2 show vrrp interface 57-35
58 RERP Configuration Commands 58-1
58.1 Related Configuration Commands 58-1
58.1.1 rerp enable 58-1
58.1.2 rerp hello-interval 58-2

58.1.3 rerp fail-interval 58-3
58.1.4 rerp region 58-3
58.1.5 ring 58-4
58.1.6 edge-ring 58-5
58.1.7 major-ring 58-6
58.2 Showing and Monitoring Commands 58-6
58.2.1 show rerp 58-7
58.2.2 show rerp statistics 58-7
58.2.3 clear rerp statistics 58-8
58.2.4 debug rerp 58-8

59 REUP Configuration Commands 59-1
59.1 Related Configuration Commands 59-1
59.1.1 switchport backup interface *interface-id* 59-1
59.1.2 switchport backup interface *interface-id* preemption 59-2
59.1.3 mac-aadress-table move update receive 59-3
59.1.4 mac-address-table move update transit 59-4
59.1.5 mac-address-table update group 59-4
59.2 Showing and Monitoring Commands 59-5
59.2.1 show interfaces [*interface-id*] switchport backup [detail] 59-5
59.2.2 show mac-address-table update group [detail] 59-6

60 RLDP Configuration Command 60-1
60.1 Configuration Related Commands 60-1
60.1.1 rldp enable 60-1
60.1.2 rldp detect-interval 60-2
60.1.3 rldp detect-max 60-3
60.1.4 rldp port 60-3
60.1.5 rldp reset 60-4
60.2 Showing and Monitoring Commands 60-5
60.2.1 show rldp 60-5
60.2.2 debug rldp 60-5

61 TPP Configuration Commands 61-1
61.1 Configuration Related Commands 61-1
61.1.1 topology guard 61-1
61.1.2 tp-guard port enable 61-2
61.2 Showing Related Commands 61-2
61.2.1 show tpp 61-2

62 Supervisor Engine Redundancy Configuration Commands 62-1

62.1 Related Configuration Commands 62-1
62.1.1 redundancy 62-1
62.1.2 auto-sync 62-2
62.1.3 auto-sync time-period 62-3
62.1.4 switchover timeout 62-4
62.1.5 redundancy reload 62-4
62.1.6 redundancy forceswitch 62-5
62.2 Showing and Monitoring Commands 62-6
62.2.1 show redundancy states 62-6
62.2.2 show redundancy auto-sync 62-6
62.2.3 show redundancy switchtimeout 62-7

63 File System Configuration Commands 63-1
63.1 Configuration Related Commands 63-1
63.1.1 cd 63-1
63.1.2 cp 63-2
63.1.3 ls 63-3
63.1.4 makefs 63-3
63.1.5 mkdir 63-4
63.1.6 mv 63-5
63.1.7 pwd 63-5
63.1.8 rm 63-6
63.1.9 rmdir 63-6

64 Memory Configuration Commands 64-1
64.1 Showing Commands 64-1
64.1.1 show memory 64-1
64.1.2 memory-lack exit-policy 64-2
64.1.3 show memory protocols 64-3

65 CPU-LOG Configuration Commands 65-1
65.1 Related System Management commands 65-1
65.1.1 show cpu 65-1
65.1.2 cpu-log 65-5

66 Syslog Configuration Commands 66-1
66.1 Related Configuration Commands 66-1
66.1.1 logging on 66-1
66.1.2 terminal monitor 66-2
66.1.3 logging buffered 66-2
66.1.4 Logging server 66-4

66.1.5 logging file flash 66-5
66.1.6 logging console 66-6
66.1.7 logging monitor 66-7
66.1.8 logging trap 66-8
66.1.9 logging source interface 66-9
66.1.10 logging source ip| ipv6 66-10
66.1.11 logging facility 66-11
66.1.12 logging count 66-12
66.1.13 logging rate-limit 66-13
66.1.14 logging synchronous 66-14
66.1.15 service sequence-numbers 66-15
66.1.16 service timestamps 66-16
66.1.17 service sysname 66-17
66.1.18 more flash 66-18
66.1.19 clear logging 66-19
66.2 Showing Related Command 66-19
66.2.1 show logging 66-19
66.2.2 show logging count 66-21
67 Module Hot-plugging/ unplugging Configuration Commands 67-1
67.1 Related Configuration Commands 67-1
67.1.1 install slot-num moduletype 67-1
67.1.2 no install slot-num 67-2
67.1.3 remove configuration module slot-num 67-3
67.1.4 reset module slot-num 67-4
67.2 Showing Related Command 67-4
67.2.1 show version module detail [module-num] 67-4
67.2.2 show version slots [slot-num] 67-5
68 LCD Configuration Commands 68-1
68.1 Related Configuration Commands 68-1
68.1.1 lcd trap-number num 68-1
68.1.2 memory-rate rising-threshold num 68-2
69 USB configuration Commands 69-1
69.1 Related Configuration Commands 69-1
69.1.1 show usb 69-1
69.1.2 usb remove 69-2
70 POE Management Configuration Commands 70-3
70.1 Configurtion Related Command 70-3

70.1.1 poe enable 70-3
70.1.2 poe-power lower lower 70-3
70.1.3 poe-power upeer upper 70-4
70.1.4 poe disconnect-mode mode 70-5
70.2 Show Related Command 70-5
70.2.1 show poe interfaces 70-5
70.2.2 show poe powersupply 70-6

1 CLI Authorization Configuration Commands

1.1 alias

You can use the **alias** command to configure an alias of a command in the global configuration mode. Use the **no** form of the command to remove the alias of a specified command or all the aliases under one mode.

alias *mode command-alias original-command*

no alias *mode* [*command-alias*]

Parameter description

Parameter	Description
mode	Mode of the command represented by the alias
command-alias	Alias of the command
original-command	Syntax of the command represented by the alias

Default Settings

Some commands in the privileged EXEC mode have default alias names.

Command mode

Global configuration mode.

Usage guidelines

The following table lists the default alias of the commands in the privileged EXEC mode.

Alias	Actual Command
h	**help**
p	**ping**
s	**show**

u	**undebug**
un	**undebug**

The default alias cannot be deleted by the **no alias exec** command.

By setting the alias, you can use a word to replace a command. For example, you can create an alias to represent the first part of a command, and then type the rest part of the command.

The mode of the command represented by the alias is the command mode existing in the current system. In the global configuration mode, you can use **alias ?** to list all the modes under which you can configure alias for commands.

```
DES-7210(config)# alias ?
  aaa-gs              AAA server group mode
  acl                 acl configure mode
  bgp                 Configure bgp Protocol
  config              globle configure mode
.......
```

The alias also has its help information that is displayed after * in the following format:

**command-alias=original-command*

For example, in the privileged EXEC mode, the default alias **s** stands for **show**. You can enter **s?** to query the key words beginning with **s** and the help information of the alias.

```
DES-7210# s?
*s=show  show  start-chat  start-terminal-service
```

If an alias represents more than one word, the command will be displayed in brackets. For example, if you set **sv** stand for **show version** in the privileged EXEC mode, then:

```
DES-7210# s?
*s=show  *sv="show version" show  start-chat
start-terminal-service
```

The alias must begin with the first letter of the command. The first letter of the command cannot be a space. The space before the command cannot be used as a valid alias.

```
DES-7210# s?
show  start-chat  start-terminal-service
```

The command alias also has its help information. For example, if the alias **ia** represents **ip address** in the interface configuration mode, then:

```
DES-7210(config-if)# ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
DES-7210(config-if)# ip address
```

The above help information lists the parameters of **ip address** and shows the actual command name.

You must enter an entire alias; otherwise it cannot be recognized.

Use the **show aliases** command to show the aliases setting in the system.

Examples

In the global configuration mode, use **def-route** to represent the default route setting of **ip route 0.0.0.0 0.0.0.0 192.168.1.1:**

```
DES-7210# configure terminal
DES-7210(config)# alias config def-route ip route 0.0.0.0 0.0.0.0
192.168.1.1
DES-7210(config)# def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
DES-7210(config)# def-route?
% Unrecognized command.
DES-7210(config)# end
DES-7210# show aliases config
globle configure mode alias:
def-route          ip route 0.0.0.0 0.0.0.0
192.168.1.1
```

Related commands

Command	Description
show aliases	Show the aliases settings.

1.2 privilege

To attribute the execution rights of a command to a command level, use **privilege** in the global configuration mode. The **no** form of this command recovers the execution rights of a command to the default setting.

privilege *mode* [**all**] [**level** *level* **| reset**] *command-string*

no privilege *mode* [**all**] [**level** *level*] *command-string*

Parameter description

Parameter	Description
mode	CLI mode of the command to which the execution rights are attributed.
all	Alias of the command
level	Specify the execution right levels (0–15) of a command or sub-commands
reset	Restore the command execution rights to its default level
command-string:	Command string to be authorized

Default Settings

N/A.

Command mode

Global configuration mode.

Usage guidelines

The following table lists some key words that can be authorized by command **privilege** in the CLI mode. The number of command modes that can be authorized may vary with different devices. In the global configuration mode, you can use **privilege ?** to list all CLI command modes that can be authorized.

Mode	Descripton
config	Global configuration mode.
exec	Privileged EXEC mode
interface	Interface configuration mode
ip-dhcp-pool	DHCP address pool configuration mo
keychain	KeyChain configuration mode
keychain-key	KeyChain-key configuration mode
time-range	Time-Range configuration mode

Examples

Set the password of CLI level 1 as **test** and attribute the **reload** rights to reset the device:

```
DES-7210(config)# enable secret level 1 0 test
DES-7210(config)# privilege exec level 1 reload
```

After the above setting, you can access the CLI window as level-1

user to use the **reload** command：

```
DES-7210> reload ?
  <cr>
```

You can use the key word **all** to attribute all sub-commands of reload to level-1 users:

```
DES-7210(config)# privilege exec all level 1 reload
```

After the above setting, you can access the CLI window as level-1 user to use all sub commands of the **reload** command:

```
DES-7210> reload ?
at                  reload at a specific time/date
cancel              cancel pending reload scheme
in                  reload after a time interval
<cr>
```

Related commands

Command	Description
enable secret	Set CLI-level password

1.3 show aliases

To display all the command aliases or aliases in special command modes, run the **show aliases** command in the privileged EXEC mode.

show aliases [*mode***]**

Parameter description

Parameter	Description
mode	Mode of the command represented by the alias.

Default Settings

N/A.

Command mode

EXEC mode.

Usage guidelines

Show all the configuration of aliases if the command mode has not been input.

Examples

Following example shows the command alias in the EXEC mode:

```
DES-7210# show aliases exec
exec mode alias:
```

```
h                help
p                ping
s                show
u                undebug
un               undebug
```

Related commands

Command	Description
alias	Set the alias of a command.

2 Switch Management Configuration Commands

2.1 User Management Related Commands

The user interface is the user command line interface (CLI), including the following related commands:

- **disable**
- **enable**
- **enable password**
- **enable secret**
- **service password-encryption**
- **password**
- **login**
- **login local**
- **login authentication**
- **username**
- **lock**
- **lockable**
- **telnet**
- **enable service**

2.1.1 disable

To exit from privileged user mode to normal user mode or lower the privilege level, execute the privileged user command **disable**.

disable [*privilege-level*]

Parameter description

Parameter	Description
privilege-level	Privilege level

Command mode	Privileged mode.
Usage guidelines	Use this command to return to user mode from privileged mode. If a privilege level is added, the current privilege level will be lowered to the specified level.  **Note** The privilege level following the **disable** command must be lower than the current level.
Examples	The example below lowers the current privilege level of the device down to level 10: `DES-7210# disable 10`

Related commands	**Command**	**Description**
	enable	From user mode enter to the privileged mode or log on the higher level of authority.

2.1.2 enable

To enter into the privileged user mode, execute the normal user configuration command **enable**.

For the details of the command, see the *Security Configuration Command Reference*.

2.1.3 enable password

To configure the password for different privilege level, execute the global configuration command **enable password**. The **no** form of this command is used to delete the password of the specified level.

enable password [**level** *level*] {*password* | [**0**|**7**] *encrypted-password*}

no enable password

Parameter description	**Parameter**	**Description**
	Password	Password for user to enter into the EXEC configuration layer
	Level	User's level.
	0|7	Password encryption type, "0" for no encryption, "7" for simple encryption

encrypted-password	Password text.

Command mode

Global configuration mode.

Usage guidelines

No encryption is required in general. The encryption type is required generally when the password that has been encrypted with the command for the device are to be copies and pasted.

The effective password is defined as below:

- Consists of 1 ~ 26 letter in upeer/lower case and numerals
- Leading spaces are allowed but ignored. Spaces in between or at the end are regarded as part of the password.

Caution

If an encryption type is specified and then a plaintext password is entered, it is impossible to enter into the privileged EXEC mode. A lost password that has been encrypted with any method cannot be restored. The only way is to reconfigure the device password.

Examples

The example below configures the password as **pw10**:

```
DES-7210(config)# enable password pw10
```

Related commands

Command	Description
enable secret	Set the security password

2.1.4 enable secret

To configure the security password for different privilege level, execute the global configuration command **enable secret**. The **no** form of this command is used to delete the password of the specified level.

enable secret [**level** *level*] {*secret* | [**0|5**] *encrypted-secret*}

no enable secret

Parameter description

Parameter	Description
secret	Password for user to enter into the EXEC configuration layer
level	User's level.
0|5	Password encryption type, "0" for no encryption, "5" for security encryption

encrypted-password	Password text

Command mode

Global configuration mode.

Usage guidelines

The password falls into "password" and "security" passwords. The "password" is simple encryption password, which can be set only for level 15. The "security" means the security encryption password, which can be set for level 0 ~ 15. If the two kinds of passwords exist in the system at the same time, the "password" type password will not take effect. If a "password" type password is set for a level other than 15, an alert is provided and the password is automatically converted into the "security" password. If "password" type password is set for level 15 and the same as the "security" password, an alert is provided. The password must be saved in encrypted manner, with simple encryption for the "password" type password and security encryption for the "security" type password.

Examples

The example below configures the security password as pw10:

```
DES-7210(config)# enable secret 0 pw10
```

Related commands

Command	Description
enable password	Set passwords for different privilege levels.

2.1.5 service password-encryption

To encrypt the password, execute this command. The **no** form of this command restores to the default value, but the password in cipher text cannot be restored to plain text.

service password-encryption

no service password-encryption

Parameter description

N/A.

Command mode

Global configuration mode.

Usage guidelines	This command is disabled by default. Various passwords are displayed in form of plain text, unless it is directly configured in cipher text form. After you execute the **service password-encryption** and **show running** or **write** command to save the configuration, the password transforms into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.
Examples	The example below encrypts the password: `DES-7210(config)# service password-encryption`

Related commands

Command	Description
enable password	Set passwords of different privileges.

2.1.6 password

To configure the password for line logon, execute the line configuration command **password**. The **no** form of this command is used to delete the line logon password.

password {*password* | [**0**|**7**] *encrypted-password*}

no password

Parameter description

Parameter	Description
password	Password for line of remote user
0|7	Password encryption type, "0" for no encryption, "7" for simple encryption
encrypted-password	Password text

Command mode	Line configuration mode.
Usage guidelines	This command is used to configure the authentication password for the line logon of remote user.

Examples	The example below configures the line logon password as "red":
	`DES-7210(config)# line vty 0`
	`DES-7210(config-line)# password red`

Related

Command	Description

commands	**login**	From user mode enter to the privileged mode or log on the higher level of authority.

2.1.7 login

In case the AAA is disabled, to enable simple logon password authentication on the interface, execute the interface configuration command **login**. The **no** form of this command is used to delete the line logon password authentication.

login

no login

Parameter description	N/A.
Command mode	Line configuration mode.
Usage guidelines	If the AAA security server is not enabled, this command is used for the simple password authentication at logon. The password here is the one configured for VTY or console interface.

Examples	The example below shows how to set the logon password authentication on VTY.
	`DES-7210(config)# no aaa new-model`
	`DES-7210(config)# line vty 0`
	`DES-7210(config-line)# password 0 normatest`
	`DES-7210(config-line)# login`

Related commands	Command	Description
	password	Configure the line logon password

2.1.8 login local

In case the AAA is disabled, to enable local user authentication on the interface, execute the interface configuration command **login local**. The **no** form of this command is used to delete the line local user authentication.

login local

no login local

Parameter description	N/A.
Command mode	Line configuration mode.
Usage guidelines	If the AAA security server is not enabled, this command is used for the local user authentication at logon. The user here means the one configured with the **username** command.

Examples	The example below shows how to set the local user authentication on VTY.
	`DES-7210(config)# no aaa new-model`
	`DES-7210(config)# username test password 0 test`
	`DES-7210(config)# line vty 0`
	`DES-7210(config-line)# login local`

Related commands

Command	Description
username	Configure the local user information.

2.1.9 login authentication

In case the AAA is enabled, the authentication with the AAA server must be performed for logon. Use this command to associate logon authentication method list. The **no** form of this command is used to delete the logon authentication method list.

login authentication {**default** | *list-name*}

no login authentication {**default** | *list-name*}

Parameter description

Parameter	Description
default	Name of the default authentication method list
list-name	Name of the method list available

Command mode	Line configuration mode.
Usage guidelines	If the AAA security server is enabled, this command is used for the logon authentication with the specified method list.

Examples

The example below shows how to associate method list on VTY and perform logon authentication with radius.

```
DES-7210(config)# aaa new-model
DES-7210(config)# aaa authentication login default radius
DES-7210(config)# line vty 0
DES-7210(config-line)# login authentication default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service
aaa authentication login	Configure the logon authentication method list

2.1.10 username

To set the local username, execute the global configuration mode command **username**.

username *name* {**nopassword** | **password** { *password* | [**0|7**]

encrypted-password }} **username** *name* **privilege** *privilege-level*

no username *name*

Parameter description

Parameter	Description
name	Username
password	User password
0|7	Password encryption type, 0 for no encryption, 7 for simple encryption
encrypted-password	Password text
privilege-level	User bound privilege level

Command mode

Global configuration mode.

Usage guidelines

This command is used to establish local user database for the purpose of authentication.

Note

If the type of encryption is specified as 7, the length of the entered legal cipher text should be even.

In general, it is not necessary to specify the type of encryption as 7.

Commonly, it is necessary to specify the type of encryption as 7 only when the encrypted password is copied and pasted.

Examples	The example below configures a username and password and bind the user to level 15. `DES-7210(config)# username test privilege 15 password 0 pw15`

Related commands	**Command**	**Description**
	login local	Enable local authentication

2.1.11 lock

To set a temporary password at the terminal, execute the EXEC mode command **lock**.

lock

Parameter description	N/A.
Command mode	Privileged mode.
Usage guidelines	You can lock the terminal interface but maintain the continuity of session, to prevent it from being accessed by setting the temporary password.The terminal interface can be locked by the steps below: 1. Enter the **lock** command, and the system will prompt you to enter the password: 2. Enter the password, which may be any string.The system will prompt you to confirm the entered password, and then clear the screen as well as show the "Locked" information. 3. To enter into the terminal, enter the set temporary password. To use the terminal locked function at the terminal, execute the **lockable** command in the line configuration mode, and enable the characteristic to support the terminal lock in corresponding line.

Examples

The example below locks a terminal interface:

```
DES-7210(config-line)# lockable
DES-7210(config-line)# end
DES-7210# lock
Password: <password>
Again: <password>

Locked
Password: <password>
DES-7210#
```

Related commands

Command	Description
lockable	Set to support the terminal lock function in the line.

2.1.12 lockable

To support the use of the **lock** command at the terminal, execute the **lockable** command in the line configuration mode. The terminal doesn't support the **lock** command, by default.Use the **no** command to cancel the setting.

lockable

no lockable

Parameter description

N/A.

Command mode

Line configuration mode.

Usage guidelines

This command is used to support the terminal lock function in corresponding line. To lock the terminal, execute the **lock** command in the EXEC mode.

Examples

The example below enables the terminal lock function at the console port and locks the console:

```
DES-7210(config)# line console 0
DES-7210(config-line)# lockable
DES-7210(config-line)# end
DES-7210# lock
Password: <password>
Again: <password>
```

```
Locked

Password: <password>
DES-7210#
```

Related commands

Command	Description
lock	Lock the terminal.

2.1.13 telnet

To log in one server which supports the telnet connection, use the **telnet** command to log on in the EXEC (privileged) mode.

telnet *host* [*port*] [*keyword*]

Parameter description

Parameter	Description
Host	The IP address of host or host name to be logged in.
Port	Select the TCP port number to be used for the login, 23 by default.
Keyword	The available keywords are listed in the table below:

Keyword	Description
/source-interface	Specify the interface from which the telnet connection request is sent.

Command mode

Privileged mode.

Usage guidelines

This command is used to log in a telnet server.

Examples

The example below commands telnet to 192.168.1.11, the port uses the default value, and the source interface is specified as vlan 1, the queried VRF route table is specified as vpn1.

```
DES-7210# telnet 192.168.1.11 /source-interface vlan 1 /vrf vpn1
```

Related commands

Command	Description
show sessions	Show the currently established sessions.
exit	Exit current connection.

2.1.14 enable service

To enable or disable the specified service such as **SSH Server/Telnet Server/Web Server/SNMP Agent**, use the **enable service** command in the global configuration mode:

enable service { **ssh-sesrver** | **telnet-server** | **web-server** | **snmp-agent**}

Parameter description

Keyword	Description
ssh-sesrver	Enable and disable SSH Server.
telnet-server	Enable and disable Telnet Server.
web-server	Enable and disable HTTP Server.
snmp-agent	Enable and disable SNMP Agent.

Command mode

Global configuration mode.

Usage guidelines

This command is used to enable the specified service. Use the **no enable service** command to disable the specified service.

Examples

Following Example:

Enable the SSH Server, Enable the function of SSH Server:

```
DES-7210(Config)# enable service ssh-sesrver
```

Related commands

Command	Description
show service	View the service status of the current system.

2.2 Basic System Management Related Commands

The system management includes related commands as follows:

- **clock set**
- **clock update-calendar**
- **exec-timeout**
- **hostname**
- **session-timeout**
- **show clock**
- **show running-config**
- **show startup-config**

- **reload**
- **show reload**
- **prompt**
- **banner motd**
- **banner login**
- **speed**
- **show line**
- **write**

2.2.1 clock set

To configure system clock manually, execute one of the two formats of the privileged user command **clock set**:

clock set *hh:mm:ss month day year*

Parameter description

Parameter	Description
hh:mm:ss	Current time, in the format of Hour (24-hour): Minute: Second
day	Date (1-31) of month
month	Month (1-12) OF year
year	Year (1993-2035), abbreviation is not allowed.

Command mode

Privileged mode.

Usage guidelines

Use this command to set the system time to facilitate the management.

For devices without hardware clock, the time set by the **clock set** command takes effect for only the current setting. Once the device powers off, the manually set time becomes invalid.

Examples

The example below configures the current time as 10:20:30AM March 17th 2003.

```
DES-7210# clock set 10:20:30 Mar 17 2003
DES-7210# show clock
clock: 2003-3-17 10:20:32
```

Related

Command	Description

commands	**show clock**	Show current clock.

2.2.2 clock update-calendar

In the privileged EXEC mode, you can execute command **clock update-calendar** to overwrite the value of hardware clock by software clock.

clock update-calendar

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Some platforms use hardware clock to complement software clock. Since battery enables hardware clock to run continuously, even though the device is closed or restarts, hardware clock still runs. If hardware clock and software clock are asynchronous, then software clock is more accurate. Execute clock update-calendar command to copy date and time of software clock to hardware clock.
Examples	The example below copys the current time and date of software clock to hardware clock: `DES-7210# clock update-calendar`

Related commands

Command	Description
clock read-calendar	Set the softwar clock with the hardware clock value.

2.2.3 exec-timeout

To configure the connection timeout to this equipment in the LINE, use the **exec-timeout** command.Once the connection timeout in the LINE is cancelled by the **no exec-timeout** command, the connection will never be timeout.

exec-timeout *minutes [seconds]*

no exec-timeout

Parameter description

Parameter	Description
minutes	The minutes of specified timeout.
seconds	(optional parameter) The seconds of specified timeout.

Default configuration

The default timeout is 10min.

Command mode

Line configuration mode.

Usage guidelines

If there is no input/output information for this connection within specified time, this connection will be interrupted, and this LINE will be restored to the free status.

Examples

The example below specifies the connection timeout is 5’30“.

```
DES-7210(config-line)#exec-timeout 5 30
```

2.2.4 hostname

To specify or modify the hostname of the device, execute the global configuration command **hostname**.

hostname *name*

Parameter description

Parameter	Description
name	Device hostname, the string, numeral or hyphen are supported only. The maximum length is 63 characters.

Default configuration

The default hostname is DES-7210.

Command mode

Global Configuration Mode.

Usage guidelines	This hostname is mainly used to identify the device and is taken as the username for the local device in the dialup and CHAP authentication.

Examples	The example below configures the hostname of the device as D-Link:
	`DES-7210(config)# hostname D-Link`
	`D-Link(config)#`

2.2.5 session-timeout

To configure the session timeout for the remote terminal established in current LINE, use the **session-timeout** command.When the session timeout for the remote terminal in the LINE is cancelled, the session will never be timeout.

session-timeout *minutes [seconds]*

no session-timeout

Parameter description

Parameter	Description
minutes	The minutes of specified timeout.
seconds	(Optional Parameter) The seconds of specified timeout.

Default configuration	The default timeout is 0 min.
Command mode	LINE configuration mode.
Usage guidelines	If there is no input/output information for the session to the remote terminal established in current LINE within specified time, this connection will be interrupted, and this LINE will be restored to the free status.
Examples	The example below specifies the timeout of session is 5 min plus 30 second. `DES-7210(config-line)#exec-timeout 5 30`

2.2.6 show clock

To view the system time, execute the privileged user command **show clock**.

show clock [**detail**]

Parameter description

Parameter	Description
detail	Show the source of system clock.

Command mode

Privileged mode

Usage guidelines

This command is used to view current system clock, the **detail** option will show the source of the system clock.

Examples

The example below is an execution result of the **show clock** command:

```
DES-7210# show clock detail
clock: 2003-3-17 10:27:21
Clock read from calendar when system boot.
```

Related commands

Command	Description
clock set	Set the system clock.

2.2.7 show running-config

To show the configuration information current device system is running, execute the privileged user command **show running-config**.

show running-config

Command mode

Privileged mode.

2.2.8 show startup-config

To view the configuration of device stored in the Non Volatile Random Access Memory (NVRAM), execute the privileged user command **show startup-config**.

show startup-config

Command mode

Privileged mode.

Usage guidelines

The configuration of device stored in the NVRAM is that executed when the device is startup.

2.2.9 reload

To restart the device system, execute the privileged user command **reload**.

reload [*text* | **in** *mmm* | *hhh:mm* [*text*] | **at** *hh:mm* [*month day year*] [*text*] | **cancel**]

Parameter description

Parameter	Description
text	Cause to restart, 1-255 bytes
in *mmm hh:mm*	The system is restarted after specified time interval.
at *hh:mm month day year*	The system is restarted at the specified time. Up to 200 days is supported
month	Month in the range January to December
day	Date in the range 1 to 31
year	Year in the range 1993 to 2035
cancel	Cancel scheduled restart.

Command mode

Privileged mode.

Usage guidelines

This command is used to restart the device at specified time, which may facilitate the management.

Examples

The example below specifies to restart the system in 10 minutes:

```
DES-7210# reload in 10
Device will reload in 600 seconds.
```

2.2.10 show reload

To show the restart settings of the system, execute the **show reload** command in the privileged EXEC mode.

show reload

Parameter description

N/A.

Command mode

Privileged mode.

Usage guidelines	Use this command to show the restart settings of the system.

Examples	The following example shows the restart settings of the system:
	`DES-7210# show reload`
	`Reload scheduled in 595 seconds.`
	`At 2003-12-29 11:37:42`
	`Reload reason: test.`

2.2.11 prompt

To set the **prompt** command, run the **prompt** command in the global configuration mode. To delete the prompt setting, run the **no prompt** command.

prompt string

Parameter description

Parameter	Description
string	Character string of the **prompt** command. The maximum length is 32 letters.

Command mode	Global configuration mode.
Usage guidelines	If you have not set the prompt string, the prompt string is the system name, which varies with the system name. The **prompt** command is valid only in the EXEC mode.

Examples	Set the prompt string to D-Link:
	`DES-7210(config)# prompt D-Link`
	`DES-7210(config)# end`
	`D-Link`

2.2.12 banner motd

To set the Message-of-the-Day (MOTD), run the **banner motd** command in the global configuration mode. To delete the MOTD setting, run the **no banner motd** command.

banner motd *c message c*

Parameter description

Parameter	Description
c	Separator of the MOTD. Delimiters are not allowed in the MOTD.
message	Contents of an MOTD

Command mode	Global configuration mode.
Usage guidelines	This command sets the MOTD, which is displayed upon login. The letters entered after the separator will be discarded.

Examples	The following example shows the configuration of MOTD:
	`DES-7210(config)`
	`DES-7210(config)# banner motd $ hello,world $`

2.2.13 banner login

To configure the login banner, execute the **banner login** command in the global configuration mode. You can use the **no banner login** command to remove the configuration.

banner login *c message c*

Parameter description

Parameter	Description
c	Separator of the message of logging banner. Delimiters are not allowed in the MOTD.
message	Contents of login banner

Command mode	Global configuration mode.
Usage guidelines	This command sets the logging banner message, which is displayed upon login. All characters behind the terminating symbol will be discarded by the system.

Examples	The following example shows the configuration of logging banner:
	`DES-7210(config)`
	`DES-7210(config)# banner login $ enter your password $`

2.2.14 speed

To set speed at which the terminal transmits packets, execute the **speed** *speed* command in the line configuration mode. To restore the speed to its default value, run the **no speed** command.

speed *speed*

Parameter description

Parameter	Description
speed	Transmission rate (bps) on the terminal. For serial ports, the optional rates are 9600, 19200, 38400, 57600, and 115200 bps. The default rate is 9600 bps.

Command mode

Global configuration mode.

Default Configuration

The default rate is 9600.

Usage guidelines

This command sets the speed at which the terminal transmits packets.

Examples

The following example shows how to configure the rate of the serial port to 57600 bps:

```
DES-7210(config)#
DES-7210(config)# line console 0
DES-7210(config-line)# speed 57600
DES-7210(config-line)#
```

2.2.15 show line

To show the configuration of a line, execute the **show line** command in the privileged mode.

show line [**console** *line-num* | **vty** *line-num* **|** *line-num*]

Parameter description

Parameter	Description
console	Show the configuration of a console line.
vty	Show the configuration of a vty line.
line-num	Number of the line

Command mode

Privileged mode.

Usage guidelines

This command shows the configuration information of a line.

Examples

The following example shows the configuration of console port:

```
DES-7210# show line console 0
CON     Type    speed   Overruns
* 0     CON     9600    45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
             ^^x     none       ^M
Timeouts:      Idle EXEC    Idle Session
             never       never
History is enabled, history size is 10.
Total input: 53564 bytes
Total output:  395756 bytes
Data overflow:  27697 bytes
stop rx interrupt:  0 times
```

2.2.16 write

To perform the read/write operation for the device configurations (startup configuration or system configuration), execute the privileged user command **write**.

write [**memory | network | terminal**]

Parameter description

Parameter	Description
memory	Write the system configuration (running-config) into NVRAM, which is equivalent to **copy running-config startup-config**.
network	Save the system configuration into the TFTP server, which is equivalent to **copy running-config tftp**.
terminal	Show the system configuration, which is equivalent to **show running-config**.

Command mode

Privileged mode.

Usage guidelines

Despite of the alternative command, these commands have been widely used and accepted, so they are reserved to facilitate user's operation.

The **no** form with the command is equivalent to add the **memory** operation.

Examples

The example below saves the device configuration:

```
DES-7210# write
```

```
Building configuration...
[OK]
```

Related commands

Command	Description
show running-config	View the system configuration.
copy	Copy the device configuration files.

3 LINE Configuration Commands

3.1 Configuration Related Commands

3.1.1 line

To enter the specified LINE mode, use the following command:

line [**aux | console | tty |vty**] *first-line* [*last-line*]

Parameter description	**Parameter**	**Description**
	aux	Auxiliary port, on the routers.
	console	Console port
	tty	Asynchronous port, on the routers.
	vty	Virtual terminal line, applicable for telnet/ssh connection.
	first-line	Number of first-line to enter
	last-line	Number of last-line to enter

Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	Access to the specified LINE mode.
Examples	Enter the LINE mode from LINE VTY 1 to 3: `DES-7210(config)# line vty 1 3`

Related commands	N/A.

3.1.2 line vty

This command can be used to increase the number of VTY connections currently available. The number of currently available VTY connections can be decreased by using the **no** form of this command.

line vty *line-number*

no line vty *line-number*

Default configuration	By default, there are five available VTY connections, numbered 0--4.
Command mode	Global configuration mode.
Usage guidelines	When you need to increase or decrease the number of available VTY connections, use the above commands.

Examples	Increase the number of available VTY connections to 20. The available VTY connections are numbered 0--19.
	`DES-7210(config)# line vty 19`
	Decrease the number of available VTY connections to 10. The available VTY connections are numbered 0-9.
	`DES-7210(config)# line vty 10`

Related commands	N/A.

3.1.3 transport input

To set the specified protocol under Line that can be used for communication, use the **transport input** command. Use **default transport input** to restore the protocols under Line that can be used for communication to the default value.

transport input {all | ssh | telnet | none}

default transport input

Parameter description

Parameter	Description
all	Allow all the protocols under Line to be used for communication
ssh	Allow only the SSH protocol under Line to be used for communication
telnet	Allow only the Telnet protocol under Line to be used for communication
none	Allow none of protocols under Line to be used for communication

Default configuration

By default, VTY allows all the protocols to be used for communication. The default value of other types of TTYs is NONE, indicating that no protocols are allowed for communication. After some protocols are set to be available for communication, use the **default transport input** command to restore the setting to the default value.

Command mode

Line configuration mode.

Usage guidelines

This command is used to set the protocols in the Line mode that are available for communication. By default, VTY allows all the protocols for communication. After protocols available for communication are set, only these protocols can connect on the specific VTY successfully. Use the **show running** command to view configuration information under Line.

Note: You can restore the default configuration by using the **default transport input** command. The **no transport input** command is used to disable all the communication protocols in the LINE mode. The setting result is the same as that of **transport input none**.

Examples

Specify that only the Telnet protocol is allowed to login in line vty 0 4:

```
DES-7210# configure terminal
DES-7210(config)# line vty 0 4
DES-7210(config-line)# transport input telnet
```

Related commands

Command	Description
show running	Show status information

Version description	The software version must be later than R10.1.

3.1.4 access-class

Set the applied ACL (Access Control List) in Line. Use the **access-class** *acl-no* **{ in | out }** command to configure the ACL in Line. Use the no **access-class** *access-list-number* {**in | out}** command to cancel the ACL configuration in LINE.

[no] access-class *access-list-number* **{in | out}**

Parameter description

Parameter	Description
access-list-number	Specify the ACL defined by access-list
in	Perform access control over the incoming connections
out	Perform access control over the outgoing connections

Default configuration	By default, no ACL is configured under Line. All connections are accepted, and all outgoing connections are allowed.
Command mode	Line configuration mode.
Usage guidelines	This command is used to configure ACLs under Line. By default, all the incoming and outgoing connections are allowed, and no connection is filtered. After **access-class** is configured, only the connections that pass access list filtering can be established successfully. Use the **show running** command to view configuration information under Line.

Examples	In line vty 0 4, configure access-list for the accepted connections to 10:
	`DES-7210# configure terminal`
	`DES-7210(config)# line vty 0 4`
	`DES-7210(config-line)# access-class 10 in`

Related commands

Command	Description
show running	Show status information

Version description	The software version must be later than R10.1.

4 Upgrade and Maintenance Configuration Commands

4.1 Configuration Related Commands

The following describes how to upgrade and maintain by using the COPY command in the CLI environment of the main program.

- Upgrade and maintain by Xmodem protocol: **copy xmodem** command.
- Upgrade and maintain by Tftp protocol: **copy tftp** command.

4.1.1 copy xmodem

Upgrade and maintain by using the xmodem protocol or upload and download by using the xmodem protocol.

copy flash: *filename* **xmodem**

copy xmodem flash: *filename*

Parameter description

Parameter	Description
filename	The name of files in the equipment.

Default

N/A.

Command mode

Privileged mode.

Usage guidelines

If the file is transmitted successfully, show the length of the transmitted file; otherwise, show the failure information. Any files can be transmitted by TFTP, such as main program file and parameter file. The Xmodem can only be transmitted in the out-band (serial ports).

The following shows two examples: The first one transmits the files to the switch from the host via the xmodem protocol. The second uploads the configuration file in the switch to the host via the xmodem protocol.

Caution If there is a space in the file name, quotation mask is necessary, for example: **copy xmodeam flash**: “filename” or **copy flash**: ”filename” xmodem

Examples

The following is an example of upload and download:

```
DES-7210# copy xmodem flash: config.text
DES-7210# copy flash: config.text xmodem
```

Related commands N/A.

4.1.2 copy tftp

Upgrade and maintain by the tftp protocol or upload and download by the tftp protocol.

copy flash: *filename* **tftp**:*//location/filename*

copy tftp:*//location/filename* **flash**: *filename*

copy flash: *filename* **tftp**:*//location/filename* **vrf** *vrfname*

copy tftp:*//location/filename* **flash**: *filename* **vrf** *vrfname*

Parameter description

Parameter	Description
filename	File name
vrfname	VRF name

Default N/A.

Command mode Privileged user mode.

Usage guidelines If the file is transmitted successfully, show the length of the transmitted file. Otherwise, show the failure information. Any files can be transmitted by TFTP, such as main program file and parameter file. The TFTP transmission is carried out by the network port.

Caution If there is a space in the source file name, quotation mask is necessary for the TFTP link, for example:
copy tftp:”*//location/filename”* **flash**: *filename* **vrf** *vrfname*

	So does the destination file name, for example: **copy tftp:**//localtion/filename **flash:**"filename" **vrf** vrfname
Examples	The following is two examples: The first one transmits the backup parameter file (config.bak) from the local host (ip 192.168.12. 1) to the switch; The second one transmits the file (switch.bin) from the switch to the local switch (ip 192.168.12.1): DES-7210# **copy tftp:***//192.168.12.1/confg.bak* **flash:** *config.text* DES-7210# **copy flash:** *swhich.bin* **tftp:***//192.168.12.1/ Config.bak*
Related commands	N/A.

5 Network Connectivity Test Tool Configuration Commands

5.1 Configuration Related Commands

The network connectivity test tool configuration includes:

- **ping**
- **traceroute**
- **line-detect**

5.1.1 ping

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

ping [**vrf**] [*vrf-name*] [**ip**] [*ip-address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*]]

Parameter description

Parameter	Description
vrf-name	VRF name
ip-address	Specifies an IPv4 address.
length	Specifies the length of the packet to be sent.
times	Specifies the number of packets to be sent.
timeout	Specifies the timeout time.
data	Specifies the data to fill in.
source	Specifies the source IPv4 address.

Default

Five packets with 100Byte in length are sent to the specified IP address within specified time (2s by default).

Command mode

Privileged mode.

Usage guidelines

The ping command can be used in the ordinary user mode and the privileged mode. In the ordinary mode, only the basic functions of ping are available. In the privileged mode, in addition to the basic functions, the extension functions of the ping are also available. For the ordinary functions of ping, five packets of 100Byte in length are sent to the specified IP address within the specified period (2s by default). If response is received, '!' is displayed. If no response is received, '.' displayed, and the statistics is displayed at the end. For the extension functions of ping, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Examples

The example below shows the ordinary ping.

```
DES-7210# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout
is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 1/2/10 ms
```

The example below shows the extension ping.

```
DES-7210# ping 192.168.5.197 length 1500 ntimes 100
timeout 3
Sending 100, 1000-byte ICMP Echoes to 192.168.5.197,
timeout is 3 seconds, data ffff source 192.168.4.10:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip
min/avg/max = 2/2/3 ms
DES-7210#
```

Platform description

The command is supported by all equipments.

5.1.2 traceroute

Execute the traceroute command to show all gateways passed by the test packets from the source address to the destination address.

traceroute [**ip** *ip-address*][*ip-adress* [**probe** *number*] [**source** *source-address*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]

Parameter description

Parameter	Description
ip-address	Specifies an IPv4 address.
number	Specifies the number of probe packets to be sent.
source-address	specifies the source IPv4 address.
seconds	Specifies the timeout time.
minimum maximum	Specifies the minimum and maximum TTL values.

Command mode

Privileged mode.

Usage guidelines

Use the traceroute command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

Examples

The following is two examples of the application bout traceroute, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
DES-7210# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36

1     192.168.12.1        0 msec   0 msec   0 msec
2     192.168.9.2         4 msec   4 msec   4 msec
3     192.168.9.1         8 msec   8 msec   4 msec
4      192.168.0.10       4 msec   28 msec  12 msec
5      192.168.9.2        4 msec   4 msec   4 msec
6      202.101.143.154    12 msec  8 msec   24 msec
7      61.154.22.36       12 msec  8 msec   22 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
DES-7210# traceroute 202.108.37.42
```

```
  < press Ctrl+C to break >
Tracing the route to 202.108.37.42

1     192.168.12.1      0 msec    0 msec  0 msec
2     192.168.9.2       0 msec    4 msec  4 msec
3     192.168.110.1     16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129      12 msec   28 msec  12 msec
6     61.154.8.17       8 msec    12 msec  16 msec
7     61.154.8.250      12 msec   12 msec  12 msec
8     218.85.157.222    12 msec   12 msec  12 msec
9      218.85.157.130   16 msec   16 msec  16 msec
10     218.85.157.77    16 msec   48 msec  16 msec
11     202.97.40.65     76 msec   24 msec  24 msec
12     202.97.37.65     32 msec   24 msec  24 msec
13     202.97.38.162    52 msec   52 msec  224 msec
14     202.96.12.38     84 msec   52 msec  52 msec
15     202.106.192.226  88 msec   52 msec  52 msec
16     202.106.192.174    52 msec   52 msec  88 msec
17     210.74.176.158   100 msec  52 msec  84 msec
18     202.108.37.42    48 msec   48 msec  52 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) and the spent time are displayed, and gateway 4 fails.

```
DES-7210# traceroute www.ietf.org

Translating "www.ietf.org"...[OK]
  < press Ctrl+C to break >
Tracing the route to 64.170.98.32

 1     192.168.217.1      0 msec  0 msec  0 msec
 2     10.10.25.1         0 msec  0 msec  0 msec
 3     10.10.24.1         0 msec  0 msec  0 msec
 4     10.10.30.1         10 msec 0 msec  0 msec
 5     218.5.3.254        0 msec  0 msec  0 msec
 6     61.154.8.49        10 msec 0 msec  0 msec
 7     202.109.204.210    0 msec  0 msec  0 msec
 8     202.97.41.69       20 msec 10 msec 20 msec
 9     202.97.34.65       40 msec 40 msec 50 msec
 10    202.97.57.222      50 msec 40 msec 40 msec
 11    219.141.130.122    40 msec 50 msec 40 msec
 12    219.142.11.10      40 msec 50 msec 30 msec
 13    211.157.37.14      50 msec 40 msec 50 msec
 14    222.35.65.1        40 msec 50 msec 40 msec
 15    222.35.65.18       40 msec 40 msec 40 msec
 16    222.35.15.109      50 msec 50 msec 50 msec
 17    *      *      *
```

```
                18    64.170.98.32    40 msec 40 msec 40 msec
```

5.1.3 line-detect

To detect the line status, execute this command:

line-detect

Parameter description	N/A.
Default Configuration	N/A.
Command mode	Interface configuration mode.
Usage guidelines	This command is used to detect the line status and locate the problem in case of a line failure, for example, the line is torn down.

Examples

```
DES-7210(config)# int gigabitEthernet 3/1
DES-7210(config-if)# line-detect
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state     length(meters)
---- ---------- --------------
A      Ok          2
B      Ok          1
C      Short       1
D      Short       1
```

The command is described as follows:

Field	Description
pairs	Number of line pairs included. For example, the twisted pair includes four pairs of lines.
state	Status of the current line pair: OK, Short or Open. In general, the 100M twisted pairs A and B are OK, C and D are Short. The 1000M twisted pairs A, B, C and D are all OK.
length	Length of the line in meter. Only the length of the line pair whose status is OK takes effect. Since the length is calculated based on the transmission time of signal, there may have a certain difference. The length of the line pair whose status is Short or Open is the length from the port to the faulty point.

6 Interface Configuration Commands

6.1 Configuration Related Commands

Interface configuration includes the following commands:

- **interface aggregateport**
- **interface fastEthernet**
- **interface giagbitEthernet**
- **interface tenGigabitEthernet**
- **interface vlan**
- **medium-type**
- **description**
- **shutdown**
- **speed**
- **duplex**
- **flowcontrol**
- **mtu**
- **carrier-delay**
- **clear counters**
- **clear interface**
- **switchport**
- **switchport mode**
- **switchport access**
- **switchport trunk**
- **snmp trap link-status**

6.1.1 interface aggregateport

Use this command to access or create an aggregate port and enter interface configuration mode. Use the **no** form of the command to remove this port.

interface aggregateport *port-number*

Parameter description

Parameter	Description
port-number	Aggregate port number. Its range depends on the equipment and extended modules.

Command mode

Global configuration mode.

Usage guidelines

According to some rules, you can add other ports to an aggregate port. All the port members of an aggregate port are considered in a whole, and their attributes depend on the ones of the aggregate port. You can use **show interfaces** or **show interfaces aggregateport** commands to display the interface configuration.

Examples

```
DES-7210(config)#interface aggregateport 3
DES-7210(config-if)#
```

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description

The DES-7200 series supports up to 8 port members and create up to 128 AP globally.

6.1.2 interface fastEthernet

Use this command to select a Ethernet interface, and enter the interface configuration mode.

interface fastEthernet *mod-num/port-num*

Parameter description

Parameter	Description
mod-num/port-num	The range depends on the device and the extended module.

Command mode

Global configuration mode.

Usage guidelines	The **no** form of the command is not available, and this interface type cannot be deleted. Use **show interfaces** or **show interfaces fastEthernet** to display the interface configurations.
Examples	`DES-7210(config)# interface fastEthernet 1/2` `DES-7210(config-if)#`

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.3 interface giagbitEthernet

Use this command to select a Gigabit Ethernet interface, and enter the interface configuration mode.

interface gigabitEthernet *mod-num/port-num*

Parameter description

Parameter	Description
mod-num/port-num	The range depends on the device and the extended module.

Command mode	Global configuration mode.
Usage guidelines	The **no** form of the command is not available, and this interface type cannot be deleted. Use **show interfaces** or **show interfaces gigabitEthernet** to display the interface configurations.
Examples	`DES-7210(config)# interface gigabitEthernet 1/2` `DES-7210(config-if)#`

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.4 interface tenGiagbitEthernet

Use this command to select a 10G Ethernet interface, and enter the interface configuration mode.

interface tenGigabitEthernet *mod-num/port-num*

Parameter description

Parameter	Description
mod-num/port-num	The range depends on the device and the extended module.

Command mode

Global configuration mode.

Usage guidelines

The **no** form of the command is not available, and this interface type cannot be deleted. Use **show interfaces** or **show interfaces tenGigabitEthernet** to display the interface configurations.

Examples

```
DES-7210(config)# interface tenGigabitEthernet 1/2
DES-7210(config-if)#
```

Related commands

Command	Description
show interfaces	Show the interface information.

Platform Description

No product supports this command till now.

6.1.5 interface vlan

Use the **interface vlan** command in the global configuration mode to access or create the SVI (Switch Virtual Interface). Use the **no** form of the command to remove the SVI.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Parameter description

Parameter	Description
vlan-id	VLAN ID. Its range depends by products.

Command mode

Global configuration mode.

Usage guidelines

Use **show interfaces** or **show interfaces vlan** to display the interface configurations.

Examples

```
DES-7210(config)# interface vlan 2
```

```
DES-7210(config-if)#
```

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.6 medium-type

Use this command to select the medium type for an interface. Use the **no** form of the command to restore it to the default setting.

medium-type { **fiber | copper** }

no medium-type

Parameter description

Parameter	Description
fiber	Optical interface.
copper	Copeer interface.

Default configuration

Copeer interface.

Command mode

Interface configuration (physical interface, except for AP and SVI)

Usage guidelines

If a port can be selected as an optical port or electrical port, you can only select one of them. Once the media type is selected, the attributes of the port, for example, status, duplex, flow control, and rate, all mean those of the currently selected media type. After the port type is changed, the attributes of the new port type take the default values, which can be modified as needed.

Examples

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# medium-type copeer
```

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description	The 12 SFP interfaces of the 24SFP/12GT line cards and 1210/100/1000M BASE-T interfaces allow for dynamic switching. The combo interface is not supported to automatically determine whether the current port is the SFP interface or the 10/100/1000M BASE-T interface.

6.1.7 description

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

description *string*

no description

Parameter description

Parameter	Description
string	Interface alias

Default configuration

By default, there is no alias.

Command mode

Interface configuration mode.

Usage guidelines

Use **show interfaces** to display the interface information, including the alias.

Examples

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# description GBIC-1
```

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.8 shutdown

Use the **shutdown** command in the interface configuration mode to disable an interface. Use the **no** form of the command to enable a disabled port or switch virtual interface (SVI).

shutdown

no shutdown

Command mode	Interface configuration mode
Usage guidelines	Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the **no shutdown** command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

Examples	Shut down Ap 1**:**
	`DES-7210(config)# interface aggregateport 1`
	`DES-7210(config-if)# shutdown`
	Enable Ap 1**:**
	`DES-7210(config)# interface aggregateport 1`
	`DES-7210(config-if)# no shutdown`

Related commands

Command	Description
clear interface	Reset the hardware.
show interfaces	Show the interface information.

Note If you use the script to run **no shutdown** frequently and fapidly, the system may prompt the interface status reversal.

6.1.9 speed

Use this command to configure the speed on the port. Use the **no** form of the command to restore it to the default setting.

Parameter description

Parameter	Description
10	Means that the transmission rate of the interface is 10Mbps.
100	Means that the transmission rate of the interface is 100Mbps.
1000	Means that the transmission rate of the interface is 1000Mbps.
10G	Means that the transmission rate of the interface is 10Gbps.
auto	Self-adaptive

Default configuration	Auto.
Command mode	Interface configuration mode.
Usage guidelines	If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use **show interfaces** to display configuration. The rate varies by interface types. For example, you cannot set the rate of a SFP interface to 10M or 100M.
Examples	`DES-7210(config)# interface gigabitethernet 1/1` `DES-7210(config-if)# speed 100`

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.10 duplex

Use the **duplex** command in the interface configuration mode to specify the duplex mode for the interface. Use the **no** form of the command to restore it to the default setting.

duplex {**auto | full | half**}

no duplex

Parameter description

Parameter	Description
auto	Self-adaptive full duplex and half duplex
full	Full duplex
half	Half duplex

Default configuration	Auto.
Command mode	Interface configuration mode.

Usage guidelines	The duplex mode is associated with the interface type. Use **show interfaces** to display the duplex mode of the interface

Examples

```
DES-7210(config-if)# duplex full
```

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.11 flowcontrol

Use this command to enable or disable the flow control. Use the **no** form of the command to restore it to the default setting.

flowcontrol {**auto | off | on**}

no flowcontrol

Parameter description

Parameter	Description
auto	Self-negotiate the flow control.
off	Disable the flow control.
on	Enable the flow control.

Default configuration	By default, flow control is disabled.
Command mode	Interface configuration mode.
Usage guidelines	Use **show interfaces** to display the flow control configurations.

Examples

This example shows how to enable flow control on fastEthernet port 1/1:

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# flowcontrol on
```

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.12 mtu

Use this command to set the MTU supported on the interface.

mtu *num*

Parameter description

Parameter	Description
num	64 to 9216 (or 65536, which varies by products)

Default configuration

By default, the num is 1500.

Command mode

Interface configuration mode.

Usage guidelines

Set the maximum transmission unit (MTU) supported on the interface. DES-7200 now supports the setting on physical interfaces.

Examples

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# mtu 9216
```

Related commands

Command	Description
show interfaces	Show the interface information.

6.1.13 carrier-delay

In the interface configuration mode, execute the **carrier-delay** command to set the carrier delay on the interface, and the **no carrier-delay** command to restore it to the default value.

carrier-delay [*seconds*]

no carrier-delay

Parameter description

Parameter	Description
seconds	Optional parameter in the range of 1 to 60 seconds

Default configuration

The default carrier delay is 2 seconds.

Command mode	Interface configuration mode
Usage guidelines	This parameter refers to the delay after which the carrier detection signal DCD of the interface link changes from the Down status to the Up status. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upeer data link layer for renegotiation. If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route aggregation so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is shorter than the time used for route aggregation, you should set the parameter to a higher value to avoid unnecessary route vibration.

Examples	The following example shows how to configure the carrier delay of serial interface to 5 seconds:
	`DES-7210(config)# interface gigabitethernet 1/1`
	`DES-7210(config)# carrier-delay 5`

6.1.14 clear counters

Use this command to clear the counters on the specified interface.

clear counters [*interface-id*]

Parameter description

Parameter	Description
interface-id	Interface type and interface ID

Command mode	Privileged mode.
Usage guidelines	In the privileged EXEC mode, use the **show interfaces** command to display the counters or the **clear counters** command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.
Examples	`DES-7210# clear counters gigabitethernet 1/1`

Related

Command	Description

commands	**show interfaces**	Show the interface information.

6.1.15 clear interface

Reset the interface hardware.

clear interface *interface-id*

Parameter description

Parameter	Description
interface-id	Interface type and interface ID

Command mode Privileged mode.

Usage guidelines This command is only used on the switch port, member port of the L2 Aggregate port, routing port, and member port of the L3 aggregate port. This command is equal to the **shutdown** and **no shutdown** commands.

Examples

```
DES-7210# clear interface gigabitethernet 1/1
```

Related commands

Command	Description
shutdown	Shutdown the interface.

6.1.16 switchport

In the interface configuration mode, you can use **switchport** without any parameter to configure an interface as Layer 2 mode. Use the **no switchport** command without any parameter to configure it as Layer 3 interface.

switchport

no switchport

Default All the interfaces are in Layer 2 mode by default.

Command mode Interface configuration mode.

Usage guidelines	This command is valid only for physical interfaces. The **switchport** command is used to disable the interface and re-enable it. In this status, the device will send the information to indicate the connect status. If the interface is changed to Layer 3 mode from Layer 2, all the attributes in Layer 2 mode will be cleared.
Examples	`DES-7210(config-if)# switchport`

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description	Only DES-7200 supports the creation of L3 aggregate ports, up to 128 L3 Aps globally. Up to 2000 IP addresses are supported.

6.1.17 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or an 802.1Q tunnel. Use the **no** form of the command to restore it to the default setting.

switchport mode {**access | trunk**}

no switchport mode

Parameter description

Parameter	Description
access	Configure the switch port as an access port.
trunk	Configure the switch port as a trunk port.

Default configuration	The default mode of switch port is access port.
Command mode	Interface configuration mode.

Usage guidelines	If a switch port mode is access port, it can be the member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN. A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use **switchport trunk** to define the allowed-VLANs list.

Examples

```
DES-7210(config-if)# switchport mode trunk
```

Related commands

Command	Description
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.
switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port.

6.1.18 switchport access

Use this command to configure an interface as a statics access port and add it to a VLAN. Use the **no** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter description

Parameter	Description
vlan-id	The VLAN ID at which the port to be added.

Default configuration

By default, the switch port is an access port and the VLAN is VLAN 1.

Command mode

Interface configuration mode.

Usage guidelines

Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the interface to the VLAN.

If the port is a trunk port, the operation does not take effect.

Examples	DES-7210(config)# **interface gigabitethernet** *1/1* DES-7210(config-if)# **switchport access vlan** *2*

Related commands	**Command**	**Description**
	switchport mode	Specify the interface as Layer 2 mode(switch port mode).
	switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

6.1.19 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the **no** form of the command to restore it to the default setting.

switchport trunk {**allowed vlan** {*all* **|** [**add | remove | except**] **vlan-list** }**| native vlan** *vlan-id*}

no switchport trunk {**allowed vlan | native vlan**}

Parameter description	**Parameter**	**Description**
	allowed vlan *vlan-list*	Configure the list of VLANs allowed on the trunk port. *vlan-list* can be a VLAN or a range of VLANs starting with the smaller VLAN ID and ending with the larger VLAN ID and being separated by hyphen, for example, 10 to 20. The segments can be separated with a comma (,), for example, 1 to 10, 20 to 25, 30, 33. all means that the allowed VLAN list contains all the supported VLANs; add means to add the specified VLAN list to the allowed VLAN list; remove means to remove the specified VLAN list from the allowed VLAN list; except means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
	native vlan *vlan-id*	Specify the native VLAN.

Default configuration	The allowed VLAN list is all, the Native VLAN is VLAN1.

Command mode	Interface configuration mode.
Usage guidelines	**Native VLAN**: A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged. **Allowed-VLAN List:** By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk by configuring allowed VLAN lists on a trunk. Use **show interfaces switchport** to display configuration.

Examples	The example below removes port 1/15 from VLAN 2:
	`DES-7210(config)# interface fastethernet 1/15`
	`DES-7210(config-if)# switchport trunk allowed vlan remove 2`
	`DES-7210(config-if)# end`
	`DES-7210# show interfaces fastethernet1/15 switchport`
	`Switchport is enabled`
	`Mode is trunk port`
	`Access vlan is 1,Native vlan is 1`
	`Protected is disabled`
	`Vlan lists is`
	`1,3-4094`

Related commands

Command	Description
show interfaces	Show the interface information.
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.

6.1.20 snmp trap link-status

You can set whether to send LinkTrap on a port. If the function is enabled, the SNMP will send the LinkTrap when the link status of the port changes. The **no** form of this command prevents the SNMP from sending the LinkTrap.

snmp trap link-status

no snmp trap link-status

Default configuration	This function is enabled. If the link status of the port changes, the SNMP sends the LinkTrap.
Command mode	Interface configuration mode.
Usage guidelines	For an interface (for instance, Ethernet interface, AP interface, and SVI interface), this command sets whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.

Examples	Do not send LinkTrap on the interface:
	`DES-7210(config)# interface gigabitEthernet 1/1`
	`DES-7210(config-if)# no snmp trap link-status`
	Following configuration shows how to configure the interface to forwarding Link trap:
	`DES-7210(config)# interface gigabitEthernet 1/1`
	`DES-7210(config-if)# snmp trap link-status`

Related commands

Command	Function
DES-7210(config-if)# **snmp trap link-status**	Enable sending LinkTrap on the interface.
DES-7210(config-if)# **no snmp trap link-status**	Disable sending LinkTrap on the interface.

6.2 Showing Related Command

6.2.1 show interfaces

Use this command to show the interface information.

show interfaces [*interface-id*] [**counters | description | status | switchport | trunk**]

Parameter description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregate port, or SVI).
counters	The counters on the interface.

description	The description of the interface, including the link status.
status	All the link status of the Layer 2 interface, including the rate and duplex.
switchport	Layer 2 interface information.
trunk	Trunk port, applicable for physical port and aggregate port.

Default configuration

Show all the information.

Command mode

Privileged mode.

Usage guidelines

Show the basic information if no parameter is specified.

Examples

```
DES-7210# show interfacesgigabitEthernet 0/1 switchport
Interface Switchport ModeAccess Native Protected VLAN lists
--------- ---------- --------- ------ ------ --------- ----------
GigabitEthernet 0/1 enabled Access 11 Disabled ALL
```

Related commands

Command	Description
duplex	Duplex
flowcontrol	Flow control status.
interface gigabitEthernet	Select the interface and enter the interface configuration mode.
interface aggregateport	Create or access the aggregate port, and enter the interface configuration mode.
interface vlan	Create or access the switch virtual interface (SVI), and enter the interface configuration mode.
shutdown	Disable the interface.
speed	Configure the speed on the port.
switchport priority	Configure the default 802.1q interface priority.
switchport protected	Specify the interface as a protected port.

7 Aggregate Port Configuration Commands

7.1 Configuration Related Commands

7.1.1 port-group

Use this command to assign a physical interface to be a member port of an aggregate port. Use the **no** form of the command to remove the membership from the aggregate port.

port-group *port-group-number*

no port-group

Default configuration

By default, the physical port does not belong to any aggregate port.

Parameter description

Parameter	Description
port-group-number	Number of the member group of an aggregate port, the interface number of the aggregate port

Command mode

Interface configuration mode.

Usage guidelines

All the members of an aggregate port belong to a VLAN or configured to be trunk ports. The ports belonging to different native VLANs cannot form an aggregate port.

Examples

This example shows how to specify the Ethernet interface 1/3 and 1/4 as members of AP 3:

```
DES-7210(config)# interface gigabitethernet 1/3
DES-7210(config-if)# port-group 3
```

Platform description	DES-7200 supports up to 8 member ports and create up to 128 AP globally.

7.1.2 aggregateport load-balance

Specify a load-balance algorithm. Use the **no** command to return it to the default setting.

aggregateport load-balance {**dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst ip** }

no aggregateport load-balance

Parameter description

Parameter	Description
dst-mac	Traffic is distributed according to the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
src-mac	Traffic is distributed according to the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
Src-dst-ip	Traffic is distributed according to the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
dst-ip	Traffic is distributed according to the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
src-ip	Traffic is distributed according to the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different

		ports, and those from the same addresses are distributed to the same port.
	src-dst-mac	Traffic is distributed according to the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.

Default configuration	Traffic is distributed according to the destination and source MAC addresses of the incoming packets.
Command mode	Global configuration mode.
Usage guidelines	Use **show aggregateport** to display load-balance configuration.
Examples	`DES-7210(config)# aggregateport load-balance dst-mac`

Related commands

Command	Description
show aggregateport load-balance	Use this command to display aggregate port configurations.

Platform description	DES-7200 supports all load balance algorithms.

7.2 Showing Related Command

7.2.1 show aggregateport

Use this command to display the aggregate port configurations.

show aggregateport {[*aggregate-port-number*] **summary** | **load-balance**}

Parameter description

Parameter	Description
aggregate-port-number	Number of the aggregate port.

	load-balance	Show the load-balance algorithm on the aggregate port.
	summary	Show the summary of the aggregate port.

Command mode

Privileged mode.

Usage guidelines

If the aggregate port number is not specified, all the aggregate port information will be displayed.

Examples

```
DES-7210# show aggregateport 1 summary
AggregatePort  MaxPorts       SwitchPort Mode   Ports
-------------  --------       -------------   ------
Ag1               8            Enabled     ACCESS
```

Related commands

Command	Description
aggregateport load-balance	Configure a load-balance algorithm of AP.

8 LACP Configuration Commands

8.1 Configuration Related Commands

The VRRP configuration commands include:

- **port-group mode**
- **lacp system-priority**
- **lacp port-priority**

8.1.1 port-group mode

Use this command to enable LACP and specify the group ID and the aggregation mode. Use the **no** form of this command to disable the LACP.

port-group *key* **mode {active | passive}**

no port-group

Parameter description

Parameter	Description
key	Specify the group ID on the port to be aggregated. The key values vary with the aggregation group numbers supported for different products.
active	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
passive	Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

Default configuration By default, the LACP function is disabled on the interface.

Command mode	Interface configuration mode.
Usage guidelines	N/A
Examples	`DES-7210(config)# interface gigabitethernet 1/1` `DES-7210(config-if)# port-group 1 mode active`

Related commands

Command	Description
lacp port-priority	Set the LACP port priority.

8.1.2 lacp port-priority

Use this command to set the LACP port priority. Use the **no** form of this command to return to the default value.

lacp port-priority *port-priority*

no lacp port-priority

Parameter description

Parameter	Description
port-priority	The port priority, in the range of 0-65535.

Default configuration	By default, the port priority is 32768.
Command mode	Interface configuration mode.
Usage guidelines	When multiple ports are to be aggregated, the ports with high priorities take precedence and the port with the highest priority is selected as the master port. The port priority sequence is determined according to the wire quality.
Examples	`DES-7210(config)# interface gigabitethernet 1/1` `DES-7210(config-if)# lacp port-priority`

Related commands

Command	Description
port-group *key* **mode** {**active** | **passive**}	Enable the LACP on the port and specify the aggregation group ID and operation mode.

Plarform description

The software version must be R10.3(4) and higher.

8.1.3 lacp system-priority

Use this command to set the LACP system priority. The **no** form of it restores it to the default.

lacp system-priority *system-priority*

no lacp system-priority

Parameter description

Parameter	Description
system-priority	The LACP system priority, in the range of 0-65535.

Default configuration

By default, the system priority is 32768.

Command mode

Global configuration mode.

Usage guidelines

LACP system priority consists of the Layer2 management MAC address and its priority value, where the MAC address is fixed but the priority value is configurable. If two priorities are equal, then the smaller the MAC address is, the higher the priority is. All LACP groups on the switch share the system priority. Changing the system priority may influence the whole aggregation groups on the switch.

Examples

```
DES-7210(config)# lacp system-priority 4096
```

Related

Command	Description

commands	**port-group** *key* **mode** {**active** | **passive**}	Enable the LACP on the port and specify the aggregation group ID and operation mode.
	lacp port-priority	Set the LACP port priority.

8.2 Showing Related Command

8.2.1 show lacp summary

Use this command to show the LACP aggregation information.

show lacp summary

Parameter description	**Parameter**	**Description**
	-	-

Command mode	Privileged mode.
Usage guidelines	N/A.

Examples

```
DES-7210# show LACP summary
Flags:S - Device is sending Slow LACPDUs   F - Device is sending fast
LACPDUs.
A - Device is in active mode.   P - Device is in passive mode.
Aggregate port 3:
Local information:
                    LACP port      Oper    Port    Port
Port    Flags    State    Priority    Key    Number  State
------------------------------------------------------------
Gi0/1    SA       bndl       4096        0x3    0x1     0x3d
Gi0/2    SA       bndl       4096        0x3    0x2     0x3d
Gi0/3    SA       bndl       4096        0x3    0x3     0x3d
Partner information:
                    LACP port        Oper    Port    Port
Port    Flags    Priority    Dev ID    Key    Number   State
------------------------------------------------------------
```

```
Gi0/1    SA    61440    00d0.f800.0002  0x3    0x1     0x3d
Gi0/2    SA    61440    00d0.f800.0002  0x3    0x2     0x3d
Gi0/3    SA    61440    00d0.f800.0002  0x3    0x3     0x3d
```

Field	Description
Local information	Show the local LACP information.
Port	Show the system port ID.
Flags	Show the port state flag: “S” indicates that the LACP is stable and in the state of periodically sending the LACPPDU; “A” indicates that the port is in the active mode.
State	Show the port aggregation information: “bndl” indicates that the port is aggregated; “Down” represents the disconnection port state; “sups” indicates that the port is not aggregated.
LACP Port Priority	Show the LACP port priority.
Oper Key	Show the port operation key.
Port Number	Show the port number.
Port State	Show the flag bit for the LACP port state.
Partner infomation	Partly show the LACP information of the peer port.
Dev ID	Partly show the system MAC information of the peer device.

Related commands

Command	Description
port-group *key* **mode**	Enable the LACP on the port and specify the aggregation group ID and operation mode.

9 VLAN Configuration Commands

9.1 Configuration Related Commands

9.1.1 vlan

Use this command to enter the VLAN configuration mode. Use the **no** form of the command to remove the VLAN.

vlan vlan-id

no vlan *vlan-id*

Parameter description

Parameter	Description
vlan-id	VLAN ID Default VLAN (VLAN 1) cannot be removed.

Command mode

Global configuration mode.

Usage guidelines

To return to the privileged EXEC mode, input **end** or pressing **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Examples

```
DES-7210(config)# vlan 1
DES-7210(config-vlan)#
```

Related commands

Command	Description
show vlan	Show member ports of the VLAN.

Platform description

DES-7200 supports up to 4093 VLANs.

9.1.2 name

Use the command to specify the name of a VLAN. Use the **no** form of the command to restore it to the default setting.

name *vlan-name*

no name

Parameter description

Parameter	Description
vlan-name	VLAN name

Default configuration

No name.

Command mode

VLAN configuration Mode.

Usage guidelines

You can view the VLAN settings by using the **show vlan** command.

Examples

```
DES-7210(config)# vlan 10
DES-7210(config-vlan)# name vlan10
```

Related commands

Command	Description
show vlan	Show member ports of the VLAN.

9.1.3 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or an 802.1Q tunnel. Use the **no** form of the command to restore the default setting.

switchport mode {**access** | **trunk**}

no switchport mode

Parameter description

Parameter	Description
access	Configure the switch port as an access port.
trunk	Configure the switch port as a trunk port.

Default configuration	By default, the switch port is an access port.
Command mode	Interface configuration mode.
Usage guidelines	If a switch port mode is access port, it can be the member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN. A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use **switchport trunk** to define the allowed-VLANs list.
Examples	`DES-7210(config-if)# switchport mode trunk`

Related commands

Command	Description
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.
switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

9.1.4 switchport access

Use this command to configure an interface as a statics access port and assign it to a VLAN. Use the **no** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter description

Parameter	Description
vlan-id	The VLAN ID at which the port to be added.

Default configuration	By default, the switch port is an access port and the VLAN is VLAN 1.
Command mode	Interface configuration mode.

Usage guidelines	Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the port to the VLAN. If the port is a trunk port, the operation does not take effect.
Examples	`DES-7210(config)# interface gigabitethernet 1/1` `DES-7210(config-if)# switchport access vlan 2`

Related commands

Command	Description
switchport mode	Specify the interface as Layer 2 mode (switch port mode).
switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

9.1.5 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the **no** form of the command to restore the default setting.

switchport trunk {**allowed vlan** { **all** | [**add** | **remove** | **except**] *vlan-list* }| **native vlan** *vlan-id*}

no switchport trunk {**allowed vlan** | **native vlan** }

Parameter description

Parameter	Description
allowed vlan *vlan-list*	Configure the list of VLANs allowed on the trunk port. *vlan-list* can be a VLAN or a range of VLANs starting with the smaller VLAN ID and ending with the larger VLAN ID and being separated by hyphen, for example, 10 to 20. The segments can be separated with a comma (,), for example, 1 to 10, 20 to 25, 30, 33. **all** means that the allowed VLAN list contains all the supported VLANs; **add** means to add the specified VLAN list to the allowed VLAN list; **remove** means to remove the specified VLAN list from the allowed VLAN list; **except** means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
native vlan *vlan-id*	Specify the native VLAN.

Default configuration	The default allowed-VLAN list is all the VLANs, the default native VLAN is VLAN 1.
Command mode	Interface configuration mode.
Usage guidelines	**Native VLAN:** A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged. **Allowed-VLAN List:** By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk port by configuring allowed VLAN lists on a trunk port . Use **show interfaces switchport** to display configuration.

Examples	The example below removes port 1/15 from VLAN 2:
	`DES-7210(config)# interface fastethernet 1/15`
	`DES-7210(config-if)# switchport trunk allowed vlan remove 2`
	`DES-7210(config-if)# end`
	`DES-7210# show interfaces fastethernet1/15 switchport`
	`Switchport is enabled`
	`Mode is trunk port`
	`Acsess vlan is 1,Native vlan is 1`
	`Protected is disabled`
	`Vlan lists is`
	`1,3-4094`

Related commands

Command	Description
show interfaces	Show the interface information.
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.

9.2 Showing Related Command

9.2.1 show vlan

Show member ports of the VLAN.

show vlan [**id** *vlan-id*]

Parameter description

Parameter	Description
vlan-id	VLAN ID

Default configuration

Show all the information by default.

Command mode

Privileged mode.

Usage guidelines

To return to the privileged EXEC mode, input **end** or pressing **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Examples

```
DES-7210# show vlan id 1
VLAN[1] "VLAN0001"
       GigabitEthernet 3/1
       GigabitEthernet 3/2
       GigabitEthernet 3/3
       GigabitEthernet 3/4
       GigabitEthernet 3/5
       GigabitEthernet 3/6
       GigabitEthernet 3/7
       GigabitEthernet 3/8
       GigabitEthernet 3/9
       GigabitEthernet 3/10
       GigabitEthernet 3/11
       GigabitEthernet 3/12
```

Related commands

Command	Description
name	VLAN name.
switchport access	Add the interface to a VLAN.

10 Super-VLAN Configuration Commands

10.1 Configuring Related Commands

10.1.1 supervlan

Use this command to set the VLAN as a super VLAN.

supervlan

no supervlan

Parameter description	N/A.
Command mode	VLAN configuration Mode.
Usage guidelines	To return to the privileged EXEC mode, input **end** or press **Ctrl+C**. To return to the global configuration mode, input **exit.**
Examples	`DES-7210(config)# vlan 3` `DES-7210(config-vlan)# supervlan`

Related commands

Command	Description
show supervlan	Show the super VLAN information.

Platform description	N/A.

10.1.2 subvlan

Use this command to set the sub VLAN of this super VLAN or delete sub VLAN.

subvlan *vlan-id-list*

no subvlan *[vlan-id-list]*

Parameter description

Parameter	Description
vlan-id-list	Sub VLAN ID of the VLAN. Multiple VLANs are supported.

Command mode

VLAN configuration Mode.

Usage guidelines

Use **no subvlan** command to delete all sub VLANs of this super VLAN.

Examples

```
DES-7210(config)# vlan 3
DES-7210(config-vlan)# supervlan
DES-7210(config-vlan)# subvlan 5
DES-7210(config-vlan)# subvlan 7-19
```

Related commands

Command	Description
show supervlan	Show the super VLAN information.

10.1.3 subvlan-address-range

Use this command to set the IP address range of the sub VLAN.

subvlan-address-range *start-ip end-ip*

no subvlan-address-range

Parameter description

Parameter	Description
start-ip	The start IP address of this sub VLAN
end-ip	The end IP address of this sub VLAN

Command mode

VLAN configuration Mode.

Usage guidelines

To return to the privileged EXEC mode, input **end** or press **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Examples

```
DES-7210(config)# vlan 3
DES-7210(config-vlan)# subvlan-address-range
```

	192.168.3.10 192.168.3.100

Related commands	Command	Description
	show supervlan	Show the super VLAN information.

10.1.4 proxy-arp

Use this command to enable the ARP agent function of a VLAN.

proxy -arp

no proxy -arp

Parameter description	N/A.
Command mode	VLAN configuration Mode.
Usage guidelines	To return to the privileged EXEC mode, input **end** or press **Ctrl+C**. To return to the global configuration mode, input **exit.**
Examples	`DES-7210(config)# vlan 3` `DES-7210(config-vlan)# proxy-arp`

Related commands	Command	Description
	show supervlan	Show the super VLAN information.

Platform description	N/A.

10.2 Showing Related Command

10.2.1 show supervlan

Use this command to show the configuration of the super VLAN and its sub VLANs.

show supervlan

show supervlan id *vlan-id*

Parameter description

Parameter	Description
vlan-id	VLAN ID

Command mode

Privileged mode.

Usage guidelines

N/A.

Examples

```
DES-7210# show supervlan
supervlan id  supervlan arp-agent  subvlan id  subvlan arp-agent
subvlan ip range
-------    ----------  -------------    -----------------
3               ON          4               ON
                            5               ON
```

11 Protocol VLAN Configuration Commands

11.1 Configuration Related Commands

- **protocol-vlan ipv4** *addr* **mask** *addr* **vlan** *id*
- **protocol-vlan profile** *num* **frame-type** [*type*] **ether-type** [*type*]
- **protocol-vlan profile** *num* **vlan** *id*

11.1.1 protocol-vlan ipv4 *addr* mask *addr* vlan *id*

Use this command to configure the IP address, subnet mask and VLAN classification.

Parameter description

Parameter	Description
addr	IP address in the x.x.x.x format.
id	VLAN ID, the maximal VLAN the product supports

Default configuration

N/A.

Command mode

Global configuration mode.

Examples

```
DES-7210(config)# protocol-vlan ipv4 192.168.100.3 mask 255.255.255.0 vlan 100
```

Related commands

Command	Description
show protocol-vlan ipv4	
no protocol-vlan ipv4 *addr* **mask** *addr*	

	no protocol-vlan ipv4	

11.1.2 protocol-vlan profile *num* frame-type *type* ether-type *type*

Use this command to configure message type and Ethernet type profile.

Parameter description

Parameter	Description
num	Profile indexes
type	Type of message and Ethernet

Default configuration

N/A.

Command mode

Global configuration mode.

Examples

```
DES-7210(config)# protocol-vlan profile 1 frame-type ETHERII ether-type aarp
```

Related commands

Command	Description
show protocol-vlan profile	
show protocol-vlan profile *num*	
no protocol-vlan profile	
no protocol-vlan profile *num*	

Platform description

The software version must be R10.1 and later.

11.1.3 protocol-vlan profile *num* vlan *id*

Use this command to apply some profile to an interface.

Parameter description

Parameter	Description
num	Profile indexes
id	VLAN ID, the maximal VLAN the product supports.

Command mode	Interface mode.

Examples

```
DES-7210(config-if)# protocol-vlan profile 1 vlan 101
```

Related commands

Command	Description
show protocol-vlan profile	
show protocol-vlan profile *num*	
no protocol-vlan profile	
no protocol-vlan profile *num*	

Platform description	The software version must be R10.1 and later.

11.2 Showing Related Commands

- **show protocol-vlan**

11.2.1 show protocol-vlan

Show the configuration of protocol VLAN.

show protocol-vlan

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged mode.

Examples

```
DES-7210# show protocol-vlan
```

Platform description	The software version must be R10.1 and later.

12 Private VLAN Configuration Commands

12.1 Configuration Related Commands

- **private-vlan type**
- **private-vlan association**
- **private-vlan mapping**
- **switchport mode private-vlan**
- **switchport private-vlan host-association**
- **switchport private-vlan mapping**

12.1.1 private-vlan *type*

Use this command to configure the VLAN as the private VLAN.

private-vlan {**community | isolated | primary**}

no private-vlan {**community | isolated | primary**}

Parameter description

Parameter	Description
community	Configure it as the community VLAN.
isolated	Configure it as the isolated VLAN.
primary	Configure it as the primary VLAN.
no	Delete the corresponding private VLAN configuration.

Default configuration

No private VLAN is configured.

Command mode

VLAN configuration Mode.

Examples

```
DES-7210(config)# vlan 22
DES-7210(config-vlan)# private-vlan primary
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be R10.1 and later.

12.1.2 private-vlan association

Use this command to associate the secondary VLAN with the primary command.

private-vlan association {*svlist* **| add** *svlist* **| remove** *svlist*}

no private-vlan association

Parameter description

Parameter	Description
svlist	The secondary VLAN list
no	Remove the association between the primary VLAN and all the secondary VLANs.

Default configuration

No association.

Command mode

VLAN configuration Mode.

Examples

```
DES-7210(config)# vlan 22
DES-7210(config-vlan)# private-vlan association add 24-26
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be R10.1 and later.

12.1.3 private-vlan mapping

Use this command to map the secondary VLAN to the L3 SVI interface.

private-vlan mapping {*svlist* **| add** *svlist* **| remove** *svlist*}

no private-vlan mapping

Parameter description

Parameter	Description
svlist	secondary VLAN list
no	Delete the mapping.

Command mode

The interface mode corresponding to the primary VLAN

Examples

```
DES-7210(config)# interface vlan 22
DES-7210(config-if)# private-vlan mapping add 24-26
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be R10.1 and later.

12.1.4 switchport mode private-vlan

Use this command to declare the private VLAN mode of the interface.

switchport mode private-vlan {**host | promiscuous** }

no switchport mode

Parameter description

Parameter	Description
host	Host mode of the private VLAN
promiscuous	Promiscuous mode of the private VLAN
no	Delete the private VLAN configuration of the port.

Command mode

Interface mode.

Examples

```
DES-7210(config)# interface gigabitEthernet0/2
DES-7210(config-if)# switchport mode private-vlan host
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be R10.1 and later.

12.1.5 switchport private-vlan host-association

Use this command to associate the primary VLAN, which is associated with the private VLAN mode of the interface, with the secondary VLAN.

switchport private-vlan host-association *p_vid s_vid*

no switchport private-vlan host-association

Parameter description

Parameter	Description
p_vid	Primary VID.
s_vid	Secondary VID
no	Delete the host port from the private VLAN.

Command mode

Interface configuration mode.

Examples

```
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode private-vlan host
DES-7210(config-if)# switchport private-vlan host-association 22
23
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be R10.1 and later.

12.1.6 switchport private-vlan mapping

Use this command to configure the promiscuous secondary VLANs that the promiscuous mode of the private VLAN maps.

switchport private-vlan mapping *p_vid* {*svlist*|**add** *svist* |**remove** *svlist*}

no switchport private-vlan mapping

Parameter description

Parameter	Description
p_vid	Primary VID
svlist	Secondary VLAN list.
no	Remove all the promiscuous secondary VLANs.

Default configuration

No promiscuous secondary VLAN is configured.

Command mode

Hybrid interface configuration mode of private VLAN

Examples

```
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode private-vlan promiscuous
DES-7210(config-if)# switchport private-vlan mapping 22 add 23-25
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be R10.1 and later.

12.2 Showing Related Commands

- **show vlan private-vlan**

12.2.1 show vlan private-vlan

Show the configuration of private VLAN.

show vlan private-vlan [**community** | **primary** | **isolated**]

Parameter description

Parameter	Description
primary	Show the primary VLAN information.
community	Show the community VLAN information.
isolated	Show the isolated VLAN information.

Default configuration

No private VLAN is configured.

Command mode

Privileged mode.

Examples

```
DES-7210# show vlan private-vlan
```

Platform description

The software version must be R10.1 and later.

12.3 Hybrid Commands

- **switchport mode hybrid**
- **switchport hybrid native vlan**
- **switchport hybrid allowed vlan**

12.3.1 switchport mode hybrid

switchport mode hybrid

no switchport mode

Use this command to configure the port as a hybrid port.

Parameter description

Parameter	Description
no	Delete the hybrid port.

Default configuration

No hybrid port is configured.

Command mode

Interface configuration mode.

Examples	`DES-7210(config-if)# switchport mode hybrid`
Platform description	The software version must be R10.1 and later.

12.3.2 switchport hybrid native vlan

switchport hybrid native vlan *vid*

no switchport hybrid native vlan

use this command to configure the default VLAN of a hybrid port.

Parameter description

Parameter	Description
no	Restore the hybrid port to the default VLAN.

Default configuration	No default VLAN is configured.
Command mode	Interface mode.
Examples	`DES-7210(config-if)# switchport hybrid native vlan 3`
Platform description	The software version must be R10.1 and later.

12.3.3 switchport hybrid allowed vlan

switchport hybrid allowed vlan [[add] [tagged | untagged] | remove] v*list*

no switchport hybrid allowed vlan

Use this command to configure the output rules of a hybrid port.

Parameter description

Parameter	Description
no	Restore the output rules of the hybrid port to the default settings.

Default configuration	No output rules are configured.

Command mode	Interface mode.
Examples	`DES-7210(config-if)# switchport hybrid allowed vlan add untagged 3-5`
Platform description	The software version must be R10.1 and later.

13 802.1Q Tunneling Configuration Commands

13.1 Configuration Related Commands

- **switchport mode dot1q-tunnel**
- **switchport mode uplink**
- **frame-tag tpid** *tpid*
- **inner-priority-trust enable**

13.1.1 switchport mode dot1q-tunnel

Use this command to configure the interface as the 802.1Q tunneling interface.

switchport mode dot1q-tunnel

no switchport mode

Parameter description

Parameter	Description
no	Delete the corresponding 802.1Q tunneling interface configuration.

Default configuration

No 802.1Q tunneling interface is configured.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring the interface as the 802.1Q tunneling interface:

```
DES-7210(config)# interface gi 0/1
DES-7210(config-if)# switchport access vlan 22
DES-7210(config-if)# switchport mode dot1q-tunnel
```

```
DES-7210(config)# end
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be R10.1 and later.

13.1.2 switchport mode uplink

Use this command to configure the interface as a uplink port.

switchport mode uplink

no switchport mode

Parameter description

Parameter	Description
no	Remove the settings.

Default configuration

No uplink port is configured.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring the interface as a uplink port.

```
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode up-link
DES-7210(config)# end
```

Related commands

Command	Description
show vlan private-vlan	

Platform description

The software version must be R10.1 and later.

13.1.3 frame-tag tpid *tpid*

Use this command to set the manufacturer tpid.

frame-tag tpid <*tpid*>

no frame-tag tpid

Parameter description

Parameter	Description
no	Remove the setting.

Command mode

Interface configuration mode.

Examples

```
DES-7210(config)# interface g0/3
DES-7210(config-if)# frame-tag tpid 9100
DES-7210(config-if)# end
DES-7210# show frame-tag tpid
Port    tpid
------  ---------
Gi0/3     0x9100
```

Related commands

Command	Description
show frame-tag *tpid*	

Platform description

The software version must be R10.1 and later.

13.1.4 inner-priority-trust enable

Use this command to copy the priority of the inner tag to the outer tag of the packets on the interface.

inner-priority-trust enable

no inner-priority-trust enable

Parameter description

Parameter	Description
no	Remove the settings.

Command mode

Interface configuration mode.

Examples

```
DES-7210(config)# interface gigabitEthernet 0/2
DES-7210(config-if)# inner-priority-trust enable
```

Related commands	**Command**	**Description**
	show inner-priority-trust	

Platform description	The software version is R10.1 and later.

13.2 Showing Command

- **show frame-tag tpid**
- **show inner-priority-trust**

13.2.1 show frame-tag tpid

Use this command to show the configuration of interface tpid.

show frame-tag tpid [**interface <***intf-id***>**]

Parameter description	**Parameter**	**Description**
	intf-id	Specific Interface

Default configuration	The tpid is not modified.
Command mode	Privileged mode.

Examples

```
DES-7210# show frame-tag tpid
Ports    tpid
-----  ---------
Gi0/1     0x9100
```

Platform description	The software version must be R10.1 and later.

13.2.2 show inner-priority-trust

Use this command to show the priority copy configuration.

show inner-priority-trust

Parameter description	N/A.
Default configuration	Priority copy is disabled by default.
Command mode	Privileged mode.
Examples	DES-7210# **show inner-priority-trust** Port inner-priority-trust ---- ---------- Gi0/1 enable
Platform description	The software version must be R10.1 and later.

14 MAC Address Configuration Commands

14.1 Configuration Related Commands

The MAC address configuration commands include:

- **mac-address-table aging-time**
- **clear mac-address-table dynamic**
- **clear mac-address-table filtering**
- **clear mac-address-table static**
- **mac-address-table static**
- **mac-address-table filtering**
- **mac-address-table notification**
- **nmp trap mac-notification**
- **address-bind**
- **address-bind ip-address**
- **address-bind uplink**
- **address-bind install**
- **address-bind ipv6-mode**
- **mac-manage-learning uniform**
- **mac-manage-learning uniform learning-synchronization**
- **mac-manage-learning dispersive**

14.1.1 mac-address-table aging-time

Use this command to specify the aging time of the dynamic MAC address. Use the **no** form of the command to restore it to the default setting.

mac-address-table aging-time *seconds*

no mac-address-table aging-time

Parameter description

Parameter	Description
seconds	Aging time of the dynamic MAC address (in seconds). The time range depends on the switch.

Default configuration

300 seconds.

Command mode

Global configuration mode.

Usage guidelines

Use **show mac-address-table aging-time** to display configuration.

Use **show mac-address-table dynamic** to display the dynamic MAC address table.

Examples

```
DES-7210(config)# mac-address-table aging-time 150
```

Related commands

Command	Description
show mac-address-table aging-time	Use this command to display the aging time of the dynamic MAC address.
show mac-address-table dynamic	Use this command to display dynamic MAC address.

14.1.2 clear mac-address-table dynamic

Use this command to clear the dynamic MAC address.

clear mac-address-table dynamic [address *mac-addr*] **[interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
dynamic	Clear all the dynamic MAC addresses.
address *mac-addr*	Clear the specified dynamic MAC address.
interface *interface-id*	Clear all the dynamic MAC addresses of the specified interface.
vlan *vlan-id*	Clear all the dynamic MAC addresses of the specified VLAN.

Command mode	Privileged mode.
Usage guidelines	Use **show mac-address-table dynamic** to display all the dynamic MAC addresses.
Examples	Clear all the dynamic MAC addresses: `DES-7210# clear mac-address-table dynamic`

Related commands

Command	Description
show mac-address-table dynamic	Use this command to display dynamic MAC address.

14.1.3 clear mac-address-table filtering

Use this command to clear the filtering MAC address.

clear mac-address-table filtering [**address** *mac-addr*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
filtering	Clear all the filtering MAC addresses.
address *mac-addr*	Clear the specified filtering MAC address.
vlan *vlan-id*	Clear all the filtering MAC addresses of the specified VLAN.

Command mode	Privileged mode.
Usage guidelines	Use **show mac-address-table filtering** to display all the filtering MAC addresses.
Examples	Clear the filtering MAC address 00d0.f800.0c0c: `DES-7210# clear mac-address-table filtering address 00d0.f800.0c0c`

Related commands

Command	Description
mac-address-table filtering	Configure the filtering MAC address.
show mac-address-table filtering	Show the filtering MAC address.

14.1.4 clear mac-address-table static

Use this command to clear the static MAC address.

clear mac-address-table dynamic [address *mac-addr*] **[interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
static	Clear all the static MAC addresses.
address *mac-addr*	Clear the specified static MAC address.
interface *interface-id*	Clear all the static MAC addresses of the specified interface.
vlan *vlan-id*	Clear all the static MAC addresses of the specified VLAN.

Command mode

Privileged mode.

Usage guidelines

Use **show mac-address-table static** to display all the static MAC addresses.

Examples

The example below is to clear the static MAC address 00d0.f800.073c**:**

```
DES-7210# clear mac-address-table static address 00d0.f800.073c
```

Related commands

Command	Description
mac-address-table static	Configure the static MAC address.
show mac-address-table static	Show the static MAC address.

14.1.5 mac-address-table static

Use this command to configure a static MAC address. Use the **no** form of the command to remove a static MAC address.

mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

Parameter description

Parameter	Description
mac-addr	Destination MAC address of the

	specified entry
vlan-id	VLAN ID of the specified entry.
interface-id	Interface (physical interface or aggregate port) that packets are forwarded to

Default configuration

No static MAC address is configured by default.

Command mode

Global configuration mode.

Usage guidelines

A static MAC address has the same function as the dynamic MAC address that the switch learns. Compared with the dynamic MAC address, the static MAC address will not be aged out. It can only be configured and removed by manual. Even if the switch is reset, the static MAC address will not be lost. A static MAC address shall not be configured as a multicast address. Use **show mac-address-table static** to display the static MAC address. Use **clear mac-address-table static** to clear static MAC address.

Examples

When the packet destined to 00d0 f800 073c arrives at VLAN4, it will be forwarded to the specified port gigabitethernet 1/1:

```
DES-7210(config)# mac-address-table static 00d0.f800.073c vlan 4
interface gigabitethernet 1/1
```

Related commands

Command	Description
show mac-address-table static	Show the static MAC address.
clear mac-address-table static	Clear the static MAC address.

Platform description

For the DES-7200 series, the global entry number in the MAC address table is 16000 and the global static MAC address number is 1000.

14.1.6 mac-address-table filtering

Use this command to configure the filtering MAC address. Use the **no** form of the command to remove the filtering address.

mac-address-table filtering *mac-address* **vlan** *vlan-id*

no mac-address-table filtering mac-address vlan vlan-id

Parameter description

Parameter	Description
mac-address	Filtering Address
vlan *vlan-id*	VLAN ID. Its range depends on the switch.

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

The filtering MAC address shall not be a multicast address. Use **show mac-address-table filtering** to display the filtering MAC addresses.

Examples

```
DES-7210(config)# mac-address-table filtering 00d0f8000000 vlan 1
```

Related commands

Command	Description
clear mac-address-table filtering	Clear the filtering MAC address.
show mac-address-table filtering	Show the filtering MAC address.

14.1.7 mac-address-table notification

Use this command to enable the MAC address notification function. You can use The **no** form of the command to disable this function.

mac-address-table notification [**interval** *value* | **history-size** *value*]

no mac-address-table notification [**interval** | **history-size**]

Parameter description

Parameter	Description
interval *value*	Specify the interval of sending the MAC address trap message, 1 second by default.
history-size *value*	Specify the maximum number of the entries in the MAC address notification table, 50 entries by default.

Default configuration

By default, the interval is 1 and the maximum number of the entries in the MAC address notification table is 50.

Command mode

Global configuration mode.

Usage guidelines

The MAC address notification function is specific for only dynamic MAC address and secure MAC address. No MAC address trap message is generated for static MAC addresses. In the global configuration mode, you can use the **snmp-server enable traps mac-notification** command to enable or disable the switch to send the MAC address trap message.

Examples

```
DES-7210(config)# mac-address-table notification
DES-7210(config)# mac-address-table notification interval 40
DES-7210(config)# mac-address-table notification history-size 100
```

Related commands

Command	Description
snmp-server enable traps	Set the method of handling the MAC address trap message..
show mac-address-table notification	Show the MAC address notification configuration and the MAC address trap notification table.
snmp trap mac-notification	Enable the MAC address trap notification function on the specified interface.

14.1.8 snmp trap mac-notification

Use this command to enable the MAC address trap notification on the specified interface. You can use The **no** form of the command to disable this function.

snmp trap mac-notification {**added** | **removed**}

no snmp trap mac-notification {**added** | **removed**}

Parameter description

Parameter	Description
added	Notify when a MAC address is added.
removed	Notify when a MAC address is removed

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Use **show mac-address-table notification interface** to display configuration.

Examples

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# snmp trap mac-notification added
```

Related commands

Command	Description
mac-address-table notification	Enable MAC address notification.
show mac-address-table notification	Show the MAC address notification configuration and the MAC address notification table.

14.1.9 address-bind

Use this command to configure IP address-MAC address binding.

address-bind *ip-address mac-address*

no address-bind *ip-address*

Parameter description

Parameter	Description
ip-address	IP address to be bound
mac-address	MAC address to be bound

Command mode

Global configuration mode.

Usage guidelines	If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.
Examples	This is an example of binding the IP address 3.3.3.3 and the MAC address 00d0.f811.1112. `DES-7210(config)# address-bind 3.3.3.3 00d0.f811.1112`

Related commands

Command	Description
show address-bind	Show the IP address-MAC address binding table.

Platform description	DES-7200 supports up to 1000 IP address-MAC address binding.

14.1.10 address-bind *ip-address*

Use this command to configure IP address-MAC address binding.

address-bind *ip-address mac-address*

no address-bind *ip-address*

Parameter description

Parameter	Description
ip-address	IP address to be bound
mac-address	MAC address to be bound

Command mode	Global configuration mode.
Usage guidelines	If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.
Examples	This is an example of binding the IP address 3.3.3.3 and MAC address 00d0.f811.1112. `DES-7210(config)# address-bind 3.3.3.3 00d0.f811.1112`

Related commands

Command	Function
show address-bind	Show the IP address-MAC address binding table.

Platform description

DES-7200 supports up to 1000 IP address-MAC address binding.

14.1.11 address-bind uplink

Use this command to configure IP address-MAC address binding.

address-bind uplink *intf-id*

no address-bind uplink *intf-id*

Parameter description

Parameter	Description
intf-id	Exceptional port

Command mode

Global configuration mode.

Usage guidelines

If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.

Examples

Following example is to set the fa 0/1 port as an exceptional port for address binding.

```
DES-7210(config)#address-bind uplink fa0/1
```

Related commands

Command	Function
show address-bind uplink	Show the exceptional port of address binding.

Platform description

The version must be R10.1 and later.

14.1.12 address-bind install

Use this command to install or uninstall the exceptional port.

address-bind install

no address-bind install

Parameter description	N/A.
Command mode	Global configuration mode.
Usage guidelines	If you have installed the exceptional port, you can run this command to make installation policy take effect.

Examples	Install fa 0/1 port:
	`DES-7210(config)# address-bind uplink fa0/1`
	`DES-7210(config)# address-bind install`

Related commands

Command	Function
show address-bind uplink	Show the exceptional port of the address binding.

Platform description	The version must be R10.1 and later.

14.1.13 address-bind ipv6-mode

Use this command to set the IP mode of IP address binding.

Set the compatbile mode:

address-bind ipv6-mode compatible

Set the loose mode:

address-bind ipv6-mode loose

Set the compatbile mode:

address-bind ipv6-mode strict

Parameter description

N/A.

Command mode

Global configuration mode.

Default value

Strict mode

Usage guidelines

There are three IP address binding modes: compatible, loose and strict. The following table shows the forwarding rules corresponding to binding modes.

Mode	IPv4 forwarding rule	IPv6 forwarding rule
Strict	Only the packets matching IPv4 and MAC are forwarded.	No IPv6 packets are forwarded (default).
Loose	Only the packets matching IPv4 and MAC are forwarded.	All IPv6 packets are forwarded.
compatible	Only the packets matching IPv4 and MAC are forwarded.	Only the IPv6 packets whose source MAC address is the bound MAC address are forwarded.

Examples

Bind the IP address 192.168.5.2 and the MAC address 00do.f822.33aa and forward the corresponding packets:

```
DES-7210# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# address-bind 00d0.f822.33aa ip 192.168.5.2
DES-7210(config)# address-bind ipv6-mode compatible
```

Related commands

Command	Function
show address-bind uplink	Show the exceptional port of the address binding.

14.1.14 mac-manage-learning uniform

Use this command to set the management and learning mode of the dynamic MAC address to the uniform mode.

Parameter description	N/A.
Command mode	Global configuration mode.
Usage guidelines	Setting the management and learning mode of the dynamic MAC address to the uniform mode can improve the L2 switching efficiency. After changing the MAC learning mode, you must save it and restart before the new mode takes effect.
Examples	N/A.

Related commands

Command	Function
show mac-address-table mac-manage-learning	Show the MAC management and learning mode.

14.1.15 mac-manage-learning uniform learning-synchronization

Use this command to synchronize the dynamic MAC address in the whole device in the uniform mode.

[no] mac-manage-learning uniform learning-sychronization

Parameter description	N/A.
Command mode	Global configuration mode.
Usage guidelines	In the uniform mode, the synchronization of the dynamic MAC address in the whole device can further improve the L2 switching efficiency. You can use the **no** form of this command to cancel the synchronization.

Examples	N/A.

Related commands

Command	Function
show mac-address-table mac-manage-learning	Show the MAC address management and learning mode.

14.1.16 mac-manage-learning dispersive

Use this command to set the management and learning mode of the dynamic MAC address to the dispersive mode.

Parameter description	N/A.
Command mode	Global configuration mode.
Usage guidelines	After the management and learning mode of the dynamic MAC address is set to the dispersive mode, the device can learn more MAC addresses.
Examples	N/A.

Related commands

Command	Function
show mac-address-table mac-manage-learning	Show the MAC address management and learning mode.

14.2 Showing Related Command

The MAC address showing commands include:

- **show mac-address-table address**
- **show mac-address-table aging-time**
- **show mac-address-table count**
- **show mac-address-table dynamic**
- **show mac-address-table filtering**

- **show mac-address-table interface**
- **show mac-address-table notification**
- **show mac-address-table static**
- **show mac-address-table vlan**
- **show address-bind**
- **show mac-address-table mac-manage-learning**

14.2.1 show mac-address-table address

Use this command to show all types of MAC addresses (including dynamic address, static address and filtering address)

show mac-address-table [**address** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
address *mac-addr*	Specified MAC address.
interface *interface-id*	Interface ID
vlan *vlan-id*	VLAN ID

Command mode

Privileged mode.

Command mode

```
DES-7210# show mac-address-table address 00d0.f800.1001
Vlan       MAC Address         Type    Interface
----------  -------------------- --------
1          00d0.f800.1001      STATIC   Gi1/1
```

Related commands

Command	Description
show mac-address-table static	Show the static MAC address.
show mac-address-table filtering	Show the filtering MAC address.
show mac-address-table dynamic	Show the dynamic MAC address.
show mac-address-table interface	Show all types of MAC addresses of the specified interface
show mac-address-table vlan	Show all types of MAC addresses of the specified VLAN
show mac-address-table count	Show the address counts in the MAC address table.

	show mac-address-table static	Show the static MAC address.
	show mac-address-table filtering	Show the filtering MAC address.

14.2.2 show mac-address-table aging-time

Use this command to display the aging time of the dynamic MAC address.

show mac-address-table aging-time

Command mode	Privileged mode.

Examples

```
DES-7210# show mac-address-table aging-time
Aging time   : 300
```

Related commands

Command	Description
mac-address-table aging-time	Specify the aging time of the dynamic MAC address.

14.2.3 show mac-address-table count

Use this command to display the mac-address-table count.

show mac-address-table count

Command mode	Privileged mode.

Examples

```
DES-7210# show mac-address-table count
Dynamic Address Count  : 51
Static  Address Count  : 0
Filter  Address Count  : 0
Total Mac Addresses    : 51
Total Mac Address Space Available: 8139
```

Related commands

Command	Description
show mac-address-table static	Display the static address.
show mac-address-table filtering	Display the filtering address.
show mac-address-table dynamic	Display the dynamic address.

	show mac-address-table address	Display all the address information of the specified address.
	show mac-address-table interface	Display all the address information of the specified interface.
	show mac-address-table vlan	Display all the address information of the specified vlan.

14.2.4 show mac-address-table dynamic

Use this command to show the dynamic MAC address.

show mac-address-table dynamic [**address** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN of the entry
interface-id	Interface that the packet is forwarded to. (It may be a physical port or an aggregate port)

Default configuration

All the MAC addresses are displayed by default.

Command mode

Privileged mode.

Examples

```
DES-7210# show mac-address-table dynamic
Vlan    MAC Address         Type    Interface
------------------------ -------- -------------------
1    0000.0000.0001      DYNAMIC  gigabitethernet 1/1
1    0001.960c.a740      DYNAMIC  gigabitethernet 1/1
1    0007.95c7.dff9      DYNAMIC  gigabitethernet 1/1
1    0007.95cf.eee0      DYNAMIC  gigabitethernet 1/1
1    0007.95cf.f41f      DYNAMIC  gigabitethernet 1/1
1    0009.b715.d400      DYNAMIC  gigabitethernet 1/1
1    0050.bade.63c4      DYNAMIC  gigabitethernet 1/1
```

Related commands

Command	Description
clear mac-address-table dynamic	Clear the dynamic MAC address.

14.2.5 show mac-address-table filtering

Use this command to show the filtering MAC address.

show mac-address-table static [**addr** *mac-addr*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry

Command mode

Privileged mode.

Examples

```
DES-7210# show mac-address-table filtering
Vlan       MAC Address       Type    Interface
-------  ----------------- ------- -----------
  1       0000.2222.2222     FILTER Not available
```

Related commands

Command	Description
clear mac-address-table filtering	Clear the filtering MAC address.
mac-address-table filtering	Configure the filtering MAC address.

14.2.6 show mac-address-table interface

Use this command to show all the MAC address information of the specified interface (including static and dynamic MAC address).

show mac-address-table interface [*interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
interface-id	Show the MAC address information of the specified Interface(physical interface or aggregate port).
vlan-id	Show the MAC address information of the VLAN.

Command mode

Privileged mode.

Examples

```
DES-7210# show mac-address-table interface
gigabitethernet 1/1
```

```
Vlan    MAC Address    Type     Interface
-----  -------------- -------- ----------------
1     00d0.f800.1001  STATIC   gigabitethernet 1/1
1     00d0.f800.1002  STATIC   gigabitethernet 1/1
1     00d0.f800.1003  STATIC   gigabitethernet 1/1
1     00d0.f800.1004  STATIC   gigabitethernet 1/1
```

Related commands

Command	Description
show mac-address-table static	Show the static MAC address.
show mac-address-table filtering	Show the filtering MAC address.
show mac-address-table dynamic	Show the dynamic MAC address.
show mac-address-table address	Show all types of MAC addresses.
show mac-address-table vlan	Show all types of MAC addresses of the specified VLAN.
show mac-address-table count	Show the address counts in the MAC address table.

14.2.7 show mac-address-table notification

Use this command to show the MAC address notification configuration and the MAC address notification table.

show mac-address-table notification [**interface** [*interface-id*] **| history**]

Parameter description

Parameter	Description
interface *interface-id*	Interface ID. Show the MAC address notification configuration on the interface.
history	Show the MAC address notification history.

Default configuration

The MAC address notification configuration is shown by default.

Command mode

Privileged mode.

Examples

```
DES-7210# show mac-address-table notification interface
Interface        MAC Added Trap  MAC Removed Trap
```

```
---------        --------------      --------------
GigabitEthernet1/14   Disabled        Disabled
DES-7210# show mac-address-table notification
MAC Notification Feature: Disabled
Interval between Notification Traps: 1 secs
Maximum Number of entries configured in History Table:1
Current History Table Length: 0
DES-7210# show mac-address-table notification history
History Index: 0
MAC Changed Message:
Operation:ADD Vlan: 1 MAC Addr: 00f8.d012.3456 GigabitEthernet 3/1
```

Related commands

Command	Description
mac-address-table notification	Enable MAC address notification.
snmp trap mac-notification	Enable the MAC address trap notification function on the specified interface.

14.2.8 show mac-address-table static

Use this command to show the static MAC address.

show mac-address-table static [**addr** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry
interface-id	Interface of the entry (physical interface or aggregate port)

Command mode

Privileged mode.

Examples

Show only static MAC addresses

```
DES-7210# show mac-address-table static
Vlan       MAC Address         Type     Interface
----------  -------------------- -------- ---------
1    00d0.f800.1001    STATIC   gigabitethernet 1/1
1    00d0.f800.1002    STATIC   gigabitethernet 1/1
1    00d0.f800.1003    STATIC   gigabitethernet 1/1
```

Related

Command	Description

commands	**mac-address-table static**	Configure the static MAC address.
	clear mac-address-table static	Clear the static MAC address.

14.2.9 show mac-address-table vlan

Use this command to show all types of MAC addresses of the specified VLAN

show mac-address-table vlan [*vlan-id*]

Parameter description	**Parameter**	**Description**
	vlan-id	VLAN ID of the entry

Command mode	Privileged mode.

Examples

```
DES-7210# show mac-address-table vlan 1
Vlan       MAC Address         Type     Interface
----------  -------------------- -------- ---------
1     00d0.f800.1001    STATIC   gigabitethernet 1/1
1     00d0.f800.1002    STATIC   gigabitethernet 1/1
1     00d0.f800.1003    STATIC   gigabitethernet 1/1
```

Related commands	**Command**	**Description**
	show mac-address-table static	Show the static MAC address.
	show mac-address-table filtering	Show the filtering MAC address.
	show mac-address-table dynamic	Show the dynamic MAC address.
	show mac-address-table address	Show all types of MAC addresses.
	show mac-address-table interface	Show all types of MAC addresses of the specified interface.
	show mac-address-table count	Show the address counts in the MAC address table.

14.2.10 show address-bind

Use this command to show IP address-MAC address binding.

show address-bind

Command mode	Privileged mode.
Usage guidelines	N/A.
Examples	DES-7210# **show address-bind** IP Address Binding MAC Addr ------------ ----------------- 3.3.3.3 00d0.f811.1112 3.3.3.4 00d0.f811.1117

Related commands

Command	Description
address-bind	Enable IP address-MAC address binding.

14.2.11 show mac-address-table mac-manage-learning

Use this command to show the management and learning mode of the dynamic MAC address.

Command mode	Privileged mode.
Usage guidelines	N/A.
Examples	DES-7210# show mac-address-table mac-manage-learning ######MAC manage-learning running mode: uniform configuration mode: uniform dynamic address learning-synchronization: off.

	Command	Function
Related commands	**mac-manage-learning uniform**	Set the management and learning mode of the dynamic MAC address to the uniform mode.
	mac-manage-learning uniform learning-synchronization	Synchronize the dynamic MAC address in the whole device.
	mac-manage-learning dispersive	Set the management and learning mode of the dynamic MAC address to the dispersive mode.

15 DHCP Snooping Configuration Commands

15.1 DHCP Snooping Global Commands

The following is the command under the DHCP snooping global mode:

- **ip dhcp snooping**
- **ip dhcp snooping vlan**
- **ip dhcp snooping bootp-bind**
- **ip dhcp snooping verify mac-address**
- **ip dhcp snooping information option**
- **ip dhcp snooping database write-delay**
- **ip dhcp snooping database write-to-flash**

15.1.1 ip dhcp snooping

Use this command to enable the DHCP snooping function globally. The **no** form of this command will disable the DHCP snooping function globally.

[**no**] **ip dhcp snooping**

Parameter description	N/A.
Default	Disabled
Command mode	Global configuration mode

Usage guidelines

Enable the DHCP snooping function on the switch. You can use the **show ip dhcp snooping** command to view whether the DHCP snooping function is enabled.

Note that DHCP Snooping cannot coexist with private VLAN.

Examples

The following is an example of enabling the DHCP snooping function.

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping
DES-7210(config)# end
DES-7210# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping Verification of hwaddr field status: DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface         Trusted         Rate limit (pps)
------------------------  -------    ---------------
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of DHCP snooping.
ip dhcp snooping vlan	Configure DHCP snooping enabled VLAN.

15.1.2 ip dhcp snooping vlan

Use this command to enable DHCP snooping for the specific VLAN. The **no** form of this command will disable the DHCP snooping function for the corresponding VLAN.

[**no**] **ip dhcp snooping vlan** {*vlan-rng* **|** {*vlan-min* [*vlan-max*]}}

Parameter description

Parameter	Description
vlan-rng	VLAN range of effective DHCP snooping.
vlan-min	Minimum VLAN of effective DHCP snooping.
vlan-max	Maximum VLAN of effective DHCP snooping.

Default

By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

Command mode	Global configuration mode.
Usage guidelines	Use this command to configure effective DHCP snooping VLAN by character string.

Examples	The following example enables the DHCP snooping function in VLAN1000.
	`DES-7210# configure terminal`
	`DES-7210(config)# ip dhcp snooping vlan 1000`
	`DES-7210(config)# end`

Related commands

Command	Description
ip dhcp snooping	Global switch of DHCP snooping.

15.1.3 ip dhcp snooping bootp-bind

Use this command to enable DHCP snooping bootp bind function. The **no** form of this command will disable the function.

[**no**] **ip dhcp snooping bootp-bind**

Parameter description	N/A.
Default	Disabled
Command mode	Global configuration mode.
Usage guidelines	By default, the DHCP Snooping only forwards Bootp packets. With this function enabled, it can snoop Bootp packets. After the Boop client requests an address successfully, the DHCP Snooping adds the Bootp user to the static binding database.

Examples	The following example enables the DHCP snooping bootp bind function.
	`DES-7210# configure terminal`
	`DES-7210(config)# ip dhcp snooping bootp-bind`

```
DES-7210(config)# end
DES-7210# show ip dhcp snooping
Switch DHCP snooping status : ENABLE
Verification of hwaddr field status : DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface            Trusted       Rate limit (pps)
-----------------------  -------    ------------
```

Related commands

Command	Description
show ip dhcp snooping	Show the configuration of the DHCP snooping.

15.1.4 ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message. The **no** form of this command disables this function.

[**no**] **ip dhcp snooping verify mac-address**

Parameter description

N/A.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

Use this command to enable checking the validity of the source MAC address of the DHCP request message. Once the function is enabled, the system will discard the DHCP request message that fails to pass the source MAC address check.

Examples

The following is an example of enabling the check of the source MAC address of the DHCP request message.

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping verify mac-address
DES-7210(config)# end
DES-7210# show ip dhcp snooping
```

```
Switch DHCP snooping status: ENABLE
Verification of hwaddr field status: ENABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface        Trusted         Rate limit (pps)
-----------------------  -------   ------------------
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

15.1.5 ip dhcp snooping information option

Use this command to add option82 to the DHCP request message. The **no** form of this command disables this function.

[no] ip dhcp snooping information option

Parameter description

N/A

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines

This command adds option82 to the DHCP request message based on which the DHCP server assigns IP address.

Examples

Add option82 to the DHCP request message:

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping information option
DES-7210(config)# end
DES-7210# show ip dhcp snooping
Switch DHCP snooping  status                 :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time       :   0
DHCP snooping option 82 status               :   DISABLE
```

```
DHCP Snooping Support Bootp bind status: ENABLE
Interface              Trusted      Rate limit (pps)
---------------------- -------      ----------------
```

Related commands

Command	Function
show ip dhcp snooping	Show the configuration of the DHCP Snooping.

15.1.6 ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP snooping binding database into the flash periodically. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping database write-delay** *time*

Parameter description

Parameter	Description
time	The interval at which the system writes the dynamic user information of the DHCP snooping database into the flash.

Default Disabled

Command mode Global configuration mode.

Usage guidelines This function can avoid loss of user information after restart. In that case, users need to obtain IP addresses again for normal communication.

Examples The following is an example of setting interval at which the switch writes the user information into the flash as 3600s:

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping database write-delay 3600
DES-7210(config)# end
DES-7210# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping Verification of hwaddr field status: ENABLE
DHCP snooping database write-delay time: 3600
DHCP snooping option 82 status: DISABLE
DHCP Snooping Support Bootp bind status: ENABLE
```

```
Interface          Trusted          Rate limit (pps)
-----------------------  -------     ---------------
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

15.1.7 ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

ip dhcp snooping database write-to-flash

Parameter description N/A.

Default N/A.

Command mode Global configuration mode.

Usage guidelines Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

Examples The following is an example of writing the dynamic user information of the DHCP binding database into flash.

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping database write-to-flash
DES-7210(config)# end
DES-7210#
```

Related commands N/A.

15.2 DHCP snooping Interface Mode Commands

There are several commands under the DHCP snooping interface mode as follows:

- **ip dhcp snooping suppression**
- **ip dhcp snooping trust**

- **ip dhcp snooping limit rate**

15.2.1 ip dhcp snooping suppression

Use this command to set the port to be the suppression status. The no form of this command will set the port to be no suppression status.

[**no**] **ip dhcp snooping trust**

Parameter description	N/A.
Default	Disabled
Command mode	Interface configuration mode.
Usage guidelines	This command can deny all DHCP request messages under the port, that is, all the users under the port are prohibited to request addresses through DHCP.

Examples	The following is an example of setting **fastethernet** 0/2 to be suppression status:
	`DES-7210# configure terminal`
	`DES-7210(config)# interface fastEthernet 0/2`
	`DES-7210(config-if)# ip dhcp snooping suppression`
	`DES-7210(config-if)# end`

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

15.2.2 ip dhcp snooping trust

Use this command to set the ports of the switch as trusted ports. The no form of this command sets the ports as untrust ports.

[**no**] **ip dhcp snooping trust**

Parameter description	N/A.
Default	All ports are untrust ports.

Command mode	Interface configuration mode.
Usage guidelines	Use this command to set the port as trust port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrust port will be discarded.

Examples	The following is an example of setting **fastEthernet** *0/1* as a trust port:
	`DES-7210# configure terminal`
	`DES-7210(config)# interface fastEthernet 0/1`
	`DES-7210(config-if)# ip dhcp snooping trust`
	`DES-7210(config-if)# end`
	`DES-7210# show ip dhcp snooping`
	`Switch DHCP snooping status: ENABLE`
	`DHCP snooping Verification of hwaddr field status: DISABLE`
	`DHCP snooping database write-delay time: 0 seconds`
	`DHCP snooping option 82 status: ENABLE`
	`DHCP Snooping Support Bootp bind status:ENABLE`
	`Interface Trusted Rate limit (pps)`
	`----------- ------- ----------`
	`FastEthernet0/1 yes unlimited`

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

15.2.3 ip dhcp snooping limit rate

Use this command to set rate limit of receiving DHCP packets on the interface. The **no** form of this command removes the setting.

[**no**] **ip dhcp snooping limit rate** *rate-value*

Parameter description

Parameter	Description
rate-value	Rate of receiving DHCP packets (pps).

Default	No rate limit.

Command mode	Interface configuration mode.
Usage guidelines	This function takes effect for all the interfaces of the VLAN controlled by the DHCP Snooping, including trust interface. For some CPP-enabled products, CPP will restrict the rate of DHCP packets by hardware. CCP-based rate limit takes precedence over DHCP Snooping-based rate limit. For CPP, please refer to specific chapters. You can view the rate limit setting on the corresponding interface by **show ip dhcp snooping** command. Note that DES-7200 does not support rate limit of DHCP packets on an interface.

Examples

The following example sets rate limit of port 1 as 100:

```
DES-7210# configure terminal
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# ip dhcp snooping limit rate 100
DES-7210(config-if)# end
DES-7210# show ip dhcp snooping
Switch DHCP snooping  status: ENABLE
DHCP snooping  Verification of hwaddr field status: DISABLE
DHCP snooping database write-delay time:0 seconds
DHCP snooping option 82 status:ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                Trusted      Rate limit (pps)
-----------------------  -------      ----------------
GigabitEthernet 0/1         NO              100
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

15.3 Showing Related Commands

- **show ip dhcp snooping**
- **show ip dhcp snooping binding**

15.3.1 show ip dhcp snooping

Use this command to view the setting of the DHCP snooping.

show ip dhcp snooping

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples	Show the information of DHCP Snooping.
	`DES-7210# show ip dhcp snooping`
	`Switch DHCP snooping status : ENABLE`
	`Verification of hwaddr field status : DISABLE`
	`DHCP snooping database write-delay time: 0 seconds`
	`DHCP snooping option 82 status: ENABLE`
	`DHCP snooping Support Bootp bind status: ENABLE`
	`Interface Trusted Rate limit (pps)`
	`------------------------ ------- ------------`

Related commands

Command	Description
ip dhcp snooping	Enable the DHCP snooping globally.
ip dhcp snooping verify mac-address	Enable the check of source MAC address of DHCP Snooping packets.
ip dhcp snooping write-delay	Set the interval of writing user information to FLASH periodically.
ip dhcp snooping information option	Add option82 to the DHCP request message.
ip dhcp snoooping bootp-bind	Enable the DHCP snooping bootp bind function.
ip dhcp snooping trust	Set the port as a trust port.

15.3.2 show ip dhcp snooping binding

Use this command to view the information of the DHCP snooping binding database.

show ip dhcp snooping binding

Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples	Show the information of the DHCP Snooping binding database.
	`DES-7210# show ip dhcp snooping binding`
	`Total number of bindings: 1`
	`MacAddress IpAddress Lease Type VLAN Interface`
	`00d0.f801.0101 192.168.1.1 - static 1 fastethernet 0/1`

Related commands

Command	Description
ip dhcp snooping binding	Add the static user information to the DHCP Snooping database.
clear ip dhcp snooping binding	Clear the dynamic user information from the DHCP snooping binding database.

15.4 Other DHCP Snooping Configuration Commands

The configuration of other dhcp snooping includes the commands as follows:

- **clear ip dhcp snooping binding**
- **debug ip dhcp snooping**

15.4.1 clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP snooping binding database.

clear ip dhcp snooping binding

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.

Usage guidelines	If users want to clear the current dynamic user information from the DHCP snooping binding database, use this command.

Examples

The following example demonstrates how to clear the dynamic database information from the DHCP snooping binding database.

```
DES-7210# clear ip dhcp snooping binding
DES-7210# show ip dhcp snooping binding
Total number of bindings: 0
MacAddress IpAddress Lease(sec) Type VLAN Interface
---------- ---------- ---------- -------- ---- ---------
```

Related commands

Command	Description
show ip dhcp snooping binding	Show the information of the DHCP snooping binding database.

15.4.2 debug ip dhcp snooping

Use this command to trun on the debugging switch of the DHCP snooping.

debug ip dhcp snooping

Default	Turned off
Command mode	Privileged EXEC mode.

Examples

The following example demonstrates how to turn on the debugging switch of the DHCP snooping.

```
DES-7210# debug ip dhcp snooping
DES-7210# show ip dhcp snooping binding
```

16 IGMP Snooping Configuration Commands

16.1 Configuration Related Commands

IGMP Snooping includes the commands in the profile configuration mode and the global configuration mode respectively.

Commands in the Profile configuration mode include:

- **deny**
- **permit**
- **range**

Commands in the global configuration mode include:

- **ip igmp profile**
- **ip igmp snooping dyn-mr-aging-time**
- **ip igmp snooping fast-leave enable**
- **ip igmp snooping filter**
- **ip igmp snooping ivgl**
- **ip igmp snooping ivgl-svgl**
- **ip igmp snooping limit-ipmc vlan server**
- **ip igmp snooping max-groups**
- **ip igmp snooping query-max-response-time**
- **ip igmp snooping source-check default-server**
- **ip igmp snooping source-check port**
- **ip igmp snooping suppression enable**
- **ip igmp snooping svgl**
- **ip igmp snooping svgl profile**
- **ip igmp snooping vlan mrouting interface**
- **ip igmp snooping vlan mrouting interface profile**

- **ip igmp snooping vlan mdevice learn pim-dvmrp**
- **ip igmp snooping vlan static interface**

16.1.1 deny

To deny the forwarding of the multicast streams in the range specified by the profile, execute the **deny** configuration command in the profile configuration mode.

deny

Parameter description	N/A
Default	The forwarding of the multicast streams in the range specified by the profile is denied.
Command mode	Profile configuration mode.
Usage guidelines	First, configure the multicast range using the **range** command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Examples	The following is an example of deny the forwarding of the multicast stream 224.2.2.2:
	`DES-7210(config)# ip igmp profile 1`
	`DES-7210(config-profile)# range 224.2.2.2`
	`DES-7210(config-profile)# deny`

Related commands

Command	Description
ip igmp profile	Create a profile.
range	Configure the multicast address range.

16.1.2 permit

To permit the forwarding of the multicast streams in the range specified by the profile, execute the **permit** command in the profile configuration mode. In this way, the interface associated with this profile will forward the specified multicast stream only.

permit

Parameter description	N/A
Default	The forwarding of the multicast streams in the range specified by the profile is denied.
Command mode	Profile configuration mode.
Usage guidelines	First, configure the multicast range using the **range** command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration to take effective.

Examples	The following is an example of allowing the forwarding of the multicast stream 224.2.2.2:
	`DES-7210(config)# ip igmp profile 1`
	`DES-7210(config-profile)# range 224.2.2.2`
	`DES-7210(config-profile)# permit`

Related commands

Command	Description
ip igmp profile	Create a profile.
range	Configure the multicast address range.

16.1.3 range

To specify the range of multicast streams, execute the **range** command in the profile configuration mode. You can specify either a single multicast address or a range of multicast addresses. Use the **no** form of the command to remove the specified multicast IP address.

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter description

Parameter	Description
low-ip-address	Start address of a range
high-ip-address	End address of a range

Default	N/A.

Command mode

Profile configuration mode.

Usage guidelines

You can specify a behavior after configuring the address range, for example deny by default. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Examples

The following is an example of creating a profile whose multicast stream is in the range 224.2.2.2 to 224.2.2.244:

```
DES-7210(config)# ip igmp profile 1
DES-7210(config-profile)# range 224.2.2.2 224.2.2.244
```

Related commands

Command	Description
ip igmp profile	Create a profile.
deny	Deny the forwarding of the multicast streams in the range specified by the profile.
permit	Permit the forwarding of the multicast streams in the range specified by the profile.

16.1.4 ip igmp profile

This is a mode navigation command. Use this command to select a profile and enter the IGMP profile configuration mode.

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

Parameter description

Parameter	Description
profile-number	Profile number, in the range from 1 to 65535

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

The profile must be applied to the specified interface in order to make the profile take effect.

Examples

The following is an example of creating a profile numbered 1 and entering the profile configuration mode.

```
DES-7210(config)# ip igmp profile 1
DES-7210(config-profile)#
```

Related commands

Command	Description
range	Configure the multicast address range.

16.1.5 ip igmp snooping dyn-mr-aging-time

To configure the aging time of the routing interface that the switch learns dynamically, execute the **ip igmp snooping dyn-mr-aging-time** command .

ip igmp snooping dyn-mr-aging-time *time*

no ip igmp snooping dyn-mr-aging-time

Parameter description

Parameter	Description
time	Aging time of the routing interface that the switch learns dynamically

Default configuration

300s.

Command mode

Global configuration mode.

Usage guidelines

When the dynamic routing interface learning function is enabled, this command sets the aging time of the routing interface. If the aging time is set too short, the routes may be added and deleted frequently.

Examples

Set the aging time of the routing interface that the switch learns dynamically to 100 s:

```
DES-7210(config)# ip igmp snooping dyn-mr-aging-time 100
```

Related commands

Command	Function
ip igmp snooping	Enable IGMP snooping.

16.1.6 ip igmp snooping fast-leave enable

To enable the fast leave function, execute the **ip igmp snooping fast-leave enable** command in the global configuration mode. The **no** form of this command is used to disable the function.

ip igmp snooping fast-leave enable

no ip igmp snooping fast-leave enable

Parameter description

Parameter	Description
N/A	

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines

After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message.

Examples

The following example shows how to enable the fast leave function on the switch:

```
DES-7210(config)# ip igmp snooping fast-leave
```

Related commands

Command	Function
N/A	

16.1.7 ip igmp snooping filter

To configure a port to receive a specific set of multicast streams, execute the **ip igmp snooping filter** command in the interface configuration mode to associate the port to a specific profile. The **no** form of this command is used to delete the associated profile.

ip igmp snooping filter *profile-number*

no ip igmp snooping filter *profile-number*

Parameter description

Parameter	Description
profile-number	Profile number

Default N/A.

Command mode Interface configuration mode.

Usage guidelines A specific profile must be created before association.

Examples The following example demonstrates how to associate profile 1 to a megabit port 0/1:

```
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# ip igmp snooping filter 1
```

Related commands

Command	Description
ip igmp profile	Create a profile.

16.1.8 ip igmp snooping ivgl

To enable IGMP snooping and enter the IVGL mode, execute the **ip igmp snooping ivgl** command in the global configuration mode. The **no** form of this command is used to disable IGMP snooping.

ip igmp snooping ivgl

no ip igmp snooping

Parameter description N/A.

Default Disabled.

Command mode Global configuration mode.

Usage guidelines After this mode is set, for multicast frames with the same multicast address yet in different VLANs, the **IGMP snooping** function handles only the same group as that in the multicast address table (GDA),

	other multicast frames are forwarded.
Examples	The following example demonstrates how to enable IGMP snooping and enter the IVGL mode: `DES-7210(config)# ip igmp snooping ivgl`

Related commands

Command	Description
ip igmp snooping svgl	Enable **igmp snooping** and enter the SVGL mode.
ip igmp snooping ivgl-svgl	Enable **igmp snooping** and enter the **hybrid** mode.

16.1.9 ip igmp snooping ivgl-svgl

To enable IGMP snooping and enter the ivgl-svgl mode, execute the **ip igmp snooping ivgl-svgl** command in the global configuration mode. The **no** form of this command is used to disable IGMP snooping.

ip igmp snooping ivgl-svgl

no ip igmp snooping

Parameter description	N/A.
Default	Disabed.
Command mode	Global configuration mode.
Usage guidelines	After this mode is set, IVGL and SVGL coexist.
Examples	The following example demonstrates how to enable IGMP snooping and enter the ivgl-svgl mode on the device: `DES-7210(config)# ip igmp snooping ivgl-svgl`

Related commands

Command	Description
ip igmp snooping svgl	Enable **igmp snooping** and enter the SVGL mode.

	ip igmp snooping ivgl	Enable **igmp snooping** and enter the IVGL mode.

16.1.10 ip igmp snooping limit-ipmc vlan server

To add a multicast source IP address check entry, execute the **ip igmp snooping limit-ipmc vlan** command in the global configuration mode. The **no** form of this command is used to delete a source IP checklist entry.

ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

no ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

Parameter description

Parameter	Description
Vid	VLAN ID of the source IP address check entry
Gaddress	Multicast address
Saddress	Multicast source IP address (multicast server)

Default N/A.

Command mode Global configuration mode.

Usage guidelines The source IP address check function must be enabled before an entry can be added.

Examples The following is an example of adding an entry to the multicast source IP address check table.

```
DES-7210(config)# ip igmp snooping limit-ipmc vlan 1 address 224.0.0.1 server 192.168.4.243
```

Related commands

Command	Description
ip igmp snooping source-check default-server	Configure a default source IP address while enabling the IP check function.

16.1.11 ip igmp snooping max-groups

To configure the maximum number of groups that can be added dynamically to this interface, execute the **ip igmp snooping max-groups** command in the interface configuration mode. The **no** form of this command is used to remove the configuration.

ip igmp snooping max-groups *number*

no ip igmp snooping max-groups

Parameter description

Parameter	Description
number	The parameter ranges 0 to 4294967294.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines If a maximum number of multicast groups are configured, the device will no longer receive and process IGMP Report messages when the number of multicast groups on this interface is beyond the range.

Examples The following example shows how to configure the maximum number of multicast groups to 100 on the megabit interface 0/1:

```
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# ip igmp snooping max-group 100
```

Related commands

Command	Description
ip igmp snooping filter	Filter multicast groups that pass through a port.

16.1.12 ip igmp snooping query-max-response-time

This command specifies the time for the switch to wait for the member join message after receiving the **query** message. If the switch does not receive the member join message within the specified time, it considers that the member has left and then deletes the member.

ip igmp snooping query-max-response-time *time*

no ip igmp snooping query-max-resposne-time

Parameter description

Parameter	Description
time	The aging time of the routing inerface that the switch learns dynamically.

Default configuration	10s.
Command mode	Global configuration mode.
Usage guidelines	You can specify the time for the switch to wait for the member join message after receiving the **query** message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member. This command lets you adjust the waiting time after receiving the **query** message.
Examples	Set the aging time of the routing interface that the switch learns dynamically to 100s. `DES-7210(config)# ip igmp snooping query-max-response-time 100`

Related commands

Command	Function
ip igmp snooping	Configure a multicast routing interface.

16.1.13 ip igmp snooping source-check default-server

The source IP address check is used to permit one or several IPMC flows from the server of the specified IP address.

To configure the source IP address check function of IGMP snooping, execute the **ip igmp snooping source-check default-server** command in the global configuration mode. The **no** form of this command is used to disable the source IP address check function.

ip igmp snooping source-check default-server *address*

no ip igmp snooping souce-check

Parameter description

Parameter	Description
address	Default multicast source IP address (IP address of the default multicast server)

Default	Disabled.

Command mode	Global configuration mode.
Usage guidelines	The source IP address check function takes effect globally. Once it is enabled, only the IPMC streams from the specified IP address are permitted. The device allows users to configure the source IP address of all IPMC streams, called default multicast server. The default server must be set as long as the source IP address check function is enabled.
Examples	The following example shows how to enable the multicast source IP address check function and configure a default source IP address. `DES-7210(config)# ip igmp snooping source-check default-server 192.168.4.243`

Related commands

Command	Description
Ip igmp snooping limit-ipmc vlan server	Add an entry to the source IP check table.

16.1.14 ip igmp snooping source-check port

The source port check function is used to permit one or several IPMC flows from the mroute port.

To configure the source port check function of IGMP snooping, execute the **ip igmp snooping source-check port** command in the global configuration mode. The no form of this command is used to disable the source port check function.

ip igmp snooping source-check port

no ip igmp snooping source-check port

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The source port check function takes effect globally. Once it is enabled, only the IPMC streams from the specified port are permitted.

Examples	The following example shows how to enable the source port check function of IGMP snooping. `DES-7210(config)# ip igmp snooping source-check port`

Related commands	**Command**	**Description**
	Ip igmp snooping source-check default-server	Enable the multicast source IP address check function.

16.1.15 ip igmp snooping suppression enable

To enable IGMP snooping suppression, execute the **ip igmp snooping suppression enable** command in the global configuration mode.The **no** form of this command is used to disable IGMP snooping suppression..

ip igmp snooping suppression enable

no ip igmp snooping suppression enable

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	After you execute this command to enable the suppression function, the switch begins to suppress the **IGMP v1/v2** report messages.
Examples	The following example shows how to enable IGMP snooping suppression on the device: `DES-7210(config)# ip igmp snooping suppression`
Related commands	N/A

16.1.16 ip igmp snooping svgl

To enable IGMP snooping and enter the SVGL mode, execute the **ip igmp snooping svgl** command in the global configuration mode. The **no** form of this command is used to disable IGMP snooping.

ip igmp snooping svgl

no ip igmp snooping

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The SVGL works only when the multicast IP address range is configured.
Examples	The following example demonstrates how to enable IGMP snooping and enter the SVGL mode: `DES-7210(config)# ip igmp snooping svgl`

Related commands

Command	Description
ip igmp snooping ivgl	Enable **igmp snooping** and enter the IVGL mode.
ip igmp snooping ivgl-svgl	Enable **igmp snooping** and enter the hybrid mode

16.1.17 ip igmp snooping svgl profile

To specify the multicast group address range applied in the SVGL/IVGL-SVGL mode, execute the **ip igmp snooping profile** *profile-number* command in the global configuration mode. Use the **no ip igmp snooping profile** command to cancel the association.

ip igmp snooping profile *profile-number*

no ip igmp snooping profile

Parameter description

Parameter	Description
profile-number	Profile number, in the range of 1-65535.

Default No profile is associated.

Command mode Global configuration mode.

Usage guidelines When the IGMP Snooping works in the SVGL or IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode. That is to say, the member ports of the multicast forwarding entry can be forwarded across the VLANs while the member ports of the multicast forwarding entry in the other multicast address range must belong to the same VLAN. By default, no profile is associated.

Examples

```
DES-7210(config)# ip igmp snooping svgl profile 1
```

Related commands

Command	Description
ip igmp snooping ivgl	Enable **igmp snooping** and enter the IVGL mode.
ip igmp snooping ivgl-svgl	Enable **igmp snooping** and enter the hybrid mode

16.1.18 ip igmp snooping vlan mrouting interface

Routing interface is a port through which a multicast device is directly connected to a multicast neighbouring device. To configure a multicast routing interface, execute the **ip igmp snooping vlan mrouting interface** command in the global configuration mode. The **no** form of this command is used to delete a routing interface.

ip igmp snooping vlan *vid* **mrouting interface** *interface-id*

no ip igmp snooping vlan *vid* **mrouting interface** *interface-id*

Parameter description

Parameter	Description
vid	VLAN ID of a routing interface
interface-id	Interface ID

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.
Examples	The following example demonstrates how to configure a multicast routing interface on the equipment: `DES-7210(config)# ip igmp snooping vlan 1 mrouting interface fastEthernet 0/1`

Related commands

Command	Description
ip igmp snooping source-check port	Enable the multicast source port check function.

16.1.19 ip igmp snooping vlan mrouting interface profile

By deffault, the routing interface forwards the multicast frames of all the mlticast IP addresses in the VLAN as a member of a VLAN. Sometimes administrator does not want to forward some multicast frames to a multicast device. At this point, the administrator can use the IGMP Profile to filter the range of multicast frames to be forwarded by the routing interface by executing the **ip igmp snooping vlan mdevice interface profile** command in the global configuration mode. The **no** form of this command is used to eliminate the association between a port and a profile.

ip igmp snooping vlan *vid* **mdevice interface** *interface-id* **profile** *profile-num*

no ip igmp snooping vlan *vid* **mdevice interface** *interface-id* **profile**

Parameter description

Parameter	Description
vid	VLAN ID of a routing interface
interface-id	Interface ID
profile-num	Profile number

Default	N/A.

Command mode	Global configuration mode.
Usage guidelines	A profile must be created first. After association, only the multicast frames complying with this profile can be forwarded to this routing interface.
Examples	The following example demonstrates how to associate a profile to a multicast routing interface: `DES-7210(config)# ip igmp snooping vlan 1 mdevice interface fastEthernet 0/1 profile 1`

Related commands

Command	Description
ip igmp snooping vlan mdevice interface	Configure a multicast routing interface.

16.1.20 ip igmp snooping vlan mdevice learn pim-dvmrp

To configure a device to listen to the IGMP query/dvmrp or PIM packets dynamically in order to automatically identify a routing interface, execute the **ip igmp snooping vlan mdevice learn** command in the global configuration mode. The **no** form of this command is used to disable the dynamic learning.

ip igmp snooping vlan *vid* **mdevice learn pim-dvmrp**

no ip igmp snooping vlan *vid* **mdevice learn pim-dvmrp**

Parameter description

Parameter	Description
vid	VLAN ID of a routing interface

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.
Examples	The following example demonstrates how to enable the dynamic

routing interface learning function on the equipment:

```
DES-7210(config)# ip igmp snooping vlan 1 mdevice learn pim-dvmrp
```

Related commands

Command	Description
ip igmp snooping vlan *vid* **mdevice learn pim-dvmrp**	Enable the dynamic routing interface learning function on the multicast routing port.

16.1.21 ip igmp snooping vlan static interface

Once IGMP snooping is enabled, a port can receive a certain multicast frame without being afftected by various IGMP messges by executing the **ip igmp snooping vlan static interface** command in the global configuration mode. The **no** form of this command is used to delete a static configuration.

ip igmp snooping vlan *vid* **static** ip-addr **interface** *interface-id*

no ip igmp snooping vlan *vid* **static** *ip-addr* **interface** *interface-id*

Parameter description

Parameter	Description
vid	VLAN ID of a routing interface
ip-addr	Multicast IP address
interface-id	Interface ID

Default N/A.

Command mode Global configuration mode.

Usage guidelines Multiple multicast IP addresses can be configured for an interface.

Examples

The following example demonstrates how to configure a static multicast address on a port:

```
DES-7210(config)# ip igmp snooping vlan 1 static 224.0.0.2 interface fastEthernet 0/1
```

Related commands

Command	Description
ip igmp snooping vlan mdevice interface	Configure a multicast routing interface

16.2 Displaying and Monitoring Commands

It includes the following commands:

- **show ip igmp snooping [gda-table | interface | mdevice]**
- **show ip igmp profile** [*profile-number*]
- **clear ip igmp snooping gda-table**
- **clear ip igmp snooping statistics**
- **debug igmp-snp**

16.2.1 show ip igmp snooping

Use this command to show related information of igmp snooping.

show ip igmp snooping [**gda-table** | **interfaces** | **mdevice**| **statistics** [**vlan** *vlan-id*]]

	Parameter	Description
Parameter description	*none*	Show the function configuration of IGMP snooping.
	gda-table	Show multicast forwarding rule table.
	interfaces	Show the configuration of igmp snooping filtring
	mdevice	Show interface configuration of multicast device.
	statistics [**vlan** *vlan-id*]	Show the igmp snooping statistics.

Command mode	Privileged EXEC mode.

Examples

The following example demonstrates how to process 100 multicast group on the interface fa0/1:

```
DES-7210(config-if)# ip igmp snooping gda-table
Abbr:M - mrouter
D – dynamic
S – static
VLAN    Address          Member ports
----------------------------------------
1      233.3.3.3         Gi0/2(S)
2      234.4.4.4         Gi0/11(S)
1      233.4.4.4         Ag2(S)
```

16.2.2 show ip igmp profile [profile-number]

Use this command to show the profile information.

show ip igmp profile

show ip igmp profile *profile-number*

Parameter description

Parameter	Description
none	Show configuration information of all profiles.
profile-number	Show configuration information of the designated profile.

Command mode

Privileged EXEC mode.

Examples

```
DES-7210(config-if)# show ip igmp profile
Profile    1
Permit
range 224.0.1.0,   239.255.255.255
```

16.2.3 clear ip igmp snooping gda-table

Use this command to clear the forwarding information dynamically learned.

clear ip igmp snooping gda-table

Parameter

N/A

description	
Command mode	Privileged EXEC mode.

16.2.4 clear ip igmp snooping statistics

Use this command to clear the statistics dynamically learned.

clear ip igmp snooping statistics

Parameter description	N/A
Command mode	Privileged EXEC mode.

16.2.5 debug igmp-snp

Use the following commands to turn on igmp service debug switch. The **no** form of this command closes debug switch.

debug igmp-snp

debug igmp-snp event

debug igmp-snp packet

debug igmp-snp msf

debug igmp-snp warning

undebug igmp-snp

undebug igmp-snp event

undebug igmp-snp packet

undebug igmp-snp msf

undebug igmp-snp warning

Parameter description

Parameter	Description
none	Show all debug information of IGMP Snooping.
event	Show the debug information of IGMP Snooping event.

packet	Show the debug information of IGMP Snooping packet.
msf	Show the debug information exchanged between the IGMP Snooping and multicast.
warning	Show all debug information of IGMP Snooping warning.

Command mode	Privileged EXEC mode.

17 PIM Snooping Configuration Commands

17.1 Configuration Related Command

PIM SNOOPING configuration includes following commands:

- **ip pim snooping** (global configuration mode)
- **ip pim snooping dr-flood**
- **ip pim snooping** (interface configuration mode)
- **show ip pim snooping**
- **show ip pim snooping mroute**
- **show ip pim snooping neighbor**
- **show ip pim snooping statistics**
- **show ip pim snooping vlan**
- **clear ip pim snooping statistics**
- **clear ip pim snooping vlan**
- **debug ip psnp event**
- **debug ip psnp mst**
- **debug ip psnp port**
- **debug ip psnp timer**

17.1.1 ip pim snooping (global configuration mode)

This command enables or disables the PIM snooping globally.

ip pim snooping

no ip pim snooping

Parameter description	N/A
Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	DES-7210# **configure terminal** DES-7210(config)# **ip pim snooping**

Note

Before enabling PIM Snooping, enable IGMP Snooping in the global configuration mode. Or it fails to set up the Layer 2 forward entry of the multicast flow between the routers, even if the PIM Snooping has been enabled.

If you disable PIM Snooping globally, then the PIM Snooping function will be ineffective in all VLANs.

17.1.2 ip pim snooping dr-flood

Use the **ip pim snooping dr-flood** command to enable PIM Snooping to flood the multicast flow towards DR. With DR flood configured, the multicast data will be forwarded through the Layer 2 port, no matter whether the Join packets are received on the port towards DR or not.

Use the **no** form of this command to disable the DR flood function.

ip pim snooping

no ip pim snooping

Parameter description	N/A
Default configuration	Enabled.

Command mode	Global configuration mode.

Examples

```
DES-7210# configure terminal
DES-7210(config)# ip pim snooping dr-flood
```

Note If the multicast source exists in the VLAN, to enable the DR to send the registered packets to the RP, the multicast flow must be flooded to DR. To this end, DR flood function is disabled only when the multicast source does not exist in the VLAN.

17.1.3 ip pim snooping (interface configuration mode)

This command enables or disables the PIM snooping on the interface.

ip pim snooping

no ip pim snooping

Parameter description	N/A
Default configuration	Disabled.
Command mode	Interface configuration mode.

Examples

```
DES-7210# configure terminal
DES-7210(config)# interface vlan 199
DES-7210(config-if)# ip pim snooping
```

Note If you disable PIM Snooping globally, then the PIM Snooping function will be ineffective in all VLANs.

17.1.4 show ip pim snooping

Use this command to show global configuration information of PIM snooping.

show ip pim snooping [detail]

Parameter description

Parameter	Description
detail	Show the detailed information.

Command mode

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

Examples

The following example shows the global configuration information of the PIM snooping function:

```
DES-7210# show ip pim snooping
Global runtime mode       : Enabled
Global admin mode     : Enabled
DR Flooding status        : Enabled
Number of user enabled VLANs: 2
User enabled VLANs: 199 198
```

The following are the description for each field:

Field	Description
Global runtime mode	Global PIM Snooping running mode. **Enabled** indicates the current normal running mode; **Disabled** indicates the current unavailable running mode.
Global admin mode	Global PIM Snooping configuration mode. **Enabled** indicates the global PIM Snooping has been enabled. **Disabled** indicates the global PIM Snooping has been disabled.
DR Flooding status	DR Flooding status. **Enabled** indicates this function has been enabled. **Disabled** indicates this function has been disabled.

Number of user enabled VLANs	Configure the PIM Snooping VLAN numbers.
User enabled VLANs	The configured PIM Snooping VLAN lists.

17.1.5 show ip pim snooping mroute

Use this command to display the PIM Snooping forwarding entry information.

show ip pim snooping mroute [*A.B.C.D A.B.C.D***]**

Parameter description

Parameter	Description
A.B.C.D A.B.C.D	The group address and the source address for the entry.

Command mode

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

Examples

The following example shows the information of the PIM snooping forwarding entry:

```
DES-7210#show ip pim snooping mroute
Flags:  JOIN/PRUNE - (*,G), (S,G) Join/Prune
SGR-PP - (S,G,R) PrunePending, SGR-P - (S,G,R) Prune

VLAN 199: 1 mroutes
(*, 229.1.1.1), 00:06:12/00:03:06
214.199.199.10 -> 214.199.199.2, 00:06:12/00:03:06, JOIN
Downstream ports: 2/20
Upstream  ports: 2/32
Outgoing  ports: 2/32 2/20
```

The following are the description for each field:

Field	Description
Downstream ports	The downstream Layer 2 ports.
Upstream ports	The upstream Layer 2 ports
Outgoing ports	The outgoing ports for the multicast flow.

17.1.6 show ip pim snooping neighbor

Use this command to display the PIM Snooping neighbor information.

show ip pim snooping neighbor

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode.

Examples

The following example shows the information of the PIM snooping neighbor:

```
DES-7210#show ip pim snooping neighbor
IP Address      Port   Uptime/Expires   Flags
VLAN 199: 2 neighbors
214.199.199.2    2/32  00:18:25/00:01:04
214.199.199.10   2/20  00:18:09/00:01:03  DR
```

The following are the description for each field:

Field	Description
IP Address	The neighbor IP address.
Port	The Layer 2 port connecting to the neighbor.
Uptime/Expires	The creating and aging time of the neighbor.
Flags	Explain whether DR or not.

17.1.7 show ip pim snooping statistics

Use this command to display the PIM Snooping statistics.

show ip pim snooping statistics

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode.

Examples

The following example shows the information of the PIM snooping statistics:

```
DES-7210#show ip pim snooping statistics
PIMv2 statistics:
Process Enqueue          : 2954
Process PIMv2 input queue max size reached    : 4
Error - Process Enqueue            : 0
Error - Drops                  : 0
Error - IP header generic error        : 0
Error - IP header dest ip not 224.0.0.13        : 0
Error - PIM header payload len too short        : 0
Error - PIM header checksum                : 0
Error - PIM header version not 2           : 0
```

17.1.8 show ip pim snooping vlan

Use this command to display related information of PIM-Snooping VLAN.

show ip pim snooping vlan *interface-number* **[mroute] [neighbor] [statistics]**

Parameter description

Parameter	Description
interface-number	Show VLAN ID.
mroute	Show the forwarding table information in the VLAN.
neighbor	Show the neighbor information in the VLAN.
statistics	Show the statistics in the VLAN.

Command mode

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

Examples

The following example shows the information of the PIM Snooping VLAN 199:

```
DES-7210# show ip pim snooping vlan 199
4 neighbors (0 DR priority incapable)
1 mroutes
DR is 214.199.199.4
```

The following example shows the forwarding table information of the PIM Snooping VLAN 199:

```
DES-7210# show ip pim snooping vlan 199
mroute
Flags:    JOIN/PRUNE - (*,G), (S,G)
Join/Prune
SGR-PP - (S,G,R) PrunePending, SGR-P -
(S,G,R) Prune

VLAN 199: 1 mroutes
(*, 229.1.1.1), 02:09:51/00:02:41
214.199.199.4 -> 214.199.199.1,
02:09:41/00:02:41, JOIN
Downstream ports: 2/32
Upstream  ports: 2/34
Outgoing  ports: 2/32 2/34
```

The following example shows the neighbor information of the PIM Snooping VLAN 199:

```
DES-7210# show ip pim snooping vlan 199
neighbor
IP Address      Port   Uptime/Expires
Flags
VLAN 199: 4 neighbors
214.199.199.4   2/32   02:34:58/00:01:17
DR
214.199.199.3   2/36   02:22:19/00:05:10
214.199.199.2   2/34   02:33:34/00:05:35
214.199.199.1   2/20   02:34:59/00:01:26
```

The following example shows thestatistics of the PIM Snooping VLAN 199:

```
DES-7210# show ip pim snooping vlan 199
statistics
PIMv2 statistics for vlan 199:
Hello                                 :
23
Join/Prunes                           :
```

```
22
Other types                              :
24
Hello option holdtime [1]
 : 23
Hello option DR priority
[19]                : 23
Hello option Generation ID
[20]             : 23
Hello option Lan Prune Delay
[2]             : 19

Join/Prune not
modified                   : 11
Join/Prune
modified                        : 5
Join/Prune suppressed                  :
1

Error - Hello hold option missing
 : 0
Error - Hello option
length                  : 0
Error - Hello option
unknown               : 4

Error - Join/Prune Address
Family           : 0
Error - Join/Prune Unknown up/down neighbor
 : 5
```

17.1.9 clear ip pim snooping statistics

Use this command to clear the PIM Snooping statistics.

clear ip pim snooping statistics

Parameter description	N/A
Command mode	Privileged EXEC mode.

Examples

The following example clear the PIM Snooping statistics:

```
DES-7210#clear ip pim snooping statistics
```

17.1.10 clear ip pim snooping vlan

Use this command to clear a PIM Snooping VLAN.

clear ip pim snooping vlan *interface-number* **[mroute] [neighbor] [statistics]**

Parameter description

Parameter	Description
interface-number	Clear VLAN ID.
mroute	Clear the forwarding table information in the VLAN.
neighbor	Clear the neighbor information in the VLAN.
statistics	Clear the statistics in the VLAN.

Command mode

Privileged EXEC mode.

Examples

The following example clears the forwarding table information of the PIM Snooping VLAN 199:

```
DES-7210# show ip pim snooping vlan 199
mroute *
```

The following example clears the neighbor information of the PIM Snooping VLAN 199:

```
DES-7210# show ip pim snooping vlan 199
neighbor *
```

The following example clears the statistics of the PIM Snooping VLAN 199:

```
DES-7210# show ip pim snooping vlan 199
statistics *
```

17.1.11 debug ip psnp event

Use this command to enable the PIM Snooping event debugging switch. Use the **no** form of this command to disable the switch.

debug ip psnp event

no debug ip psnp event

Parameter description	N/A
Command mode	Privileged EXEC mode.
Examples	The following example enable the PIM Snooping event debugging switch: `DES-7210#debug ip psnp event`

17.1.12 debug ip psnp mst

Use this command to enable the PIM Snooping entry operation debugging switch. Use the **no** form of this command to disable the switch.

debug ip psnp mst

no debug ip psnp mst

Parameter description	N/A
Command mode	Privileged EXEC mode.
Examples	The following example enable the PIM Snooping entry operation debugging switch: `DES-7210#debug ip psnp mst`

17.1.13 debug ip psnp packet

Use this command to enable the PIM Snooping packet process debugging switch. Use the **no** form of this command to disable the switch.

debug ip psnp packet [hello] [join-prune]
no debug ip psnp packet [hello] [join-prune]

Parameter description

Parameter	Description
hello	Hello packet debugging switch.
Join-prune	Join/Prune packet debugging switch.

Command mode Privileged EXEC mode.

Examples The following example enable the PIM Snooping Hello packet process debugging switch:

```
DES-7210#debug ip psnp packet hello
```

17.1.14 debug ip psnp port

Use this command to enable the PIM Snooping port management and neighbor information debugging switch. Use the **no** form of this command to disable the switch.

debug ip psnp port

no debug ip psnp port

Parameter description N/A

Command mode Privileged EXEC mode.

Examples The following example enable the PIM Snooping port management debugging switch:

```
DES-7210#debug ip psnp port
```

17.1.15 debug ip psnp timer

Use this command to enable the PIM Snooping timer debugging switch. Use the **no** form of this command to disable the switch.

debug ip psnp timer

no debug ip psnp timer

Parameter description N/A

Command mode	Privileged EXEC mode.
Examples	The following example enable the PIM Snooping timer debugging switch: `DES-7210#debug ip psnp timer`

18 MSTP Configuration Commands

18.1 Configuration Related Commands

18.1.1 spanning-tree

Use this command to enable MSTP and configure its basic settings globally. The **no** form of the command disables the spanning-tree function. The **no** form of the command with parameters only restores the corresponding parameters to the default values, but does not disable the spanning-tree function.

spanning-tree [**forward-time** *seconds*|**hello-time** *seconds* |**max-age** *seconds*]

no spanning-tree [**forward-time** | **hello-time** | **max-age**]

Parameter description

Parameter	Description
forward-time *seconds*	Interval at which the port status changes
hello-time *seconds*	Interval at which the switch sends the BPDU message
max-age *seconds*	Maximum aging time of the BPDU message

Default configuration Disabled.

Command mode Global configuration mode.

Usage guidelines	The values of **forward-time, hello time** and **max-age** are interrelated. Modifying one of these three parameters will affect the others. There is a restricted relationship among the above three values. 2*(Hello Time+1.0snd) <= Max-Age Time <= 2*(Forward-Delay–1.0snd) If the values do not according with the condition, the settings do not work.

Examples	Enable the spanning-tree function:
	`DES-7210(config)# spanning-tree`
	Configure the BridgeForwardDelay:
	`DES-7210(config)# spanning-tree forward-time 10`

Related commands

Command	Description
show spanning-tree	Show the global STP configuration.
spanning-tree mst cost	Set the PathCost of an STP interface.
spanning-tree tx-hold-count	Set the global TxHoldCount of STP.

18.1.2 spanning-tree bpdufilter

Use this command to enable BPDU filter on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU filter function on the interface.

spanning-tree bpdufilter [**enabled** | **disabled**]

Parameter description

Parameter	Description
enabled	Enable BPDU filter on the interface.
Disabled	Disable BPDU filter on the interface.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7210(config)# interface gigabitethernet 1/1`

	DES-7210(config-if)# **spanning-tree bpdufilter enable**

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

18.1.3 spanning-tree bpduguard

Use this command to enable the BPDU guard function on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU guard function on the interface.

spanning-tree bpduguard [**enabled** | **disabled**]

Parameter description

Parameter	Description
enabled	Enable BPDU guard on the interface.
disabled	Disable BPDU guard on the interface.

Default configuration Disabled.

Command mode Interface configuration mode.

Examples

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# spanning-tree bpduguard enable
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

18.1.4 spanning-tree link-type

Use this command to configure the link type of the interface. Use the **no** form of the command to restore the configuration to the default value.

spanning-tree link-type [**point-to-point** | **shared**]

no spanning-tree link-type

Parameter description

Parameter	Description
point-to-point	Set the link type of the interface to point-to-point.
shared	Forcibly set the link type of the interface to shared.

Default configuration

For a full-duplex interface, its link type is set to point-to-point link; for a half-duplex interface, its link type is set to shared.

Command mode

Interface configuration mode.

Examples

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# spanning-tree link-type
point-to-point
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

18.1.5 spanning-tree max-hops

Use this command to set the maximum number of hops(Max-hopsCount) of the BPDU message in the global configuration mode, the number of hops in a region that the BPDU message passes before being dropped. This parameter takes effect for all instances. Use the **no** form of the command to restore it to the default setting.

spanning-tree max-hops *hop-count*

no spanning-tree max-hops

Parameter description

Parameter	Description
hop-count	Number of hops in a region that the BPDU message passes before being dropped. The range is 1 to 40 hops.

Default configuration

The default is 20 hops.

Command mode	Global configuration mode.
Usage guidelines	In the region, the BPDU message sent by the root bridge includes a Hot Count field. When the BPDU message passes a device, the Hop Count is decreased by 1 until it reaches 0, which indicates the BPDU message times out. The device will drop the BPDU message whose Hop Count is 0. Changing the **max-hops** command affects all instances.
Examples	This example shows how to set the max-hops of the spanning tree to 10 for all instances: `DES-7210(config)# spanning-tree max-hops 10` You can verify your setting by entering the **show spanning-tree mst** command in the privileged configuration mode.

Related commands

Command	Description
show spanning-tree	Show the MSTP information.

18.1.6 spanning-tree mode

Use this command to set the STP version in the global configuration mode. Use the **no** form of the command to restore the version of the spanning-tree to the default setting.

spanning-tree mode [**stp** | **rstp** | **mstp**]

no spanning-tree mode

Parameter description

Parameter	Description
stp	Spanning tree protocol(IEEE 802.1d)
rstp	Rapid spanning tree protocol(IEEE 802.1w)
mstp	Multiple spanning tree protocol(IEEE 802.1s)

Default configuration	MSTP version.
Command mode	Global configuration mode.

Examples	`DES-7210(config)# spanning-tree mode stp`

Related commands

Command	Description
show spanning-tree	Show the spanning-tree configuration.

18.1.7 spanning-tree mst configure

Use this command to enter the MST configuration mode in the global configuration mode and configure the MSTP region. Use the **no** form of the command to restore all parameters (name, revision, vlan map) to the default values.

spanning-tree mst configuration

no spanning-tree mst configuration

Default configuration	By default, all VLANs are mapped to the instance 0,*name* is empty, and *revision* is 0.
Command mode	Global configuration mode.
Usage guidelines	To return to the privileged EXEC mode, enter **end** or **Ctrl+C.** To return to the global configuration mode, enter **exit**. After entering the MST configuration mode, you can use the following commands to configure parameters: **instance** *instance-id* **vlan** *vlan-range*: Adds the VLANs to the MST instance. The range of *instance-id* is 0 to 64 and the range of VLAN is 1 to 4095. The *vlan-range* can be a collection of some inconsecutive VLANs separated with comma or some consecutive VLANs in the form of start VLAN number–end VLAN number. For example, **instance 10 vlan 2,3,6-9** means that VLANs 2, 3, 6, 7, 8, 9 are added to instance 10. By default, all VLANs are in Instance0. To remove a VLAN from an instance, use the **no** form of the command: **no instance** *instance-id* [**vlan** *vlan-range*]. (In this case, the range of instance is 1 to 64). **name** *name*: Specify the MST name, a string of up to 32 characters. You can use the **no name** command to restore it to the default setting. **revision** *version*: Set the MST versions in the range 0 to 65535. You can use the **no name** command to restore it the default setting. **Show**: Shows the information of the MST region.

Examples

This example shows how to enter the MST configuration mode, and map VLANs 3. 5 to 10 to MST instance 1:

```
DES-7210(config)# spanning-tree mst configuration
DES-7210(config-mst)# instance 1 vlan 3, 5-10
DES-7210(config-mst)# name region 1
DES-7210(config-mst)# revision 1
DES-7210(config-mst)# show
MST configuration
Name [region1]
Revision 1
Instance  Vlans Mapped
----------  --------------------
0       1-2,4,11-4094
1       3,5-10
---------------------------------
DES-7210(config-mst)# exit
DES-7210(config)#
```

To remove VLAN 3 from instance 1, execute this command after entering the MST configuration mode:

```
DES-7210(config-mst)# no instance 1 vlan 3
```

Delete instance 1:

```
DES-7210(config-mst)# no instance 1
```

You can verify your settings by entering the **show** command of the MST configuration commands.

Related commands

Command	Description
show spanning-tree mst	Show the MST region configuration.
instance *instance-id* **vlan** *vlan-range*	Add VLANs to the MST instance.
name	Configure the name of MST.
revision	Configure the version of MST.
show	Show the MST mode in the MST configuration mode.

18.1.8 spanning-tree mst cost

Use this command to set the path cost of an instance in the interface configuration mode. Use the **no** form of the command to restore it to the default setting.

spanning-tree [**mst** *instance-id*] **cost** *cost*

no spanning-tree [**mst** *instance-id*] *cost*

Parameter description

Parameter	Description
instance-id	Instance ID in the range of 0 to 64
cost	Path cost in the range of 1 to 200,000,000

Default configuration

The default instance-id is 0.

The default value is calculated by the link rate of the interface automatically.

- 1000 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

Command mode

Interface configuration mode.

Usage guidelines

A higher cost value means a higher path cost.

Examples

This example shows how to set the path cost to 400 on the interface associated with instances 3:

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# spanning-tree mst 3 cost 400
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* command in the privileged EXEC mode.

Related commands

Command	Description
show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst port-priority	Configure the priority of an interface.
spanning-tree mst priority	Configure the priority of an instance.

18.1.9 spanning-tree mst port-priority

Use this command to configure the interface priority for different instances in the interface configuration mode. It will determine which interface of a loop in a region is in charge of forwarding. Use the **no** form of the command to restore it to the default setting.

spanning-tree [**mst** *instance-id*] **port-priority** *priority*

no spanning-tree [**mst** *instance-id*] **port-priority**

Parameter description

Parameter	Description
Instance-id	Instance ID in the range of 0 to 64
priority	Interface priority. Sixteen integers are available: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, which are the multiples of 16.

Default configuration

The default instance-id is 0.
The default priority is 128.

Command mode

Interface configuration mode.

Usage guidelines

When a loop occurs in the region, the interface of the higher priority will be in charge of forwarding. If all interfaces have the same priority value, the interface of the smaller number will be in charge of the forwarding.

Examples

This example shows how to set the priority of **gigabitethernet 1/1** to 10 in instance 20:

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# spanning-tree mst 20 port-priority 0
```

You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged command.

Related commands

Command	Description
show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst cost	Set the path cost.
spanning-tree mst priority	Set the device priority for different instances.

18.1.10 spanning-tree mst priority

Use this command to set the device priority for different instances in the global configuration mode. Use the **no** form of the command to restore it to the default setting.

spanning-tree [**mst** *instance-id*] **priority** *priority*

no spanning-tree [**mst** *instance-id*] **priority**

Parameter description

Parameter	Description
instance-id	Instance ID in the range of 0 to 64
priority	Device priority. Sixteen integers are available: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152,53248, 57344 and 61440, which are all multiples of 4096.

Default configuration

The default instance ID is 0.

The default device priority is 32768.

Command mode

Global configuration mode.

Examples

The following example sets the device priority of the Instance as 8192.

```
DES-7210(config-if)# spanning-tree mst 20 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst** instance **interface** *instance-id* command in the privileged EXEC mode.

Related commands

Command	Description
show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst cost	Set path cost.
spanning-tree mst port-priority	Set the port priority of an instance.

18.1.11 spanning-tree reset

Use this command to restore the **spanning-tree** configuration to the default value. This command does not have the **no** form.

spanning-tree reset

Parameter description	N/A.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# spanning-tree reset`

Related commands

Command	Description
show spanning-tree	Show the global STP configuration.
show spanning-tree interface	Show the STP configuration of the interface.

18.1.12 spanning-tree tx-hold-count

Use this command to configure the TxHoldCount of the STP in the global configuraiton mode, the maximum number of the BPDU messages sent in one second. Use the **no** form of the command to restore it to the default setting.

spanning-tree tx-hold-count *tx-hold-count*

no spanning-tree tx-hold-count

Parameter description

Parameter	Description
tx-hold-count	Maximum number of the BPDU messages sent in one second in the range 1 to 10.

Default configuration	The default value is 3.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# spanning-tree tx-hold-count 5`

Related commands	Command	Description
	show spanning-tree	Show the global MSTP configuration.

18.1.13 spanning-tree pathcost method

Use this command to configure the path cost of the port. Use the **no** form of the command to restore it to the default setting.

spanning-tree pathcost method [**long** | **short**]

no spanning-tree pathcost method

Parameter description	Parameter	Description
	long	Adopt the 802.1t standard to configure path cost.
	short	Adopt the 802.1d standard to configure path cost.

Default configuration	Adopt the 802.1T standard to set path cost by default.

Command mode	Global configuration mode.

Examples	`DES-7210(config-if)# spanning-tree pathcost method long`

Related commands	Command	Description
	show spanning-tree interface	Show the STP configuration of the interface.

18.1.14 spanning-tree portfast

Use this command to enable the portfast on the interface. You can use the **disabled** option of this command to disable the portfast feature on the interface.

spanning-tree portfast [**disabled**]

Parameter description	Parameter	Description
	disabled	Disable the portfast on the interface.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	DES-7210(config)# **interface gigabitethernet** *1/1* DES-7210(config-if)# **spanning-tree portfast**

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

18.1.15 spanning-tree portfast bpduguard default

Use this command to enable the GPDU guard globally. You can use the **no** form of the command to disable the BPDU guard.

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Once the BPDU guard is enabled on the interface, it will enter the error-disabled status if the BPDU message arrives at the interface. Use the **show spanning-tree** command to display the configuration.
Examples	DES-7210(config)# **spanning-tree portfast bpduguard default**

Related commands	**Command**	**Description**
	show spanning-tree interface	Show the global STP configuration.

18.1.16 spanning-tree portfast bpdufilter default

Use this command to enable the BPDU filter function globally. You can use the **no** form of the command to disable the BPDU filter.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Once the BPDU filter is enabled, the BPDU message is neither received nor sent on the interface. Use the **show spanning-tree** command to display the configuration.
Examples	`DES-7210(config)# spanning-tree portfast bpdufilter default`

Related commands	**Command**	**Description**
	show spanning-tree interface	Show the global STP configuration.

18.1.17 spanning-tree portfast default

Use this command to enable the portfast feature on all interfaces globally. Use the **no** form of the command to disable the portfast on all interfaces globally.

spanning-tree portfast default

no spanning-tree portfast default

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# spanning-tree portfast default`

Related commands

Command	Description
show spanning-tree interface	Show the global STP configuration.

18.1.18 spanning-tree tc- protection

Use this command to enable **tc-protection** globally. Use The **no** form of this command to disable **tc- protection** globally.

spanning-tree tc- protection

no spanning-tree tc- protection

Parameter description	N/A.
Default configuration	Enabled.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# spanning-tree tc-protection`

18.1.19 spanning-tree tc-protection tc-guard

Use this command to enable **tc-guard** globally to prevent the spread of TC messages. Use the **no** form of this command to disable **tc-guard** globally.

spanning-tree tc- protection tc-guard

no spanning-tree tc- protection tc-guard

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# spanning-tree tc- protection tc-guard`

18.1.20 spanning-tree tc-guard

Use this command to enable **tc-guard** on the interface to prevent the spread of TC messages. Use the **no** form of this command to disable **tc-guard** on the interface.

spanning-tree tc-guard

no spanning-tree tc-guard

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# spanning-tree tc-guard`

18.1.21 spanning-tree guard root

Use this command to enable **root guard** on the interface to prevent the change of current root bridge position because of error configuration and illegal packet attack. Use the **no** form of this command to disable **root guard** on the interface.

spanning-tree guard root

no spanning-tree guard root

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7210(config)# spanning-tree guard root`

18.1.22 spanning-tree loopguard default

Use this command to enable **loop guard** globally to prevent the root port or backup port from generating loop since they can not receive bpdu. Use the **no** form of this command to disable **loop guard**.

spanning-tree loopguard default

no spanning-tree loopguard default

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# spanning-tree loopguard default`

18.1.23 spanning-tree guard loop

Use this command to enable **loop guard** on the interface to prevent the root port or backup port from generating loop since they can not receive bpdu. Use the **no** form of this command to disable **loop guard**.

spanning-tree guard loop

no spanning-tree guard loop

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7210(config)# spanning-tree guard loop`

18.1.24 spanning-tree guard none

Use this command to disable **guard** on the interface. Use the **no** form of this command to delete **guard** on the interface.

spanning-tree guard none

no spanning-tree guard none

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7210(config)# spanning-tree guard none`

18.1.25 spanning-tree autoedge

Use this command to enable Autoedge on the interface. Use the **disabled** option of this command to disable Autoedge on the interface.

spanning-tree autoedge [**disabled**]

Parameter description	The **disabled** parameter is used to disable **Autoedge** on the interface.
Default configuration	Enabled.
Command mode	Interface configuration mode.
Examples	`DES-7210(config)# interface gigabitethernet 1/1` `DES-7210(config-if)# spanning-tree autoedge disabled`

Related commands

Command	Function
show spanning-tree interface	Show the STP configuration information of the interface.

18.1.26 bpdu src-mac-check

Use this command to enable the BPDU source MAC address check function on the interface. Use the **no** form of this command to disable the function.

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

Parameter description

Parameter	Description
H.H.H	Indicate that only the BPDU messages from this MAC address are received.
no	Indicate that the BPDU messages from any MAC address are received.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7210(config)# interface gigabitethernet 1/1` `DES-7210(config-if)# bpdu src-mac-check 00d0.f800.1e2f`

18.1.27 clear spanning-tree detected-protocols

Use this command to force the interface to send the RSTP BPDU message and check the BPDU messages.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Parameter description

Parameter	Description
interface-id	ID of the interface

Default configuration N/A.

Command mode Privileged configuration mode.

Examples

```
DES-7210# clear spanning-tree detected-protocols
```

Related commands

Command	Description
show spanning-tree interface	Show the STP configuration of the interface.

18.1.28 spanning-tree compatible enable

Use this command to send the message selectively carried with MSTI according to the interface attibute of current port to realize interconnection with other vendors.

spanning-tree compatible enable

no spanning-tree compatible enable

Parameter description N/A.

Default configuration Disabled.

Command mode Interface configuration mode.

Examples

```
DES-7210(config)# spanning-tree compatible enable
```

18.1.29 logging event status

Use this command to control the switch of log about the forwarding status change on the spanning tree port..

logging event status

no logging event status

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	`DES-7210(config)# logging event status`

18.2 Showing Related Command

18.2.1 show spanning-tree

Use this command to display the global spanning-tree configurations.

show spanning-tree [**summary** |**forward-time** | **hello-time** | **max-age** | **inconsistentports | tx-hold-count** | **pathcost** *method* | *max_hops*]

Parameter description

Parameter	Description
summary	Show the information of MSTP instances and forwarding status of the interfaces.
inconsistentports	Show the block port due to root guard or loop guard.
forward-time	Show BridgeForwardDelay.
hello-time	Show BridgeHelloTime.
max-age	Show BridgeMaxAge.
max-hops	Show the maximum hops of an instance.
tx-hold-count	Show TxHoldCount.

	pathcost *method*	Show the method used for calculating path cost.

Command mode	Privileged EXEC mode.

Examples	`DES-7210# show spanning-tree hello-time`

Related commands	**Command**	**Description**
	spanning-tree pathcost method	Set the pathcost method.
	spanning-tree forward-time	Set BridgeForwardDelay.
	spanning-tree hello-time	Set BridgeHelloTime.
	spanning-tree max-age	Set BridgeMaxAge.
	spanning-tree max-hops	Set the maximum hops of an instance.
	spanning-tree tx-hold-count	Show TxHoldCount.

18.2.2 show spanning-tree interface

Use this command to show the STP configuration of the interface, including the optional spanning tree.

show spanning-tree interface *interface-id* [{**bpdufilter** | **portfast** | **bpduguard** | **link-type** }]

Parameter description	**Parameter**	**Description**
	interface-id	Interface ID
	bpdufilter	Show the status of BPDU filter.
	portfast	Show the status of portfast.
	bpduguard	Show the status of BPDU guard.
	link-type	Show the link type of an interface.

Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show spanning-tree interface gigabitethernet 1/5
```

Related commands

Command	Description
spanning-tree bpdufilter	Enable the BPDU filter feature someone the interface.
spanning-tree portfast	Enable the portfast on the interface.
spanning-tree bpduguard	Enable the BPDU guard on the interface.
spanning-tree link-type	Set the link type of the interface to point-to-point.

18.2.3 show spanning-tree mst

In privileged EXEC mode, use this command to display the information of MST and instances.

show spanning-tree mst {**configuration** |*instance-id* [**interface** *interface-id*] }

Parameter description

Parameter	Description
configuration	The MST configuration of the equipment.
instance-id	Instance number
interface-id	Interface number

Default configuration

All the instances are displayed by default.

Command mode

Privileged mode.

Examples

```
DES-7210# show spanning-tree mst configuration
```

Related commands

Command	Description
spanning-tree mst configuration	Configure the MST region.
spanning-tree mst cost	Show the path cost of the instance.

spanning-tree mst max-hops	Show the maximum hops of the instance.
spanning-tree mst priority	Show the equipment priority of the instance.
spanning-tree mst port-priority	Show the port priority of the instance.

19 SPAN Configuration Commands

19.1 monitor session

Use this command to create a SPAN session and specify the destination port (monitoring port) and source port (monitored port). The **no** form of the command is used to delete the session or delete the source port or destination port separately.

monitor session *session_number* **{source interface** *interface-id* **[both | rx | tx] | destination interface** *interface-id* [**switch]}** [**acl** *name*]

no monitor session *session_number* **[source interface** *interface-id* **[both | rx | tx] | destination interface** *interface-id* [**switch]}** [**acl** *name*]

no monitor session all

Parameter description

Parameter	Description
session_number	SPAN session number
source interface *interface-id*	Specify the source port. *interface-id*: interface ID, which can be physical interface, not SVI. DES-7200 supports AP.
destination interface *interface-id*	Specify the destination port. *interface-id*: interface ID, which can be physical interface, not SVI. DES-7200 supports AP.
both acl *name*	Monitor the inbounding and outbounding frames simultaneously. **acl** *name/id* of monitored flow
rx	Monitor only the inbounding frames.
tx	Monitor only the outbounding frames.
all	Delete all sessions.
switch	Enable switching on the mirroring destination port. It is disabled by default.

Command mode	Global configuration mode.

Usage guidelines

Both switch port and routed port can be configured as the source port or destination port. The SPAN session has no effect on the normal operation of the equipment. You can configure a SPAN session on disabled ports. However, the SPAN does not work unless you enable the source and destination ports.

A port can not be configured as the source port and the destination port at the same time.

You will remove the whole session if you do not specify the source port or the destination port.

Use **show monitor** to display SPAN session status.

Examples

The example below describes how to create a SPAN session: session 1: If this session is set previously, clear the configuration of current session 1 firstly, and then set the frame mapping of port 1 to port 8.

```
DES-7210(config)# no monitor session 1
DES-7210(config)# monitor session 1 source interface
gigabitEthernet 1/1 both
DES-7210(config)# monitor session 1 destination interface
gigabitEthernet 1/8、
```

Note:
session 1 supports global port mirroring crossing line cards.

Related commands

Command	Description
show monitor	Use this command to display the SPAN configurations.

Platform description

DES-7200 supports up to 128 sessions.

DES-7200 does not support the source/destination MAC-based frame mirror.

19.2 Show monitor

Use this command to display the SPAN configurations.

show monitor [**session** *session_number*]

Default configuration

All SPAN sessions are displayed by default.

Parameter description

Parameter	Description
session *session_number*	SPAN session number.

Command mode

Privileged mode.

Usage guidelines

N/A.

Examples

This example shows how to use **show monitor** to display SPAN session 1**:**

```
DES-7210# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

Related commands

Command	Description
monitor session	Specify a SPAN session and the destination port (mirroring port) and the source port (mirrored port).

20 RSPAN Configuration Commands

20.1 Configuring related commands

20.1.1 monitor session

Use this command to set RSPAN session.

Set mirror device attribute:

monitor session *session_num* {**remote-destination** | **remote-source**}

Set destination mirror:

monitor session *session-num* **destination remote vlan** *vlan-id* **interface** *interface-name* [**switch**]

Set remote source mirror:

monitor session *session-num* **source interface** *interface-id* [**rx** | **tx** | **both**]

Parameter description

Parameter	Description
session-num	Session number.
vlan-id	Remote span vlan id.
interface-id	Interface number .

Command mode

Global configuration mode.

Usage guidelines

Key in **end** or **Ctrl+C** to return to the privileged mode.

Key in **exit** to return to the global configuration mode.

Examples

```
DES-7210(config)# monitor session 1 source interface fastethernet 0/1
```

```
DES-7210(config)# monitor session 1 destination
remote vlan 5 reflector-port interface fastethernet 0/5
DES-7210(config)# monitor session 1 remote-destination
```

Related commands

Command	Description
show monitor	Show monitor session information.

20.1.2 remote-span

Use this command to set **RSPAN VLAN**

[**no**] **remote-span**

Parameter description

N/A .

Command mode

VLAN configuration mode.

Usage guidelines

Key in **end** or **Ctrl+C** to return to the privileged mode.

Key in **exit** to return to the global configuration mode.

Examples

```
DES-7210(config)# vlan 5
DES-7210(config-vlan)# remote-span
```

Related commands

Command	Description
show vlan	Show VLAN information.

21 IP Address Configuration Commands

21.1 Interface Address Configuration Commands

The interface address configuration include the commands as follows:

- **ip-address**
- **ip unnumbered**

21.1.1 ip-address

Use this command to configure the IP address of an interface. The **no** form of this command can be used to delete the IP address of the interface.

ip address *ip-address network-mask* [**secondary**]

no ip address *ip-address network-mask* [**secondary**]

Parameter description

Parameter	Description
ip-address	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.
network-mask	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.
secondary	Indicates the secondary IP address that has been configured.

Default

No IP address is configured for the interface.

Usage guidelines

Interface configuration mode.

Usage guidelines

The equipment cannot receive and send IP packets before it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP).

The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value “1” are the network address. The IP address bits that correspond to value “0” are the host address. For example, the network mask of Class A IP address is “255.0.0.0”. You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask.

The DES-7200 software supports multiple IP address for an interface, in which one is the primary IP address and others are the secondary IP addresses. Theoretically, there is no limit for the number of secondary IP addresses. The primary IP address must be configured before the secondary IP addresses can be configured. The secondary IP address and the primary IP address can belong to the same network or different networks. Secondary IP addresses are often used in network construction. Typically, you can try to use secondary IP addresses in the following situations:

- A network hasn’t enough host addresses. At present, the LAN should be a class C network where 254 hosts can be configured. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the device should be connected to two networks and multiple IP addresses should be configured.
- Many older networks are layer 2-based bridge networks that have not been divided into different subnets. Use of secondary IP addresses will make it very easy to upgrade this network to an IP layer-based routing network. The equipment configures an IP address for each subnet.
- Two subnets of a network are separated by another network. You can create a subnet for the separated network, and connect the separated subnet by configuring a secondary IP address. One subnet cannot appear on two or more interfaces of a device.

Examples

In the example below, the primary IP address is configured as 10.10.10.1, and the network mask is configured as 255.255.255.0.

```
ip address 10.10.10.1 255.255.255.0
```

Related commands

Command	Description
show interface	Show detailed information of the interface.

Platform description

For the Layer 2 switch, the IP address can be configured only for the Layer 3 interface. The Level-2 address is not supported, that is, the **secondary** option is unuavailable.

21.1.2 ip unnumbered

Use this command to configure an unnumbered interface. After an interface is configured as unnumbered interface, it is allowed to run the IP protocol and can receive and send IP packets. The **no** form can be used to remove this configuration.

ip unnumbered *interface-type interface-number*

no ip unnumbered *interface-type interface-number*

Parameter description

Parameter	Description
interface-type	Interface type
interface-number	Interface number

Default

N/A.

Command mode

Interface configuration mode.

Usage guidelines

Unnumbered interface is an interface that has IP enabled on it but no IP address is assigned to it. The unnumbered interface should be associated to an interface with an IP address. The source IP address of the IP packet generated by an unnumbered interface is the IP address of the associated interface. In addition, the routing protocol process determines whether to send route update packets to an unnumbered interface according to the IP address of the associated interface. The following restrictions apply when an unnumbered interface is used:

- An Ethernet interface cannot be configured as an unnumbered interface.
- A serial interface can be configured as an unnumbered interface when it is encapsulated with SLIP, HDLC, PPP, LAPB and Frame-relay. However, when Frame-relay is used for encapsulation, only the point-to-point interface can be configured

as an unnumbered interface. X.25 encapsulation does not allow configuration as an unnumbered interface.

- You cannot detect whether an unnumbered interface works normally using the **ping** command, because no IP address is configured for the unnumbered interface. However, the status of the unnumbered interface can be monitored remotely using SNMP.
- The network cannot be started using an unnumbered interface.

Examples

In the example below the local interface is configured as an unnumbered interface, and the associated interface is FastEthernet 0/1. An IP address must be configured for the associated interface.

```
ip unnumbered fastEthernet 0/1
```

Related commands

Command	Description
show interface	Show detailed information of the interface.

Platform description

This command is not supported on the Layer 2 switch.

21.2 Address Resolution Protocol (ARP) Configuration Commands

The address resolution protocol (ARP) configuration commands include as follows:

- **arp**
- **arp retry interval**
- **arp retry times**
- **arp trusted num**
- **arp trusted aging**
- **arp unresolve**
- **arp gratuitous-send interval**
- **arp timeout**
- **ip proxy-arp**
- **service trustedarp**

21.2.1 arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. The **no** form of this command deletes the static MAC address mapping.

arp *ip-address MAC-address type* [**alias**]

no arp *ip-address MAC-address type* [**alias**]

Parameter description

Parameter	Description
ip-address	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
MAC-address	48-bit data link layer address
type	ARP encapsulation type. The keyword is **arpa** for the Ethernet interface.
alias	(Optional) The DES-7200 series will respond to the ARP request from this IP address after this parameter is defined.

Default

There is no static mapping record in the ARP cache table.

Command mode

Global configuration mode.

Usage guidelines

DES-7200 finds the 48-bit MAC address according to the 32-bit IP address using the ARP cache table.

Since most hosts support dynamic ARP resolution, usually static ARP mapping is not necessary. The **clear arp-cache** command can be used to delete the ARP mapping that is learned dynamically.

Examples

The following is an example of setting an ARP static mapping record for a host in the Ethernet.

```
arp 1.1.1.1 4e54.3800.0002 arpa
```

Related commands

Command	Description
clear arp-cache	Clear the ARP cache table

21.2.2 arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. The **no** form of this command is used to restore the default value, that is, retry an ARP request per second.

arp retry interval *seconds*

no arp retry interval

Parameter description

Parameter	Description
seconds	Time for retrying the ARP request message in the range of 1 to 3600 seconds, 1 second by default.

Default configuration

The retry interval of the ARP request is 1s.

Command mode

Global configuration mode.

Usage guidelines

The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.

Examples

The following configuration sets the retry interval of the ARP request as 30s.

```
arp retry interval 30
```

Related commands

Command	Function
arp retry times *number*	Set the retry time of the ARP request message.

21.2.3 arp retry times

Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. The **no** form of this command can be used to restore the default 5 times of the ARP retry requests.

arp retry times *number*

no arp retry times

Parameter description

Parameter	Description
number	The times of sending the same ARP request in the range 1 to100..When it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent.

Default configuration

If the ARP response message is not received, the ARP request message will be sent for 5 times, and then it will be timed out.

Command mode

Global configuration mode.

Usage guidelines

The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.

Examples

The following configuration will set the local ARP request not to be retried.

```
arp retry times 1
```

The following configuration will set the local ARP request to be retried for one time.

```
arp retry times 2
```

Related commands

Command	Function
arp retry interval *seconds*	Set the retry interval of the ARP request message.

21.2.4 arp trusted num

Use this command to set the maximun number of trusted ARP entries.The **no** form of this command restores it to the default value.

arp trusted num *number*

no arp trusted

Parameter description

Parameter	Description
number	Maximum number of trusted ARP entries in the range of 10 to 4096.

Default configuration

The default value is different for different products.

Command mode

Global configuration mode.

Usage guidelines

To make this command valid, enable the trusted ARP function firstly. The trusted ARP entries and other entries share the memory. Too much trusted ARP entries may lead to insufficient ARP entry space. In general, you should set the maximum number of trusted ARP entries according to your real requirements.

Examples

The following configuration sets 1000 trusted ARPs.

```
arp trusted 1000
```

Related commands

Command	Function
service trustedarp	Enable the trusted ARP function.

21.2.5 arp trusted aging

Use this command to set trusted ARP aging. The **no** form of this command restores it to the default value.

arp trusted aging

no arp trusted aging

Parameter description

N/A .

Default configuration

GSN trusted ARP is not aging by default.

Command mode	Global configuration mode.
Usage guidelines	Use this command to set trusted ARP aging. Aging time is the same as dynamic ARP aging time. Execute **arp timeout** to set aging time in interface mode.
Examples	N/A

Related commands

Command	Description
service trustedarp	Enable trusted ARP function.

21.2.6 arp unresolve

Use this command to configure the maximum number of the unresolved ARP entries. The **no** form of this command can restore it to the default value 8192.

arp unresolve *number*

no arp unresolve

Parameter description

Parameter	Description
number	The maximum number of the unresolved ARP entries in the range of 1 to 8192. The default value is 8192.

Default configuration	The ARP cache table can contain up to 8192 unresolved entries.
Command mode	Global configuration mode.
Usage guidelines	If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.

Examples

The following configuration sets the maximum number of the unresolved items as 500.

```
arp unresolved 500
```

21.2.7 arp gratuitous-send interval

Use this command to set the interval of sending the free ARP request message on the interface..The **no** form of this command disables this function on the interface.

arp gratuitous-send interval *seconds*

no arp gratuitous-send

Parameter description

Parameter	Description
seconds	The time interval to send the free ARP request message in the range 1 to 3600 seconds

Default configuration

This function is not enabled on the interface to send the free ARP request regularly.

Command mode

Interface configuration mode.

Usage guidelines

If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.

Examples

The following configuration sets to send one free ARP request to SVI 1 per second.

```
DES-7210(config)# interface vlan 1
DES-7210(config-if)# arp gratuitous-send interval 1
```

The following configuration stops sending the free ARP request to SVI 1.

```
DES-7210(config)# interface vlan 1
DES-7210(config-if)# no arp gratuitous-send
```

21.2.8 arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache. The no form of this command restores it to the default configuration.

arp timeout *seconds*

no arp timeout

Parameter description

Parameter	Description
seconds	The timeout ranging 0 to 2147483 seconds

Default

The default timeout is 3600 seconds.

Command mode

Interface configuration mode.

Usage guidelines

The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

Examples

The following is an example of setting the timeout for the dynamic ARP mapping record that is learned dynamically from FastEthernet 0/1 to 120 seconds.

```
interface fastEthernet 0/1
arp timeout 120
```

Related commands

Command	Description
clear arp-cache	Clear the ARP cache list.
show interface	Show the interface information.

21.2.9 ip proxy-arp

Use this command to enable ARP proxy funtion on the interface. The **no** form of this command disables ARP function.

ip proxy-arp

no ip proxy-arp

Default	Disabled on the version higher than 10.2(3).
Command mode	Interface configuration mode.
Usage guidelines	Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

Examples	The following is an example of enabling ARP on FastEthernet 0:
	`interface fastEthernet 0/0`
	`ip proxy-arp`

Platform description	This command is not supported on the Layer 2 switch.

21.2.10 service trustedarp

Use this command to enable the trusted ARP function.The **no** form of this command disables the trusted ARP function.

service trustedarp

no service trustedarp

Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The trusted ARP function of the device is to prevent the ARP fraud function. As a part of the GSN scheme, it should be used together with the GSN scheme. In the following three cases, the STP protocol clears not only the dynamic MAC address of a port but also the trusted entries, including

trusted MAC and trusted ARP:

1 STP is enabled.

2 The port is set to neither root port nor designed port. This may be caused when the port is up or down or the port priority is modified.

3 TC packet is received on the port, and the addresses of the ports not receiving PC packet are cleared.

Examples

The following configuration is to enable the trusted ARP function in the global configuration mode.

```
config
service trustedarp
```

21.3 Broadcast Message Processing Configuration Commands

The broadcast message processing configuration related commands include:

- **ip broadcast-addresss**
- **ip directed-broadcast**

21.3.1 ip broadcast-addresss

Use this command to define a broadcast address for an interface in the interface configuration mode. The **no** form of this command is used to remove the broadcast address configuration.

ip broadcast-addresss *ip-address*

no ip broadcast-addresss *ip-address*

Parameter description

Parameter	Description
ip-address	Broadcast address of IP network

Default The default IP broadcast address is 255.255.255.255.

Command mode Interface configuration mode.

Usage guidelines	At present, the destination address of IP broadcast packet is all “1”, represented as 255.255.255.255. The DES-7200 software can generate broadcast packets with other IP addresses through definition, and can receive both all “1” and the broadcast packets defined by itself.
Examples	The following is an example of setting the destination address of IP broadcast packets generated by this interface to 0.0.0.0. `ip broadcast-address 0.0.0.0`
Platform description	This command is not supported on the Layer 2 switch.

21.3.2 ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. The **no** form of this command is used to remove the configuration.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast

Parameter description

Parameter	Description
access-list-number	(Optional) Access list number ranging 1 to 199 and 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

Default	Disabled.
Command mode	Interface configuration mode.

Usage guidelines	IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet. The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all "1"), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast. You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets. You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast. If **no ip directed-broadcast** is configured on an interface, DES-7200 will discard the directed broadcast packets received from the directly connected network.
Examples	The following is an example of enabling forwarding of directed broadcast packet on the fastEthernet 0/1 port of a device. **interface fastEthernet** *0/1* **ip directed-broadcast**
Platform description	This command is not supported on the Layer 2 switch.

21.4 IP Address Monitoring and Maintenance Commands

The IP address monitoring and maintenance related commands include:

- **clear arp-cache**
- **show arp**
- **show arp counter**
- **show arp timeout**
- **clear ip route**
- **show ip arp**
- **show ip interface**
- **show ip redirects**

21.4.1 clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table in the global configuration mode.

clear arp-cache [*A.B.C.D*] **| interface** *interface-name*]

Command mode	Privileged mode.

Usage guidelines	This command can be used to refresh an ARP cache table.

Caution

On a NFPP-based(Network Foundation Protection Policy) device, it receives one ARP packet for every mac/ip address per second by default. If the interval of two **clear arp** times is within 1s, the second response packet will be filtered and the ARP packet will not be resolved for a short time.

Examples

The following is an example of removing all dynamic ARP mapping records.

```
clear arp-cache
```

The following is an example of removing dynamic ARP table entry 1.1.1.1

```
clear arp-cache 1.1.1.1
```

The following is an example of removing dynamic ARP table entry on interface SVI1

```
clear arp-cache interface Vlan 1
```

Related commands	Command	Description
	arp	Add a static mapping record to the ARP cache table.

21.4.2 show arp

Use this command to show the Address Resolution Protocol (ARP) cache table

show arp *[ip [mask]* | *mac-address]* | **static | complete | incomplete**

Parameter description	Parameter	Description
	ip	Show the ARP entry of the specified IP address.
	ip mask	Show the ARP entries of the network segment included within the mask.
	mac-address	Show the ARP entry of the specified MAC address.
	static	Show all the static ARP entries.
	complete	Show all the resolved dynamic ARP entries.
	incomplete	Show all the unresolved dynamic ARP entries.

Command mode	
	Any

Examples

The following is the output result of the **show arp** command:

```
DES-7210# show arp
Total Numbers of Arp: 7
Protocol   Address             Age(min)   Hardware          Type
Interface
Internet  192.168.195.68   0        0013.20a5.7a5f  arpa   VLAN 1
Internet  192.168.195.67   0        001a.a0b5.378d  arpa   VLAN 1
Internet  192.168.195.65   0        0018.8b7b.713e  arpa   VLAN 1
Internet  192.168.195.64   0        0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.63   0        001a.a0b5.3990  arpa   VLAN 1
Internet  192.168.195.62   0        001a.a0b5.0b25  arpa   VLAN 1
Internet  192.168.195.5    --       00d0.f822.33b1  arpa   VLAN 1
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
Protocol	Protocol of the network address, always to be Internet
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, ARPA for all Ethernet addresses
Interface	Interface associated with the IP addresses

The following is the output result of **show arp** *192.168.195.68*

```
DES-7210# show arp 192.168.195.68
Protocol  Address    Age(min)  Hardware       Type   Interface
Internet  192.168.195.68   1   0013.20a5.7a5f  arpa   VLAN 1
```

The following is the output result of **show arp** *192.168.195.0 255.255.255.0*

```
DES-7210# show arp 192.168.195.0 255.255.255.0
Protocol  Address    Age(min)  Hardware   Type   Interface
Internet  192.168.195.64   0   0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.2    1   00d0.f8ff.f00e  arpa   VLAN 1
Internet  192.168.195.5    --   00d0.f822.33b1  arpa   VLAN 1
Internet  192.168.195.1    0   00d0.f8a6.5af7  arpa   VLAN 1
Internet  192.168.195.51   1   0018.8b82.8691  arpa   VLAN 1
```

The following is the output result of **show arp** *001a.a0b5.378d*

```
DES-7210# show arp 001a.a0b5.378d
Protocol  Address  Age(min)  Hardware  Type   Interface
Internet  192.168.195.67   4   001a.a0b5.378d  arpa   VLAN 1
```

Platform description This command is not supported on the Layer 2 switch.

21.4.3 show arp counter

Use this command to show the number of ARP entries in the ARP cache table.

show arp counter

Parameter description	N/A.
Command mode	Any.

Examples	The following is the output result of the **show arp counter** command:
	`DES-7210# show arp counter`
	`The Arp Entry counter:0`
	`The Unresolve Arp Entry:0`
	The meaning of each field in the ARP cache table is described in Table 1.

Platform description	This command is not supported on the Layer 2 switch.

21.4.4 show arp timeout

Use this command to show the aging time of a dynamic ARP entry on the interface.

show arp timeout

Parameter description	N/A.
Command mode	Any.

Examples	The following is the output of the **show arp timeout** command:
	`DES-7210# show arp timeout`
	`Interface arp timeout(sec)`
	`---------- ----------`
	`VLAN 1 3600`
	The meaning of each field in the ARP cache table is described in Table 1.

Platform description	This command is not supported on the Layer 2 switch.

21.4.5 clear ip route

Use this command to remove the entire IP routing table or a particular routing record in the IP routing table in the privileged user mode.

clear ip route { ***** **|** *network* [*netmask*] }

Parameter description

Parameter	Description
*	Remove all the routes.
network	The network or subnet address to be removed
netmask	(Optional) Network mask

Command mode

Privileged mode.

Usage guidelines

Once an invalid route is found in the routing table, you can immediately refresh the routing table to get the updated routes. Note that, however, refreshing the entire routing table will result in temporary communication failure in the entire network.

Examples

The example below refreshes only the route of 192.168.12.0.

```
clear ip route 192.168.12.0
```

Related commands

Command	Description
show ip route	Show the IP routing table.

Platform description

This command is not supported on the Layer 2 switch.

21.4.6 show ip arp

Use this command to show the Address Resolution Protocol (ARP) cache table in the privileged user mode.

show ip arp

Parameter description

N/A.

Command mode

Privileged mode.

Examples

The following is the output of **show ip arp**:

```
DES-7210# show ip arp
Protocol Address      Age(min)Hardware       Type   Interface
Internet 192.168.7.233  23   0007.e9d9.0488  ARPA FastEthernet 0/0
Internet 192.168.7.112  10   0050.eb08.6617  ARPA FastEthernet 0/0
Internet 192.168.7.79   12   00d0.f808.3d5c  ARPA FastEthernet 0/0
Internet 192.168.7.1    50   00d0.f84e.1c7f  ARPA FastEthernet 0/0
Internet 192.168.7.215  36   00d0.f80d.1090  ARPA FastEthernet 0/0
Internet 192.168.7.127  0    0060.97bd.ebee  ARPA FastEthernet 0/0
Internet 192.168.7.195  57   0060.97bd.ef2d  ARPA FastEthernet 0/0
Internet 192.168.7.183  --   00d0.f8fb.108b  ARPA FastEthernet 0/0
```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

Platform description

This command is not supported on the Layer 2 switch.

21.4.7 show ip interface

Use this command to show the IP status information of an interface. The command format is as follows:

show ip interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Specify interface type.
interface-number	Specify interface number.

Command mode

Privileged mode.

Usage guidelines

When an interface is available, DES-7200 will create a direct route in the routing table. The interface is available in that the DES-7200 software can receive and send packets through this interface. If the interface changes from available status to unavailable status, the DES-7200 software removes the appropriate direct route from the routing table.

If the interface is unavailable, i.e. two-way communication is allowed, the line protocol status will be shown as “UP”. If only the physical line is available, the interface status will be shown as “UP”.

The results shown may vary with the interface type, because some contents are the interface-specific options.

Examples

Presented below is the output of **show ip interface**:

```
DES-7210# show ip interface
FastEthernet 0/0
IP interface state is: UP
IP interface type is: BROADCAST
IP interface metric is: 0
IP interface MTU is: 1500
IP address is:
192.168.5.133/24 (primary)
IP address negotiate is: OFF
Forward direct-boardcast is: ON
ICMP mask reply is: ON
Send ICMP redirect is: ON
Send ICMP unreachabled is: ON
DHCP relay is: OFF
Fast switch is: ON
Route horizontal-split is: ON
Help address is: 0.0.0.0
Agent ARP is: ON
Outgoing access list is not set.
Inbound access list is not set.
```

Description of fields in the results:

Field	Description
IP interface state is:	The network interface is available, and both its interface hardware status and line protocol status are “UP”.
IP interface type is:	Show the interface type, such as broadcast, point-to-point, etc.
IP interface MTU is:	Show the MTU value of the interface.

IP address is:	Show the IP address and mask of the interface.
IP address negotiate is:	Show whether the IP address is obtained through negotiation.
Forward direct-boardcast is:	Show whether the directed broadcast is forwarded.
ICMP mask reply is:	Show whether an ICMP mask response message is sent.
Send ICMP redirect is:	Show whether an ICMP redirection message is sent.
Send ICMP unreachabled is:	Show whether an ICMP unreachable message is sent.
DHCP relay is:	Show whether the DHCP relay is enabled.
Fast switch is:	Show whether the IP fash switching function is enabled.
Route horizontal-split is:	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Show the helper IP address.
Proxy ARP is:	Show whether the agent ARP is enabled.
Outgoing access list is	Show whether an outgoing access list has been configured for an interface.
Inbound access list is	Show whether an incoming access list has been configured for an interface.

21.4.8 show ip redirects

Use this command to show the default gateway

show arp timeout

Parameter description	N/A.
Command mode	Privileged EXEC mode
Examples	The following is the output of the **show ip redirectes** command:

```
DES-7210# show ip redirects
Default Gateway: 192.168.195.1
```

Related commands

Command	Description
ip default-gateway	Configure the default gateway, which is only supported on the Layer 2 switch.

Platform description

This command is not supported on the Layer 2 switch.

22 IP Service Configuration Commands

22.1 IP Service Configuration Commands

The IP service configuration related command includes as follows:

- **ip default-gateway**
- **ip mask-reply**
- **ip mtu**
- **ip redirects**
- **ip source-route**
- **ip unreachables**

22.1.1 ip default-gateway

Use this command to configure the default gateway on the Layer2 switch. Use the **no** form of this command to remove the default gateway.

ip default-gateway

no ip default-gateway

Default configuration	By default, no default gateway is configured.
Command mode	Global configuration mode.
Usage guidelines	The packets will be sent to the default gateway if the destination address is unknown. Use the **show ip redirects** command to view the default gateway.

Examples

The following is an example of setting the default gateway 192.168.1.1:

```
ip default-gateway 192.168.1.1
```

Related commands

Command	Description
show ip redirects	Show the default gateway, which is supported on the Layer 2 switch only.

Platform description

This command is supported on the Layer 2 switch only.

22.1.2 ip mask-reply

Use this command to configure the DES-7200 software to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. The **no** form of this command is used to prohibit from sending the ICMP mask response message.

ip mask-reply

no ip mask-reply

Default configuration

By default, no ICMP mask response message is sent.

Command mode

Interface configuration mode.

Usage guidelines

Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.

Examples

The following is an example of setting the FastEthernet 0/1 interface of a device to respond the ICMP mask request message.

```
interface fastEthernet 0/1
ip mask-reply
```

Platform description

This command is supported on the Layer 2 switch only.

22.1.3 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. The **no** form of this command is used to restore it to the default configuration.

ip mtu *bytes*

no ip mtu

Parameter description

Parameter	Description
bytes	Maximum transmission unit of IP packet ranging 68 to 1500 bytes

Default configuration

It is the same as the value configured in the interface command **mtu** by default.

Command mode

Interface configuration mode.

Usage guidelines

If an IP packet is larger than the IP MTU, the DES-7200 software will split this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface.

If the interface configuration command **mtu** is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

Examples

The following is an example of setting the IP MTU value of the fastEthernet 0/1 interface to 512 bytes.

```
interface fastEthernet 0/1
ip mtu 512
```

Related commands

Command	Description
mtu	Set the MTU value of an interface.

Platform description	This command is supported on the Layer 2 switch only.

22.1.4 ip redirects

Use this command to allow the DES-7200 software to send an ICMP redirection message in the interface configuration mode. The **no** form of this command is used to disable the ICMP redirection function.

ip redirects

no ip redirects

Default configuration	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path. The DES-7200 software enables ICMP redirection by default.
Examples	The following is an example of disabling ICMP redirection for the fastEthernet 0/1 interface. **interface fastEthernet** *0/1* **no ip redirects**
Platform description	This command is supported on the Layer 2 switch only.

22.1.5 ip source-route

Use this command to allow the DES-7200 software to process an IP packet with source route information in the global configuration mode. The **no** form of this command is used to disable the source route information processing function.

ip source-route

no ip source-route

Default configuration	Enabled.
Command mode	Global configuration mode.
Usage guidelines	DES-7200 supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded. The DES-7200 software supports IP source route by default.
Examples	The following is an example of disabling the IP source route. `no ip source-route`
Platform description	This command is supported on the Layer 2 switch only.

22.1.6 ip unreachables

Use this command to allow the DES-7200 software to generate ICMP destination unreachable messages. The **no** form of this command disables this function.

ip unreachables

no ip unreachables

Default configuration	Enabled.

Command mode	Interface configuration mode.
Usage guidelines	DES-7200 software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upeer protocol of this message. DES-7200 software will send ICMP host unreachable message to source data if it can not forward a message due to no routing. This command influences all ICMP destination unreachable messages.
Examples	The following example disables sending ICMP destination unreachable message on FastEthernet 0/1. **interface fastEthernet** *0/1* **no ip unreachables**
Platform description	This command is supported on the Layer 2 switch only.

23 DHCP Configuration Commands

23.1 DHCP Configuration Related Command

DHCP configuration includes the following commands:

- **bootfile**
- **client-identifier**
- **client-name**
- **default-device**
- **dns-server**
- **domain-name**
- **hardware-address**
- **host**
- **ip address dhcp**
- **ip dhcp excluded-address**
- **ip dhcp ping packet**
- **ip dhcp ping timeout**
- **ip dhcp pool**
- **lease**
- **netbios-name-server**
- **netbios-node-type**
- **network (DHCP)**
- **next-server**
- **option**
- **service dhcp**

23.1.1 bootfile

Use this command to define the startup mapping file name of the DHCP client in the DHCP address pool configuration mode.The **no** form of this command can be used to remove the definition.

bootfile file-name

no bootfile

Parameter description

Parameter	Description
file-name	Startup file name.

Default

No startup file name is defined, by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

Some DHCP clients need to download the operating system and configure the file during the startup. The DHCP server should provide the mapping file name required for the startup, so that DHCP clients can download the file from the corresponding server (such as TFTP). Other servers are defined by the **next-server** command.

Examples

The configuration example below defines the device.conf as the startup file name.

```
bootfile device.conf
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.
next-server	Configure the next server IP address of the DHCP client startup process.

23.1.2 client-identifier

Use this command to define the unique ID of the DHCP client (indicated in hex, separated by dot) in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the client ID.

client-identifier *unique-identifier*

no client-identifier

Parameter description

Parameter	Description
unique-identifier	The DHCP client ID, indicated in hex and separated by dot, for instance, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.

Default N/A.

Command mode DHCP address pool configuration mode.

Usage guidelines

When some DHCP clients request the DHCP server to assign IP addresses, they use their client IDs rather then their hardware addresses. The client ID consists of media type, MAC address and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/1, and the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where, 01 denotes the type of the Ethernet media.

The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hex code of GigabitEthernet0/1. For the definition of the media code, refer to the Address Resolution Protocol Parameters section in RFC1700.

This command is used only when the DHCP is defined by manual binding.

Examples

The configuration example below defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

```
client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

Related commands

Command	Description
hardware-address	Define the hardware address of DHCP client.
host	Define the IP address and network mask, which is used to configure the DHCP manual binding.

	ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.3 client-name

Use this command to define the name of the DHCP client in the DHPC address pool configuration mode.The **no** form of this command is used to delete the name of the DHCP client.

client-name *client-name*

no client-name

Parameter description	**Parameter**	**Description**
	client-name	Name of DHCP client, a set of standards-based ASCII characters.The name should not include the suffix domain name. For instance, you can define the name of the DHCP client as river, not river.i-net.com.cn.

Default	No client name is defined.
Command mode	DHCP address pool configuration mode.
Usage guidelines	This command can be used to define the name of the DHCP client only when the DHCP is defined by manual binding. This name should not include the suffix domain name.
Examples	The configuration example below defines a string river as the name of the client. `client-name river`

Related commands	**Command**	**Description**
	host	Define the IP address and network mask, which is used to configure the DHCP manual binding.
	ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.4 default-device

Use this command to define the default gateway of the DHCP client in the DHPC address pool configuration mode.The **no** form of this command can be used to delete the definition of the default gateway.

default-device *ip-address* [*ip-address2…ip-address8*]

no default-device

Parameter description

Parameter	Description
ip-address	Define the IP address of the equipment. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) Up to 8 gateways can be configured.

Default

No gateway is defined by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

In general, the DHCP client should get the information of the default gateway from the DHCP server. The DHCP server should specify one gateway address for the client at least, and this address should be of the same network segment as the address assigned to the client.

Examples

The configuration example below defines 192.168.12.1 as the default gateway.

```
default-device 192.168.12.1
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.5 dns-server

Use this command to define the DNS server of the DHCP client in the DHPC address pool configuration mode. The **no** form of this command can be used to delete the definition of the DNS server.

dns-server { *ip-address* [*ip-address2…ip-address8*] | **use-dhcp-client** *interface-type interface-number* }

no dns-server

Parameter description

Parameter	Description
ip-address	Define the IP address of the DNS server. At least one IP address should be configured.
ip-address2…ip-address8	(Optional) Up to 8 DNS servers can be configured.
use-dhcp-client *interface-type interface-number*	Use the DNS server learned by the DHCP client of the DES-7200 software as the DNS server of the DHCP client.

Default

No DNS server is defined by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

When more than one DNS server is defined, the former will possess higher priory, so the DHCP client will select the next DNS server only when its communication with the former DNS server fails.

If the DES-7200 software also acts as the DHCP client, the DNS server information obtained by the client can be transmitted to the DHCP client.

Examples

The configuration example below specifies the DNS server 192.168.12.3 for the DHCP client.

```
dns-server 192.168.12.3
```

Related commands

Command	Description
domain-name	Define the suffix domain name of the DHCP client.
ip address dhcp	Enable the DHCP client on the interface to obtain the IP address information.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.6 domain-name

Use this command to define the suffix domain name of the DHCP client in the DHPC address pool configuration mode. The **no** form of this command can be used to delete the suffix domain name.

domain-name *domain-name*

no domain-name

Parameter description

Parameter	Description
domain-name	Define the suffix domain name string of the DHCP client.

Default No suffix domain name by default.

Command mode DHCP address pool configuration mode.

Usage guidelines After the DHCP client obtains specified suffix domain name, it can access a host with the same suffix domain name by the host name directly.

Examples The configuration example below defines the suffix domain name i-net.com.cn for the DHCP client.

```
domain-name i-net.com.cn
```

Related commands

Command	Description
dns-server	Define the DNS server of the DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.7 hardware-address

Use this command to define the hardware address of the DHCP client in the DHPC address pool configuration mode.The **no** form of this command can be used to delete the definition of the hardware address.

hardware-address *hardware-address type*

no hardware-address

Parameter description

Parameter	Description
hardware-address	Define the MAC address of the DHCP client.
type	To indicate the hardware platform protocol of the DHCP client, use the string definition or digits definition. String option: ■ Ethernet ■ ieee802 Digits option: ■ 1 (10M Ethernet) ■ 6 (IEEE 802)

Default

No hardware address is defined by default.

If there is no option when the hardware address is defined, it is the Ethernet by default.

Command mode

DHCP address pool configuration mode.

Usage guidelines

This command can be used only when the DHCP is defined by manual binding.

Examples

The configuration example below defines the MAC address 00d0.f838.bf3d with the type ethernet.

```
hardware-address 00d0.f838.bf3d
```

Related commands

Command	Description
client-identifier	Define the unique ID of the DHCP client (Indicated by the hexadecimal numeral, separated by dot).
host	Define the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.8 host

Use this command to define the IP address and network mask of the DHCP client host in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the definition of the IP address and network mask for the DHCP client.

host *ip-address* [*netmask*]

no host

Parameter description

Parameter	Description
ip-address	Define the IP address of DHCP client.
netmask	Define the network mask of DHCP client.

Default

No IP address or network mask of the host is defined.

Command mode

DHCP address pool configuration mode.

Usage guidelines

If the network mask is not defined definitely, the DHCP server will use the natural network mask of this IP address: 255.0.0.0 for class A IP address, 255.255.0 for class B IP address, and 255.255.255.0 for class C IP address.

This command can be used only when the DHCP is defined by manual binding.

Examples

The configuration example below sets the client IP address as 192.168.12.91, and the network mask as 255.255.255.240.

```
host 192.168.12.91 255.255.255.240
```

Related commands

Command	Description
client-identifier	Define the unique ID of the DHCP client (Indicated in hex, separated by dot).
hardware-address	Define the hardware address of DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.9 ip address dhcp

Use this command to make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP in the interface configuration mode. The **no** form of this command can be used to cancel this configuration.

ip address dhcp

no ip address dhcp

Default	The interface cannot obtain the ID address by the DHCP by default.
Command mode	Interface configuration mode.
Usage guidelines	When requesting the IP address, the DHCP client of the DES-7200 software also requires the DHCP server provide 5 configuration parameter information: 1) DHCP option 1, client subnet mask, 2) DHCP option 3, it is the same as the gateway information of the same subnet, 3) DHCP option 6, the DNS server information, 4) DHCP option 15, the host suffix domain name, and 5) DHCP option 44, the WINS server information. The client of the DES-7200 software is allowed to obtain the address on the PPP, FR or HDL link by the DHCP, which should be supported by the server. At present, our server can support this function.

Examples	The configuration example below makes the FastEthernet 0 port obtain the IP address automatically.
	`interface fastEthernet 0`
	`ip address dhcp`

Related commands

Command	Description
dns-server	Define the DNS server of DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.10 ip dhcp excluded-address

Use this command to define some IP addresses and make the DHCP server not assign them to the DHCP client in the global configuration mode. The **no** form of this command can be used to cancel this definition.

ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

no ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

Parameter description

Parameter	Description
low-ip-address	Exclude the IP address, or exclude the start IP address within the range of the IP address.
high-ip-address	Exclude the end IP address within the range of the IP address.

Default

The DHCP server assigns the IP addresses of the whole address pool by default.

Command mode

Global configuration mode.

Usage guidelines

If the excluded IP address is not configured, the DHCP server attempts to assign all IP addresses in the DHCP address pool. This command can reserve some IP addresses for specific hosts to prevent these addresses are assigned to the DHCP client, and define the excluded IP address accurately to reduce the conflict detecting time when the DHCP server assigns the address.

Examples

In the configuration example below, the DHCP server will not attempt to assign the IP addresses within 192.168.12.100~150.

```
ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.
network (DHCP)	Define the network number and network mask of the DHCP address pool.

23.1.11 ip dhcp ping packet

Use this command to configure the times of pinging the IP address when the DHCP server detects address conflict in the global configuration mode. The **no** form of this command is used to restore it to the default configuration.

ip dhcp ping packet [*number*]

no ip dhcp ping packet

Parameter description	**Parameter**	**Description**
	number	(Optional) Number of packets in the range of 0 to 10, where 0 indicates disabling the ping operation. The Ping operation sends two packets by default.

Default	The Ping operation sends two packets by default.
Command mode	Global configuration mode.
Usage guidelines	When the DHCP server attempts to assign the IP address from the DHCP address pool, use the ping operation to check whether this address is occupied by other hosts. Record it if the address is occupied, otherwise, assign it to the DHCP client. The Ping operation will send up to 10 packets, two packets by default.
Examples	The configuration example below sets the number of the packets sent by the ping operation as 3. `ip dhcp ping packets 3`

Related commands	**Command**	**Description**
	clear ip dhcp conflict	Clear the DHCP history conflict record.
	ip dhcp ping packet	Configure the timeout time that the DHCP server waits for the Ping response. If all the ping packets are not responded within the specified time, it indicates that this IP address can be assigned. Otherwise, it will record the address conflict.
	show ip dhcp conflict	Show the DHCP server detects address conflict when it assigns an IP address.

23.1.12 ip dhcp ping timeout

Use this command to configure the timeout that the DHCP server waits for response when it uses the ping operation to detect the address conflict in the global configuration mode. The **no** form of this command can be used to restore it to the default configuration.

ip dhcp ping timeout *milli-seconds*

no ip dhcp ping timeout

Parameter description

Parameter	Description
milli-seconds	Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds.

Default The default timeout is 500 seconds.

Command mode Global configuration mode.

Usage guidelines This command defines the time that the DHCP server waits for a ping response packet.

Examples In the configuration example below, the waiting time of the ping response packet is 600ms.

```
ip dhcp ping timeout 600
```

Related commands

Command	Description
clear ip dhcp conflict	Clear the DHCP history conflict record.
ip dhcp ping packets	Define the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
show ip dhcp conflict	Show the address conflict the DHCP server detects when it assigns an IP address.

23.1.13 ip dhcp pool

Use this command to define a name of the DHCP address pool and enter into the DHCP address pool configuration mode in the global configuration mode.The **no** form of this command can be used to delete the DHCP address pool.

ip dhcp pool *pool-name*

no ip dhcp pool *pool-name*

Parameter description

Parameter	Description
pool-name	A string of characters and positive integers, for instance, mypool or 1.

Default	No DHCP address pool is defined by default.
Command mode	Global configuration mode.
Usage guidelines	Execute the command to enter into the DHCP address pool configuration mode: `DES-7210(dhcp-config)#` In this configuration mode, configure the IP address range, the DNS server and the default gateway.
Examples	The configuration example below defines a DHCP address pool with the name mypool0. `ip dhcp pool mypool0`

Related commands

Command	Description
host	Define the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp excluded-address	Define the IP addresses that the DHCP server cannot assign to the clients.
network (DHCP)	Define the network number and network mask of the DHCP address pool.

23.1.14 lease

Use this command to define the lease time of the IP address that the DHCP server assigns to the client in the DHCP address pool configuration mode. The **no** form of this command can be used to restore it to the default configuration.

lease { *days* [*hours*] [*minutes*] | **infinite** }

no lease

Parameter description

Parameter	Description
days	Lease time in days
hours	(Optional) Lease time in hours. It is necessary to define the days before defining the hours.
minutes	(Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes.
infinite	Infinite lease time.

Default	The lease is 1 days, by default.
Command mode	DHCP address pool configuration mode.
Usage guidelines	When the lease is getting near to expire, the DHCP client will send the request of renewal of lease. In general, the DHCP server will allow the renewal of lease of the original IP address.

Examples	The configuration example below sets the DHCP lease to 1 hour.
	`lease 0 1`
	The configuration example below sets the DHCP lease to 1 minute.
	`lease 0 0 1`

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.15 netbios-name-server

Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the WINS server.

netbios-name-server *ip-address* [*ip-address2…ip-address8*]

netbios-name-server

Parameter description

Parameter	Description
ip-address	IP address of the WINS server. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) IP addresses of WINS servers. Up to 8 WINS servers can be configured.

Default	No WINS server is defined, by default.
Command mode	DHCP address pool configuration mode.

Usage guidelines

When more than one WINS server is defined, the former has higher priory. The DHCP client will select the next WINS server only when its communication with the former WINS server fails.

Examples

The configuration example below specifies the WINS server 192.168.12.3 for the DHCP client.

```
netbios-name-server 192.168.12.3
```

Related commands

Command	Description
ip address dhcp	Enable the DHCP client on the interface to obtain the IP address.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.16 netbios-node-type

Use this command to define the node type of the master NetBIOS of the Microsoft DHCP client in the DHCP address configuration mode. The **no** form of this command can be used to delete the configuration of the NetBIOS node type.

netbios-node-type *type*

no netbios-node-type

Parameter description

Parameter	Description
type	Type of node in two modes: Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available: ■ 1: b-node. ■ 2: p-node. ■ 4: m-node. ■ 8: h-node. String: ■ b-node: broadcast node ■ p-node: peer-to-peer node ■ m-node: mixed node ■ h-node: hybrid node

Default

No type of the NetBIOS node is defined, by default.

Command mode	DHCP address pool configuration mode.
Usage guidelines	There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received. By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.
Examples	The configuration example below sets the NetBIOS node of Microsoft DHCP client as Hybrid. `netbios-node-type h-node`

Related commands

Command	Description
ip dhcp pool	Define the name of DHCP address pool and enter into the DHCP address pool configuration mode.
netbios-name-server	Configure the WINS name server of the Microsoft DHCP client NETBIOS.

23.1.17 network (DHCP)

Use this command to define the network number and network mask of the DHCP address pool in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the definition.

network *net-number net-mask*

no network

Parameter description

Parameter	Description
net-number	Network number of the DHCP address pool

	net-mask	Network mask of the DHCP address pool. If the network mask is not defined, the natural network mask will be used by default.

Default No network number or network mask is defined, by default.

Command mode DHCP address pool configuration mode.

Usage guidelines

This command defines the subnet and subnet mask of a DHCP address pool, and provides the DHCP server with an address space which can be assigned to the clients. Unless excluded addresses are configured, all the addresses of the DHCP address pool can be assigned to the clients. The DHCP server assigns the addresses in the address pool orderly. If the DHCP server found an IP address is in the DHCP binding table or in the network segment, it checks the next until it assigns an effective IP address.

The **show ip dhcp binding** command can be used to view the address assignment, and the **show ip dhcp conflict** command can be used to view the address conflict detection configuration.

Examples

The configuration example below defines the network number of the DHCP address pool as 192.168.12.0, and the network mask as 255.255.255.240.

```
network 192.168.12.0 255.255.255.240
```

Related commands

Command	Description
ip dhcp excluded-address	Define the IP addresses that the DHCP server cannot assign to the clients.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.18 next-server

Use this command to define the startup sever list that the DHCP client accesses during startup in the DHCP address configuration mode. The **no** form of this command can be used to delete the definition of the startup server list.

next-server *ip-address* [*ip-address2…ip-address8*]

no next-server

Parameter description

Parameter	Description
ip-address	Define the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) Up to 8 startup servers can be configured.

Default N/A.

Command mode DHCP address pool configuration mode.

Usage guidelines When more than one startup server is defined, the former will possess higher priory. The DHCP client will select the next startup server only when its communication with the former startup server fails.

Examples The configuration example below specifies the startup server 192.168.12.4 for the DHCP client.

```
next-server 192.168.12.4
```

Related commands

Command	Description
bootfile	Define the default startup mapping file name of the DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.
ip help-address	Define the Helper address on the interface.
option	Configure the option of the DES-7200 software DHCP server.

23.1.19 option

Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. The **no** form of this command can be used to delete the definition of option.

option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

no option

Parameter description

Parameter	Description
code	Define the DHCP option codes.
ascii *string*	Define an ASCII string.
hex *string*	Define a hex string.
ip *ip-address*	Define an IP address list.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

The DHCP provides a mechanism to transmit the configuration information to the host in the TCP/IP network. The DHCP message has a variable option field that can be defined according to the actual requirement. The DHCP client needs to carry the DHCP message with 32 bytes of option information at least. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the definition of current DHCP option, refer to RFC 2131.

Examples

The configuration example below defines the option code 19, which determines whether the DHCP client can enable the IP packet forwarding. 0 indicates to disable the IP packet forwarding, and 1 indicates to enable the IP packet forwarding. The configuration below enable the IP packet forwarding on the DHCP client.

```
option 19 hex 1
```

The configuration example below defines the option code 33, which provides the DHCP client with the static route information. The DHCP client will install two static routes: 1) the destination network 172.16.12.0 and the gateway 192.168.12.12, 2) the destination network 172.16.16.0 and the gateway 192.168.12.16.

```
option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0 192.168.12.16
```

Related commands

Command	Description
ip dhcp pool	Define the name of the DHCP address pool and enter into the DHCP address pool configuration mode.

23.1.20 service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in the global configuration mode. The **no** form of this command can be used to disable the DHCP server and the DHCP relay.

service dhcp

no service dhcp

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.
Examples	In the following configuration example, the device has enabled the DHCP server and the DHCP relay feature. `service dhcp`

Related commands

Command	Description
show ip dhcp server statistics	Show various statistics information of the DHCP server.

23.2 Showing and Monitoring Commands

- **clear ip dhcp binding**
- **clear ip dhcp conflict**
- **clear ip dhcp server statistics**
- **debug ip dhcp client**
- **debug ip dhcp server**
- **show dhcp lease**

- **show ip dhcp binding**
- **show ip dhcp conflict**
- **show ip dhcp server statistics**

23.2.1 clear ip dhcp binding

Use this command to clear the DHCP binding table in the privileged user mode:

clear ip dhcp binding { * | *ip-address* }

Parameter description

Parameter	Description
*	Delete all DHCP bindings.
ip-address	Delete the binding of the specified IP addresses.

Default

N/A.

Command mode

Privileged mode.

Usage guidelines

This command can only clear the automatic DHCP binding, but the manual DHCP binding can be deleted by the **no ip dhcp pool** command.

Examples

The example below clears the DHCP binding with the IP address 192.168.12.100.

```
clear ip dhcp binding 192.168.12.100
```

Related commands

Command	Description
show ip dhcp binding	Show the address binding of the DHCP server.

23.2.2 clear ip dhcp conflict

Use this command to clear the DHCP address conflict record in the privileged user mode:

clear ip dhcp conflict { * | *ip-address* }

Parameter description

Parameter	Description
*	Delete all DHCP address conflict records.
ip-address	Delete the conflict record of the specified IP addresses.

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	The DHCP server uses the ping session to detect the address conflict, while the DHCP client uses the address resolution protocol (ARP) to detect the address conflict. The **clear ip dhcp conflict** can be used to delete the history conflict record.
Examples	The example below clears all address conflict records. `clear ip dhcp conflict *`

Related commands

Command	Description
ip dhcp ping packets	Define the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
show ip dhcp conflict	Show the address conflict that the DHCP server detects when it assigns an IP address.

23.2.3 clear ip dhcp server statistics

Use this command to reset the counter of the DHCP server in the privileged user mode.

clear ip dhcp server statistics

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	The DHCP server carries out the statistics counter, records the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also carries out the statistics to the number of sent and received DHCP messages. The **clear ip dhcp server statistics** command can be used to delete the history counter record and carry out the statistics starting from scratch.
Examples	The example below clears the statistics record of the DHCP server.

	`clear ip dhcp server statistics`

Related commands	**Command**	**Description**
	show ip dhcp server statistics	Show the statistics record of the DHCP server.

23.2.4 debug ip dhcp client

Use this command to carry out the DHCP client debugging in the privileged user mode:

debug ip dhcp client

no debug ip dhcp client

Parameter description	N/A.
Default	Disabled.
Command mode	Privileged mode.
Usage guidelines	This command is used to show the main message content of the DHCP client during the interaction of the servers and the processing status.
Examples	The example below turns on the debugging switch of the DHCP client in the equipment. `debug ip dhcp client`

23.2.5 debug ip dhcp server

Use this command to carry out the DHCP Server debugging in the privileged user mode:

debug ip dhcp server

no debug ip dhcp server

Parameter description	N/A.
Default	Disabled.

Command mode	Privileged mode.
Usage guidelines	This command is used to show the main message content of the dhcp server during the interaction of the clients and the processing status.
Examples	The example below turns on the debugging switch of the DHCP server in the equipment. `debug ip dhcp server`

23.2.6 show dhcp lease

Use this command to show the lease information of the IP address obtained by the DHCP client.

show dhcp lease

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address.

Examples	The following is the result of the **show dhcp lease**.
	`DES-7210# show dhcp lease`
	`Temp IP addr: 192.168.5.71 for peer on Interface: FastEthernet0/0`
	`Temp sub net mask: 255.255.255.0`
	`DHCP Lease server: 192.168.5.70, state: 3 Bound`
	`DHCP transaction id: 168F`
	`Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs`
	`Temp default-gateway addr: 192.168.5.1`
	`Next timer fires after: 00:04:29`
	`Retry count: 0 Client-ID: redgaint-00d0.f8fb.5740-Fa0/0`

23.2.7 show ip dhcp binding

Use this command to show the binding condition of the DHCP address.

show ip dhcp binding [*ip-address*]

Parameter description

Parameter	Description
ip-address	(Optional) Only show the binding condition of the specified IP addresses.

Default

N/A.

Command mode

Privileged mode.

Usage guidelines

If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address.

Examples

The following is the result of the **show ip dhcp binding**.

```
DES-7210# show ip dhcp binding
IP address      client-ID   Lease expiration    Type
                Hardware address
192.168.1.2   00D0.f866.4777   IDLE          Manual
```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	The IP address to be assigned to the DHCP client.
Client-id/Hardware address	The client identifier or hardware address of the DHCP client.
Lease expiration	The expiration date of the lease. The Infinite indicates it is not limited by the time. The IDLE indicates the address is in the free status currently for it is not renewed or the DHCP client releases it actively.
Type	The type of the address binding.The Automatic indicates an IP address is assigned automatically, and the Manual indicates an IP address is assigned by manual.

Related commands	

Command	Description
clear ip dhcp binding	Clear the DHCP address binding table.

23.2.8 show ip dhcp conflict

Use this command to show the conflict history record of the DHCP sever.

show ip dhcp conflict

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	This command can show the conflict address list and excluded address list detected by the DHCP server.
Examples	The following is the output result of the **show ip dhcp conflict** command.

```
DES-7210# show ip dhcp conflict
IP address    Detection Method
 192.168.12.1    Ping

dhcpd excluded ipaddress
 192.168.12.100
```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	**The IP addresses which cannot be assigned to the DHCP client.**
Detection Method	**The conflict detection method.**
dhcpd excluded ipaddress	**The range of excluded addresses.**

Related commands	Command	Description
	clear ip dhcp confict	Clear the DHCP conflict record.

23.2.9 show ip dhcp server statistics

Use this command to show the statistics of the DHCP server.

show ip dhcp server statistics

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	This command shows the statistics of the DHCP server.
Examples	The following is the output result of the **show ip dhcp server statistics** command.

```
DES-7210# show ip dhcp server statistics
Address pools            4
Automatic bindings       4
Manual bindings          0
Expired bindings         0
Malformed messages 2

Message                 Received
BOOTREQUEST             216
DHCPDISCOVER            33
DHCPREQUEST             25
DHCPDECLINE             0
DHCPRELEASE             1
DHCPINFORM              150

Message                 Sent
BOOTREPLY               16
DHCPOFFER               9
DHCPACK                 7
DHCPNAK                 0
```

The meaning of various fields in the show result is described as

follows.

Field	Description
Address pools	Number of address pools.
Automatic bindings	Number of automatic address bindings.
Manual bindings	Number of manual address bindings.
Expired bindings	Number of expired address bindings.
Malformed messages	Number of malformed messages received by the DHCP.
Message Received or Sent	Number of the messages received and sent by the DHCP server respectively.

Related commands

Command	Description
clear ip dhcp server statistics	Delete the DHCP server statistics.

24 DHCP Relay Configuration Commands

24.1 DHCP Relay Configuration Command

DHCP configuration includes the following commands:

- **service dhcp**
- **ip helper-address**

24.1.1 service dhcp

Use this command to enable the DHCP relay in the global configuration mode. The **no** form of this command can disable the DHCP relay.

service dhcp

no service dhcp

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP response packets to the DHCP client, serving as the relay for DHCP packets.
Examples	In the following configuration example, the device has enabled the DHCP server and the DHCP relay. `service dhcp`

Related	**Command**	**Description**

commands	**ip helper-address [vrf]** *A.B.C.D*	Add an IP address of the DHCP server.

24.1.2 ip helper-address

Use this command to add an IP address of the DHCP server. The **no** form of this command deletes an IP address of the DHCP server.

The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.

Default	N/A.
Command mode	Global configuration mode, interface configuration mode.
Usage guidelines	This command can configure more than one DHCP server address in the interface modes. One DHCP request of this interface will be sent to these servers. You can select one for confirmation. The global configuration and port-based configuration of the vrf are slightly different. In the global configuration mode, if the vrf is not specified, the default address of the current server does not belong to any vrf. In the port-based configuration, if the vrf is not specified, the current default server and port configurations belong to the same vrf.

Examples	Set the addresses of two servers in the same vrf. One server address is 61.154.26.49, and the address of the vrf-based server with instance name of local is 192.168.197.1.
	`ip helper-address 61.154.26.49`
	`ip helper-address vrf local 192.168.197.1`

Related commands	**Command**	**Description**
	service dhcp	Enable the DHCP relay.

24.1.3 ip dhcp relay information option dot1x

Use this command to enable the **dhcp option dot1x** function.. The **no** form of the command is used to disable the **dhcp option dot1x** function.

Default	Disabled.

Command mode	Global configuration mode.
Usage guidelines	It is necessary to enable the DHCP Relay, and combine with the 802.1x related configuration to configure this command.
Examples	The following example enables the DHCP option dot1x function on the device. `Ip dhcp relay information option dot1x`

Related commands

Command	Description
service dhcp	Enable the DHCP Relay.
ip dhcp relay information option dot1x access-group	Configure the option dot1x acl.

24.1.4 ip dhcp relay information option dot1x access-group

Use this command to configure the **dhcp option dot1x acl**. The **no** form of this command is used to disable the **dhcp option dot1x acl**.

Default	No ACL is associated with.
Command mode	Global configuration mode.
Usage guidelines	Be sure that the ACL does not conflict with the existing ACE of the configured ACL on the interface.
Examples	The following example enables the dhcp option dot1x acl function. `Ip dhcp relay information option dot1x access-group` *`acl-name`*

Related commands

Command	Description
service dhcp	Enable the DHCP Relay.
ip dhcp relay information option dot1x	Enable the DHCP option dot1x function.

24.1.5 ip dhcp relay information option82

Use this command to configure to enable the **ip dhcp relay information option82** function. The **no** form of this command is used to disable the **ip dhcp relay information option82** function.

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	This command is exclusive with the **option dot1x** command.
Examples	The following example enables the ip dhcp relay *check server-id* function. `Ip dhcp relay check server-id`

Related commands

Command	Description
service dhcp	Enable the DHCP Relay.
ip dhcp relay information option dot1x	Enable the DHCP option dot1x function.

24.1.6 ip dhcp relay check server-id

Use this command to configure to enable the **ip dhcp relay check** *server-id* function. The **no** form of this command is used to disable the **ip dhcp relay information check** *server-id* function.

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Switch will select server to be sent according to server-id option when forwarding DHCP REQUEST via this command.
Examples	The following example enables switch by switch: t `Ip dhcp relay check server-id`

Related commands	Command	Description
	service dhcp	Enable the DHCP Relay.

24.1.7 ip dhcp relay suppression

Use this command to enable the DHCP binding globally. The **no** form of this command disables the DHCP binding globally and enables the **DHCP relay** suppression on the port.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	After executing this command, the system will not relay the DHCP request message on the interface.

Examples	The following example enables the relay suppression function on the interface 1.
	`DES-7210#`
	`DES-7210# configure terminal`
	`DES-7210(config)# interface fastEthernet 0/1`
	`DES-7210(config-if)# ip dhcp relay suppression`
	`DES-7210(config-if)# exit`
	`DES-7210(config)#`

Related commands	Command	Description
	service dhcp	Enable the DHCP Relay.

25 DNS Module Configuration Commands

25.1 Configuring Related Commands

25.1.1 ip domain-lookup

Use this command to enable the DNS to carry out the domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

ip domain-lookup

no ip domain-lookup

Default configuration	Enabled.
Command mode	Global configuration mode.
Usage guidelines	This command enables the domain name resolution function.
Examples	The following example enables the DNS domain name resolution function. `DES-7210(config)# ip domain-lookup`

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

25.1.2 ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

ip name-server *ip-address*

no ip name-server [*ip-address*]

Parameter description

Parameter	Description
ip-address	The IP address of the domain name server.

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

Add the IP address of the DNS server. Once this command is executed, the equipment will add a DNS server. When the device cannot obtain the domain name from a DNS server, it will attempt to send the DNS request to subsequent servers until it receives a response.

Up to 6 DNS servers are supported. You can delete a DNS server with the *ip-address* option or all the DNS servers.

Examples

```
DES-7210(config)# ip name-server 192.168.5.134
```

25.1.3 ip host

Use this command to configure the mapping of the host name and the IP address by manual. Use the **no** form of the command to remove the host list.

ip host *host-name ip-address*

no ip host *host*-name *ip-address*

Parameter description

Parameter	Description
host-name	The host name of the equipment
ip-address	The IP address of the equipment

Command mode	Global configuration mode.
Usage guidelines	To delete the host list, use the **no ip host** *host-name ip-address* command.
Examples	`DES-7210(config)# ip host switch 192.168.5.243`

Related commands

Command	Description
show hosts	Show the DNS related configuration information.

25.1.4 clear host

Use this command to clear the dynamically learned host name in the privileged user mode.

clear host [*host-name*]

Parameter description

Parameter	Description
host-name	Delete the dynamically learned host. "*" denotes to clear all the dynamically learned host names.

Command mode	Privileged mode.
Usage guidelines	You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** static configuration, 2) the DNS dynamic learning. Execute this command to delete the host name records learned by the DNS dynamically.
Examples	The following configuration will delete the dynamically learned mapping records from the host name-IP address buffer table. `clear host *`

Related commands

Command	Description
show hosts	Show the host name buffer table.

25.1.5 show hosts

Use this command to display DNS configuration.

show hosts

Command mode	Privileged mode.
Usage guidelines	Show the DNS related configuration information.
Examples	DES-7210# show hosts Name servers are: static host type address switch static 192.168.5.243 www.dlink.com dynamic 192.168.5.123

Related commands

Command	Description
ip host	Configure the host name and IP address mapping by manual.
ip name-server	Configure the DNS server.

26 SNTP Configuration Commands

26.1 Configuring Related Commands

26.1.1 sntp enable

Use this command to enable the SNTP function. Use the **no** form of this command to restore the default value.

[no] sntp enable

Default configuration	Disabled
Command mode	Global configuration mode.
Usage guidelines	This command shows the parameters of SNTP.
Examples	`DES-7210(config)# sntp enable`

Related commands

Command	Description
show sntp	Show the SNTP configuration.
clock update-calendar	Synchronize the software click with the hardware clock.
clock set	Set the software clock.

26.1.2 sntp server

Use this command to set the SNTP server. Since the SNTP protocol is completely compatible with the NTP protocol, you can configure the SNTP server as the public NTP server on the Internet.

sntp server *ip-addr*

no sntp server

Parameter description

Parameter	Description
ip-addr	The IP address of the NTP/SNTP server.

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

The **show sntp** command shows the parameters of SNTP.

Examples

```
DES-7210(config)# sntp server 192.168.4.12
```

Related commands

Command	Description
show sntp	Show the SNTP configuration.
sntp enable	Enable SNTP.

26.1.3 sntp interval

Use this command to set the interval for the SNTP Client to synchronize its clock with the NTP/SNTP Server.

Note that the set interval will not take effect immediately. To this end, execute the **sntp enable** command after setting the interval.

sntp interva *seconds*

no sntp interval

Parameter description

Parameter	Description
seconds	Synchronization interval in 60 to 65535

		seconds

Default configuration	1800s
Command mode	Global configuration mode.
Usage guidelines	The **show sntp** command shows the parameters of SNTP.
Examples	`DES-7210(config)# sntp interval 3600`

Related commands

Command	Description
sntp enable	Enable SNTP.
show sntp	Show the SNTP configuration.
clock update-calendar	Synchronizes the software clock with the hardware clock.

26.2 Showing Related Command

26.2.1 show sntp

Use this command to show the parameters of SNTP.

Command mode	Privileged mode.
Usage guidelines	This command shows the parameters of SNTP.

Examples

```
DES-7210# show  sntp
SNTP state          : Enable
SNTP server         : 192.168.4.12
SNTP sync interval   : 60
Time zone            : +8
```

Related commands

Command	Description
sntp enable	Enable SNTP.

show sntp	Show the SNTP configuration.

27 NTP Configuration Commands

27.1 NTP Configuring Related Commands

NTP configuration includes the following commands:

- **no ntp**
- **ntp access-group**
- **ntp authenticate**
- **ntp authentication-key**
- **ntp disable**
- **ntp master**
- **ntp server**
- **ntp synchronize**
- **ntp trusted-key**
- **ntp update-calendar**

27.1.1 no ntp

Use this command to disable the **ntp** synchronization service with the time server and clear all configuration information of **ntp**.

no ntp

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.

Usage guidelines

By default, the NTP function is disabled. However, once the NTP server or the NTP security identificaiton mechanism is configured, the NTP function will be enabled.

Examples

The configuration example below disables the NTP service.

```
no ntp
```

Related commands

Command	Description
ntp server	Specify a NTP server.

27.1.2 ntp access-group

Use this command to configure the access control priority of the ntp service. Use the **no** form of this command to cancel the access control priority.

ntp access-group {peer | serve | serve-only | query-only} *access-list-number* | *access-list-name*

no ntp access-group {peer | serve | serve-only | query-only} *access-list-number* | *access-list-name*

Parameter description

Parameter	Description
peer	Not only allow to request for the time of and control the local NTP service, but also allow the time synchronization of the local and the peer.
serve	Allow to request for the time of and control the local NTP service only, the time synchronization of the local and the peer is not allowed.
serve-only	Allow to request for the time of local NTP service only.
query-only	Allow to control and search for the local NTP service.
access-list-number	The IP access control list number, in the range of 1-99 and 1300-1999.
access-list-name	The IP access control list name.

Default

No NTP access control rule has been configured by default.

Command mode

Global configuration mode.

Usage guidelines

Use this command to configure the access control priority of the ntp service. NTP services access control function provides a minimal security measures (more secure way is to use the NTP authentication mechanism).

When an access request arrives, NTP service matches the rules in accordance with the sequence from the smallest to the largest to access restriction, and the first matched rule shall prevail. The matching order is peer, serve, serve-only, query-only.

Caution:

Control query function is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

If you do not configure any access control rules, then all accesses are allowed. However, once the access control rules are configured, only the rule that allows access can be carried out.

Examples

The following example shows how to allow the peer device in acl1 to control the query, request for and synchronize the time with the local device; and limit the peer device in acl2 to request the time for the local device:

```
DES-7210(config)# ntp access-group peer 1

DES-7210(config)# ntp access-group serve-only 2
```

Related commands

Command	Description
ip access-list	Create the IP access control list.

27.1.3 ntp authenticate

Use this command to enable NTP authentication globally.

ntp authenticate

no ntp authenticate

Parameter description

N/A.

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	If the global security identification mechanism is not used, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the security identification mechanism and configure other keys globally. The authentication standard is the trusted key specified by **ntp authentication-key** and **ntp trusted-key**.

Examples	After an authentication key is configured and specified as the global trusted key, enable the authentication mechanism.
	`ntp authentication-key 6 md5 wooooop`
	`ntp trusted-key 6`
	`ntp authenticate`

Related commands

Command	Description
ntp authentication-key	Set the global authentication key.
ntp trusted-key	Configure the global trusted key.

27.1.4 ntp authentication-key

Use this command to configure a global NTP authentication key for the NTP server.

ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

no ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

Parameter description

Parameter	Description
key-id	Key ID
key-string	Key string
enc-type	(Optional) Whether this key is encrypted, where, 0 indicates the key is not encrypted, 7 indicates the key is encrypted simply.

Default	N/A.

Command mode	Global configuration mode.
Usage guidelines	Configure the global authentication key and adopt **md5** for encryption. Each key presents the unique *key-id* identification. Customers can use the **ntp trusted-key** to set the key of *key-id as* the global trusted key. The upeer limit of the keys is 1024. However, each server can only support one key.
Examples	The following example configures an authentication key with ID 6. `ntp authentication-key 6 md5 wooooop`

Related commands

Command	Description
ntp authenticate	Enable the global security identification mechanism.
ntp trusted-key	Configure the global trusted key.
ntp server	Specify a NTP server.

27.1.5 ntp disable

Use this command to disable the function of receiving the NTP message on the interface.

ntp disable

Parameter description	N/A.
Default	The NTP message is received on the interface, by default.
Command mode	Interface configuration mode.
Usage guidelines	The NTP message received on any interface can be provided to the client to carry out the clock adjustment. The function can be set to shield the NTP message received from the corresponding interface. Note: The interface that is configured with this command can receive and send IP packets. No this command is configured on other interfaces.

Examples

The configuration example below disables the function of receiving the NTP message on the interface.

```
no ntp
```

27.1.6 ntp master

Use this command to configure the local time as the NTP master(the local time reference source is reliable), providing the synchronizing time for other devices. Use the **no** form of this command to cancel the NTP master settings.

ntp master [*stratum*]

no ntp master

Parameter description

Parameter	Description
stratum	Specify the stratum where the local time is, in the range of 1-15. The defaut stratum is 8.

Default

No NTP master is configured, by default.

Command mode

Global configuration mode.

Usage guidelines

In general, the local system synchronizes the time from the external time source directly or indirectly. However, if the time synchronization of local system fails for the network connection trouble, ect, use the command to set the reliable reference source of the local time, providing the synchronized time for other devices.

Once set, the system time can not be synchronized to the time source with higher starum.

Caution:

Using this command to set the local time as the master (in particular, specify a lower starum value), is likely to be covered by the effective clock source. If multiple devices in the same network use this command, the time synchronization instability may occur due to the time difference between the devices.

In addition, before using this command, if the system has never been synchronized with an external clock source, it is necessary to manually calibrate the system clock to prevent too much bias.

Examples	The configuration example below configures the reliable local time reference source and set the time stratum 12: `DES-7210(config)# ntp master 12`

27.1.7 ntp server

Use this command to specify a NTP server for the NTP client.

ntp server *ip-addr* [**version** *version*] [**source** *if-name*] [**key** *keyid*][**prefer**]

no ntp server *ip-addr*

Parameter description

Parameter	Description
ip-addr	Set the IP address of the NTP server.
version	(Optional) Specify the version (1-3) of NTP, NTPv3 by default.
if-name	(Optional) Specify the source interface from which the NTP message is sent (L3 interface).
keyid	(Optional) Specify the encryption key adopted when communication with the corresponding server.
prefer	(Optional) Specify the corresponding server as the prefer server.

Default	No NTP server is configured, by default.
Command mode	Global configuration mode.

Usage guidelines	At present, our system only support clients other than servers, and the upeer limit of supported synchronous servers are 20. To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server. In the same condition (for instance, precision), the prefer clock is used for synchronization. It should be noted that the configured interface is that configured with the IP address and can communicate with the corresponding NTP server when you configure the source interface of the NTP message.
Examples	The configuration example below configures the equipment in the network as NTP server. `ntp server 192.168.210.222`

Related commands

Command	Description
no ntp	Disable the NTP service function.

27.1.8 ntp synchronize

Use this command to synchronize the realtime.

ntp synchronize

no ntp synchronize

Parameter description	N/A.
Default	N/A.
Command mode	Global configuration mode.

Usage guidelines	8 consecutive packets are synchronized for the first synchronization of NTP and each server. Then the synchronization occurs every one minute. This command is used to complete the instant synchronization during the interval of auto-sync.
Examples	The following example synchronizes the NTP realtime. `ntp synchronize`

Related commands

Command	Description
ntp server	Specify a NTP server.

27.1.9 ntp trusted-key

Use this command to set a key at the global trusted key.

ntp trusted-key *key-id*

no ntp trusted-key *key-id*

Parameter description

Parameter	Description
key-id	Global trusted key ID

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

Examples	The following configures an authentication key and sets it as the corresponding server trusted key.
	`ntp authentication-key 6 md5 wooooop`
	`ntp trusted-key 6`
	`ntp server 192.168.210.222 key 6`

Related commands

Command	Description
ntp authenticate	Enable the security authentication mechanism.

	ntp authentication-key	Set the NTP authentication key.
	ntp server	Specify a NTP server.

27.1.10 ntp update-calendar

Use this command to update the calendar for the NTP client using the synchronization time of the external time source. Use the **no** form of this command to disable the update-calendar function

ntp update-calendar

no ntp update-calendar

Parameter description	N/A.
Default	By default, update the calendar periodically is not configured.
Command mode	Global configuration mode.
Usage guidelines	By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.
Examples	The following configures the NTP update calendar periodically. `DES-7210(config)# ntp update-calendar`

27.2 Showing and Monitoring Commands

- **debug ntp**
- **show ntp status**

27.2.1 debug ntp

Use this command to show the NTP debugging information.

debug ntp

no debug ntp

Parameter description	N/A.
Default	Disabled.
Command mode	Privileged mode.
Usage guidelines	To carry out the NTP function debugging, output necessary debugging information to implement the failure diagnosis and troubleshooting by this command.
Examples	The example below enables the NTP debugging switch. `debug ntp`

27.2.2 show ntp status

Use this command to show the NTP information.

show ntp status

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	If the NTP service of the system is enabled, show current NTP information. This command will not print any information before the synchronization server is added for the first time.
Examples	The example below shows the NTP information of current system. `show ntp status`

28 UDP-Helper Module Configuration Commands

28.1 Configuration Related Commands

28.1.1 udp-helper enable

Use this command to enable the forwarding function of the UDP broadcast message. The **no udp-helper enable** command is used to disable the forward function of the UDP broadcast message.

By default, the forwarding of the UDP broadcast message is disabled.

udp-helper enable

no udp-helper enable

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Enable the forwarding function of UDP-Helper. The UDP broadcast messages from the port 69,53,37,137,138,49 are forwarded by default.
Examples	The following is an example of enabling the UDP forwarding function. `DES-7210(config)# udp-helper enable`

Related commands

Command	Description
ip forward-protocol	Configure the UDP port to enable the forwarding funciton.

28.1.2 ip helper-address

Use this command to configure the destination server which the UDP broadcast message will be forwarded to. Use the **no** form of this command to delete the destination server.

ip helper-address *address*

no ip helper-address *address*

Parameter description

Parameter	Description
address	IP address of the destination server in the dotted decimal format. Each interface can support up to 20 server addresses.

Default configuration

N/A.

Command mode

Interface configuration mode.

Usage guidelines

Up to 20 destination servers can be configured on an interface. Once the forwarding destination server is configured someone an interface and UDP-Helper is enabled, the broadcast message of the specified port received from this interface will be sent to the destination server configured on this interface in unicast form.

Use the **no ip helper-address** to remove the forwarding destination server.

Examples

The following is an example of configuring the destination server where the UDP broadcast message will be forwarded to.

```
DES-7210(config-if)# ip helper-address 192.168.100.1
```

Related commands

Command	Description
ip forward-protocol	Configure the specified UDP port to enable forwarding.

28.1.3 ip forward-protocol

Use this command to configure the UDP port to enable forwarding. Use the **no** form of this command to disable forwarding on the UDP port.

ip forward-protocol udp [*port* | **tftp | domain | time | netbios-ns | netbios-dgm | tacacs]**

no ip forward-protocol udp [*port* | **tftp | domain | time | netbios-ns | netbios-dgm | tacacs]**

Parameter description

Parameter	Description
port	Port to enable forwarding. If this parameter is not specified, the broadcast message from the ports 69,53,37,137,138,49 will be forwarded by default.
tftp	Trivial File Transfer Protocol(69) Forward the broadcast message from port 69.
domain	Domain Name System(53) Forward the broadcast message from port 53.
time	Time service(37) Forward the broadcast message from port 37.
netbios-ns	NetBIOS Name Service(137) Forward the broadcast message from port 137.
netbios-dgm	NetBIOS Datagram Service(138) Forward the broadcast message from port 138.
tacacs	TAC Access Control System(49) Forward the broadcast message from port 49.

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

Enabling the UDP-Helper function will forward the broadcast message of the UDP ports 69,53,37,137,138,49 without any additional configuration, by default.

```
DES-7210(config)# ip forward-protocol udp 134
```

Related commands

Command	Description
udp-helper enable	Enable the forwarding of the UDP broadcast message.

	ip forward-protocol	Configure the UDP port to enalbe forwarding.

29 SNMP Configuration Command

29.1 Configuration Related Commands

The SNMP configuration includes the following related commands:

- **no snmp-server**
- **snmp-server chassis-id**
- **snmp-server community**
- **snmp-server contact**
- **snmp-server enable traps**
- **snmp-server host**
- **snmp-server location**
- **snmp-server packetsize**
- **snmp-server queue-length**
- **snmp-server system-shutdown**
- **snmp-server trap-source**
- **snmp-server trap-timeout**
- **snmp-server user**
- **snmp-server group**
- **snmp-server view**
- **snmp-server if-index persists**

29.1.1 no snmp-server

Use this command to disable the SNMP agent function in the global configuration mode.

no snmp-server

Default configuration	Disabled.

Command mode	Global configuration mode.
Usage guidelines	This command disables the SNMP agent services of all versions supported on the device.
Examples	The example below disables the SNMP agent service. `DES-7210(config)# no snmp-server`

29.1.2 snmp-server chassis-id

Use this command to specify the SNMP system sequential number in the global configuration mode. The **no** form of this command is used to restore it to the initial value.

snmp-server chassis-id *text*

no snmp-server chassis-id

Parameter description

Parameter	Description
text	Text of the system sequential number, numerals or characters.

Default configuration	The default sequence number is 60FF60.
Command mode	Global configuration mode.
Usage guidelines	The SNMP system sequence number is generally the sequence number of the machine to facilitate the device identification. The sequence number can be viewed through the **show snmp** command.
Examples	The example below specifies the SNMP system sequence number as 123456: `DES-7210(config)# snmp-server chassis-id 123456`

Related commands

Command	Description
show snmp	Show the SNMP information.

29.1.3 snmp-server community

Use this command to specify the SNMP community access string in the global configuration mode. The **no** format of the command cancels the SNMP community access string.

snmp-server community *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*] [*number*]

no snmp-server community *string*

Parameter description

Parameter	Description
string	Community string, which is equivalent to the communication password between the NMS and the SNMP agent
view-name	Name of the view used for management
ro	Indicate that the NMS can only read the variables of the MIB.
rw	Indicate that the NMS can read and write the variables of the MIB.
number	Sequence number of the ACL in the range of 0 to 99, which specifies the IP address range of the NMS that are permitted to access the MIB
ipaddr	IP address of the NMS accessing the MIB

Default configuration

All communities are read only by default.

Command mode

Global configuration mode.

Usage guidelines

This command is the first important command to enable the SNMP agent function. It specifies the community attribute, range of the NMSs that can access the MIB, and more.

To disable the SNMP agent function, execute the command **no snmp-server**.

Examples

The example below restricts the access to the MIB through the access list, which allows only the NMS of the IP address 192.168.12.1 to access the MIB.

```
DES-7210(config)# access-list 2 permit 192.168.12.1
DES-7210(config)# access-list 2 deny any
DES-7210(config)# snmp-server community public ro 2
```

Related commands

Command	Description
access-list	Define the access list.

29.1.4 snmp-server contact

Use this command to specify the SNMP system contact in the global configuration mode. The **no** form of this command is used to delete the system contact.

snmp-server contact *text*

no snmp-server contact

Parameter description

Parameter	Description
text	String describing the system contact.

Default configuration

N/A.

Command mode

Global configuration mode.

Examples

The example below specifies the SNMP system contract i-net800@i-net.com.cn:

```
DES-7210(config)# snmp-server contact i-net800@i-net.com.cn
```

Related commands

Command	Description
show snmp-server	Check the SNMP information.
no snmp-server	Disable the SNMP agent function.

29.1.5 snmp-server enable traps

Use this command to enable the SNMP server to actively send the SNMP Trap massage to NMS when some emergent and important events occur in the global configuration mode. The **no** format of this command is used to disable the SNMP server to actively send the SNMP Trap massage to NMS.

snmp-server enable traps [snmp]

no snmp-server enable traps

Parameter description

Parameter	Description
snmp	Enable the trap notification of SNMP events.

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines

This command must work with the global configuration command **snmp-server** to send the SNMP Trap message.

Examples

The example below enables the SNMP server to actively send the SNMP Trap message.

```
DES-7210(config)# snmp-server enable traps snmp
DES-7210(config)# snmp-server host 192.168.12.219 public snmp
```

Related commands

Command	Description
snmp-server host	Specify the SNMP host to send the SNMP Trap message.

29.1.6 snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message in the global configuration mode. The **no** form of this command is used to remove the specified SNMP host.

snmp-server host {*host-addr*| **ipv6** *ipv6-addr*} [**vrf** *vrfname*] [**traps**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]] *community-string* [**udp-port** *port-num*][*notification-type*]

no snmp-server host *host-addr*

Parameter description

Parameter	Description
host-addr	SNMP host address
ipv6-addr	SNMP host address(ipv6)
vrfname	Set the name of vrf forwarding table
version	SNMP version: V1, V2C or V3
auth | noauth | priv	Security level of SNMPv3 users
community-string	Community string or username (SNMPv3 version)

	port-num	Port of the SNMP host
	notification-type	The type of the SNMP trap message sent actively, such as **snmp**.

Default configuration

By default, no SNMP host is specified.

If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included.

Command mode

Global configuration mode.

Usage guidelines

This command must work with the **snmp-server enable traps** command in the global configuration mode to actively send the SNMP trap messages to NMS.

It is possible to configure multiple SNMP hosts to receive the SNMP Trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages have to be configured.

Examples

The example below specifies an SNMP host to receive the SNMP event trap:

```
DES-7210(config)# snmp-server host 192.168.12.219 public snmp
```

Related commands

Command	Description
snmp-server enable traps	Enable to send the SNMP trap message.

29.1.7 snmp-server location

Use this command to set the SNMP system location information in the global configuration mode. The **no** form of this command is used to remove the specified SNMP system location information.

snmp-server location *text*

no snmp-server location

Parameter description

Parameter	Description
text	String describing the system

Default configuration	Null
Command mode	Global configuration mode.
Examples	The example below specifies the system information: `DES-7210(config)# snmp-server location start-technology-city 4F of A Buliding`

Related commands

Command	Description
snmp-sever contact	Specify the system contact information.

29.1.8 snmp-server packetsize

Use this command to specify the maximum size of the SNMP packet in the global configuration mode. The **no** form of this command is used to restore it to the default value.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter description

Parameter	Description
byte-count	Packet size in the range of 484 to 17876 bytes

Default configuration	1,500 bytes.
Command mode	Global configuration mode.
Examples	The example below specifies the maximum SNMP packet size as 1,492 bytes: `DES-7210(config)# snmp-server packetsize 1492`

Related commands

Command	Description
snmp-server queue-length	Specify the length of the SNMP trap message queue.

29.1.9 snmp-server queue-length

Use this command to specify the length of the SNMP trap message queue in the global configuration mode.

snmp-server queue-length *length*

Parameter description

Parameter	Description
length	Queue length in the range of 1 to 1000

Default configuration

10.

Command mode

Global configuration mode.

Usage guidelines

The SNMP trap message queue is used to store the SNMP trap messages. This command can be used to adjust the size of the SNMP trap message queue to control the speed to sending the SNMP trap messages.

The maximum speed to send messages is 4 messages per second.

Examples

The example below specifies the speed to send the trap message to 4 messages per second:

```
DES-7210(config)# snmp-server queue-length 4
```

Related commands

Command	Description
snmp-server packetsize	Specify the maximum size of the SNMP packet.

29.1.10 snmp-server system-shutdown

Use this command to enable the SNMP system restart notification function in the global configuration mode. The **no** form of this command is used to disable the SNMP system notification function.

snmp-server system-shutdown

no snmp-server system-shutdown

Default configuration

Disabled.

Command mode	Global configuration mode.
Usage guidelines	This command is used to enable the SNMP system restart notification function. The DES-7200 sends the SNMP trap messages to the NMS to notify the system pending before the device is reloaded or rebooted.
Examples	The example below enables the SNMP system restart notification function: `DES-7210(config)# snmp-server system-shutdown`

29.1.11 snmp-server trap-source

Use this command to specify the source of the SNMP trap message in the global configuration mode. The **no** form of this command is used to restore it to the default value.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter description

Parameter	Description
interface	Interface to be used as the source of the SNMP trap message

Default configuration	The IP address of the interface where the NMP message is sent from is just the source address.
Command mode	Global configuration mode.
Usage guidelines	By default, the IP address of the interface where the NMP message is sent from is just the source address. For easy management and identification, this command can be used to fix a local IP address as the SNMP source address.
Examples	The example below specifies the IP address of Ethernet interface 0 as the source of the SNMP trap message: `DES-7210(config)# snmp-server trap-source fastethernet 0`

	Command	Description
Related commands	**snmp-server enable traps**	Enable the sending of the SNMP trap message.
	snmp-server enable host	Specify the NMS host to send the SNMP trap message.

29.1.12 snmp-server trap-timeout

Use this command to define the retransmission timout time of the SNMP trap message in the global configuration mode. The **no** form of this command is used to restore it to the default value.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

	Parameter	Description
Parameter description	*seconds*	Timeout (in seconds) of retransmit the SNMP trap message

Default configuration	30s.
Command mode	Global configuration mode.
Examples	The example below specifies the timeout period as 60 seconds. `DES-7210(config)# snmp-server trap-timeout 60`

	Command	Description
Related commands	**snmp-server queue-length**	Specify the length of the SNMP trap message queue.
	snmp-server enable host	Specify the NMS host to send the SNMP trap message.

29.1.13 snmp-server user

Use this command to set the SNMP name in the global configuration mode**.** The **no** form of this command is used to delete the user.

snmp-server user *username groupname* {**v1 | v2 | v3** [**encrypted**] [**auth** {**md5 | sha**} *auth-password*] [**priv des56** *priv-password*]} [**access** {*num* | *name*}]

no snmp-server user *username groupname* {**v1 | v2c | v3** }

Parameter description

Parameter	Description
username	User name
groupname	Group name of the user.
v1 | v2 | v3	SNMP version. But only SNMPv3 supports the following security parameters.
Encrypted	Input the password in cipher text mode. In cipher text mode, input continuous HEX alphanumeric characters. Note that the authentication password of MD5 has a length of 16 characters, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can only be used by the local SNMP engine on the switch.
Auth	Authentication mode: **md5** and **sha.** *auth-password*: Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key
priv	Encryption mode. **des56** refers to 56-bit DES encryption protocol. *priv-password*: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.

Default configuration

N/A.

Command mode

Global configuration mode.

Examples

The example below configures an SNMPv3 user with MD5 authentication and DES encryption:

```
DES-7210(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr
```

Related commands

Command	Description
show snmp user	Show the SNMP user configuration.

29.1.14 snmp-server group

Use this command to set the SNMP user group in the global configuration mode**.** The **no** form of this command is used to remove the user group.

snmp-server group ***groupnam****e* **{**v1 | v2c | v3 **{**auth | noauth | priv**}} [**read ***readview***][**write ***writeview***] [**access {***num* | ***name***}]**

no snmp-server group ***groupname*** {**v1 | v2c | v3** }

Parameter description

Parameter	Description
v1,v2c,v3	SNMP version
auth	Authenticate the messages transmitted by the user group without encryption. This applies to only SNMPv3.
noauth	Neither authenticate nor encrypt the messages transmitted by the user group. This applies to only SNMPv3.
priv	Authenticate and encrypt the messages transmitted by the user group. This applies to only SNMPv3.
readview	Associate with a read-only view.
writeview	Associate with a read-write view.

Default configuration

N/A.

Command mode

Global configuration mode.

Examples

The example below sets a user group.

```
DES-7210(config)# snmp-server group mib2user v3 priv read mib2
```

Related commands

Command	Description
show snmp group	Show the SNMP user group configuration.

29.1.15 snmp-server view

Use this command to set a SNMP view in the global configuration mode**.** The **no** form of this command is sued to delete the view.

snmp-server view *view-name* **oid-tree** {**include | exclude**}

no snmp-server view *view-name* [***oid-tree***]

Parameter description

Parameter	Description
view-name	View name
oid-tree	Specify the MIB object to associate with the view.
include	Include the sub trees of the MIB object in the view.
exclude	Exclude the sub trees of the MIB object from the view.

Default configuration

By default, a default view is set to access all MIB objects.

Command mode

Global configuration mode.

Examples

The example below sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).

```
DES-7210(config)# snmp-server view mib2 1.3.6.1 include
```

Related commands

Command	Description
show snmp view	Show the view configuration.

29.1.16 snmp-server if-index persist

Use this command to persist index on an interface**.** The **no** form of this command is sued to disable this function.

snmp-server if-index persist

no snmp-server if-index persist

Parameter description

N/A

Default configuration	Disabled
Command mode	Global configuration mode.
Examples	The example below enables the function to persist index on the interface. `DES-7210(config)# snmp-server if-index persist`

Related commands

Command	Description
show run	Show the configuration.

29.2 Showing Related Command

29.2.1 show snmp

Use this comand to show the SNMP information in the privileged mode.

show snmp [**mib | user | view | group**]

Command mode	Privileged mode.
Usage guidelines	**show snmp**: Show the SNMP information. **show snmp mib**: Show the SNMP MIBs supported in the system. **show snmp user**: Show the SNMP user information. **show snmp view**: Show the SNMP view information. **show snmp group**: Show the SNMP user group information.

Examples	The example below shows the SNMP information:
	`DES-7210# show snmp`
	`Chassis: 60FF60`
	`0 SNMP packets input`
	`0 Bad SNMP version errors`
	`0 Unknown community name`
	`0 Illegal operation for community name supplied`
	`0 Encoding errors`
	`0 Number of requested variables`
	`0 Number of altered variables`
	`0 Get-request PDUs`

```
        0 Get-next PDUs
        0 Set-request PDUs
0 SNMP packets output
        0 Too big errors (Maximum packet size 1500)
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 Response PDUs
        0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP agent: enabled
```

Related commands

Command	Description
snmp-server *chassis-id*	Specify the SNMP system sequence number.

30 RMON Configuration Commands

30.1 Configuration Related Commands

The RMON configuration commands are as follows:

- **rmon collection stats** *index* [**owner** *owner-string*]
- **rmon collection history** *index* [**owner** *owner-string*] [**buckets** *bucket-number*] [**interval** *seconds*]
- **rmon alarm** *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]
- **rmon event** *number* [**log**] [**trap** *community*] [*description-string*]
- **show rmon statistics**
- **show rmon history**
- **show rmon events**
- **show rmon alarms**

30.1.1 rmon collection stats

Use this command to monitor an Ethernet interface. The **no** form of this command remove the configuration.

rmon collection stats *index* [**owner** *owner-string*]

no rmon collection stats *index*

Default	N/A.
Command mode	Interface configuration mode.
Usage guidelines	N/A.

Examples

The example below enables monitoring the statistics of Ethernet port 1.

```
DES-7210(config)# interface fast-Ethernet 0/1
DES-7210(config-if)# rmon collection stats 1 zhansan
```

Related commands

Command	Description
rmon collection history *index* [**owner** *owner-name*] **buckets** *bucket-number* **interval** *seconds*	Add a history control entry.

30.1.2 rmon collection history

Use this command to log the history of an Ethernet interface. The **no** form of this command cancels the logging.

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

Default

N/A.

Command mode

Interface configuration mode.

Usage guidelines

The DES-7200 allows you to modify the configured history information of the Ethernet network, including **owner, buckets**, and **interval**. However, the modification does not take effect immediately until the system records history at the next time.

Examples

The example below Logs the history of Ethernet port 1.

```
DES-7210(config)# interface fast-Ethernet 0/1
DES-7210(config-if)# rmon collection history 1 zhansan buckets 10
interval 10
```

Related commands

Command	Description
rmon collection stats *index* [**owner** *owner-name*]	Add a statistical entry.

30.1.3 rmon alarm

Use this command to monitor a MIB variable. The **no** form of this command cancels the logging.

rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]

no rmon alarm *number*

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	The DES-7200 allows you to modify the configured history information of the Ethernet network, including **variable, interval, absolute/delta, owner, rising-threadhold/falling-threadhold**, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.
Examples	The example below monitors the MIB variable instance ifInNUcastPkts.6. `DES-7210(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-threshold 10 1 owner zhangsan`

Related commands

Command	Description
rmon event *number* [**log**] [**trap** *community*] **description** *string*	Add an event definition.

30.1.4 rmon event

Use this command to define an event. The **no** form of this command cancels the logging.

rmon event *number* [**log**] [**trap** *community*] [*description-string*]

no rmon alarm *number*

Default	N/A.
Command mode	Global configuration mode.

Usage guidelines	N/A.
Examples	The example below defines the event actions: log event and send trap message. `DES-7210(config)# rmon event 1 log trap rmon description "ifInNUcastPkts is too much " owner zhangsan`

Related commands	**Command**	**Description**
	rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an alarm entry.

30.2 Showing Related Commands

30.2.1 show rmon statistics

Use this command to show the statistics.

show rmon statictics

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The example below shows the statistics.
	`DES-7210# show rmon statistics`
	`Statistics: 1`
	`Data source: Gi1/1`
	`DropEvents: 0`
	`Octets: 1884085`
	`Pkts: 3096`
	`BroadcastPkts: 161`
	`MulticastPkts: 97`

```
CRCAlignErrors: 0
UndersizePkts: 0
OversizePkts: 1200
Fragments: 0
Jabbers: 0
Conflicts: 0
Pkts64Octets: 128
Pkts65to127Octets: 336
Pkts128to255Octets: 229
Pkts256to511Octets: 3
Pkts512to1023Octets: 0
Pkts1024to1518Octets: 1200
Owner: zhangsan
```

Related commands

Command	Description
rmon collection stats *index* [**owner** *owner-string*]	Add a statistical entry.

30.2.2 show rmon history

Use this command to show the history information.

show rmon history

Default N/A.

Command mode Privileged mode.

Usage guidelines N/A.

Examples

The example below shows the history information.

```
DES-7210#  show rmon history
Entry: 1
Data source: Gi1/1
Buckets requested: 65535
Buckets granted: 10
Interval: 1
Owner: zhangsan
Sample: 198
Interval start: 0d:0h:15m:0s
DropEvents: 0
Octets: 67988
Pkts: 726
```

```
BroadcastPkts: 502
MulticastPkts: 189
CRCAlignErrors: 0
UndersizePkts: 0
OversizePkts: 0
Fragments: 0
Jabbers: 0
Conflicts: 0
Utilization: 0
```

Related commands

Command	Description
rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add a history control entry.

30.2.3 show rmon alarm

Use this command to show the MIB variable information.

show rmon alarm

Default N/A.

Command mode Privileged mode.

Usage guidelines N/A.

Examples

The example below shows the MIB variable information.

```
DES-7210#  show rmon alarm
Event: 1
Description: firstevent
Event type: log-and-trap
Community: public
Last time sent: 0d:0h:0m:0s
Owner: zhangsan
Log: 1
Log time: 0d:0h:37m:47s
Log description: ipttl
Log: 2
Log time: 0d:0h:38m:56s
Log description: ipttl
```

Related commands	Command	Description
	rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an alarm entry.

30.2.4 show rmon event

Use this command to show the event information.

show rmon event

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The example below shows the event information.
	`DES-7210# show rmon event`
	`Alarm: 1`
	`Interval: 1`
	`Variable: 1.3.6.1.2.1.4.2.0`
	`Sample type: absolute`
	`Last value: 64`
	`Startup alarm: 3`
	`Rising threshold: 10`
	`Falling threshold: 22`
	`Rising event: 0`
	`Falling event: 0`
	`Owner: zhangsan`

Related commands	Command	Description
	rmon event *number* [**log**] [**trap** *community*] [*description-string*]	Add an event entry.

31 RIP Configuration Commands

31.1 Configuration Related Commands

31.1.1 address-family (RIP)

Use this command to set the RIP protocol in the address family configuration sub-mode. The **no** form of this command closes the address family sub-mode.

address-family ipv4 vrf *vrf-name*

no address-family ipv4 vrf *vrf-name*

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the VRF name associated with the sub-mode command.

Default configuration

The address family of the RIP protocol is not configured.

Command mode

Route configuration mode.

Usage Guidelines

You can use the **address-family** command to enter the address family configuration sub-mode. The prompt is **(config-router-af)#**. When you specify the VRF associated with the sub-mode for the first time, the RIP instance corresponding to the VRF will be created. In the sub-mode, you can configure the VRF RIP routing settings.

To exit the address family sub-mode and return to the route configuration mode, execute the **exit-address-family** or **exit** command.

Examples

Create a VRF with the name of vpn1 and create its RIP instance.

```
DES-7210(config)# ip vrf vpn1
DES-7210(config-vrf)# exit
DES-7210(config)# interface FastEthernet 1/0
DES-7210(config-if)# ip vrf forwarding vpn1
DES-7210(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7210(config)# router rip
DES-7210(config-router)# address-family ipv4 vrf vpn1
DES-7210(config-router)# network 192.168.1.0
DES-7210(config-router)# exit-address-family
```

Related commands

Command	Description
exit-address-family	Exit the address family configuration sub-mode.
ip vrf	Create a VRF.

Platform description

Version description

31.1.2 auto-summary (RIP)

Use this command to enable the automatic summary of RIP routes. The **no** form of this command disables the function.

auto-summary

no auto-summary

Parameter description N/A.

Default configuration Enabled.

Command mode Routing process configuration mode.

Usage The automatic RIP route summary means the subnet routes will be

guidelines

automatically summarized into the routes of the classful network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2.

The automatic RIP route summary improves the flexibility and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the routing table, reducing the size of the routing table significantly.

Advertising summarized route is more efficient than individual routes in light of the following factors:

- The summarized route is always processed preferentially in querying the RIP database.
- Any sub-route is ignored in querying the RIP database, reducing the processing time.
- Sometimes, there is a need to learn the specific sub-routes instead of the summarized route. Here it is required to disable the automatic route summary function. Only when the RIPv2 is configured, however, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.

Examples

The configuration example below disables the automatic route summary of the RIPv2.

```
DES-7210 (config)# router rip
DES-7210 (config-router)# version 2
DES-7210 (config-router)# no auto-summary
```

Related commands

Command	Description
version	Define the RIP software version: v1 or v2. Both v1 and v2 are supported by default.

Platform description

Version description

31.1.3 default-metric (RIP)

Use this command to define the default RIP metric in the route configuration mode. The **no** form of this command is used to restore it to the default value.

default-metric *metric*

no default-metric

Parameter description

Parameter	Description
metric	Default metric in the range of 1 to 16. If the metric is greater than or equal to 16, the DES-7200 regards the route unreachable.

Default configuration

The default value is 1.

Command mode

Routing process configuration mode.

Usage guidelines

This command needs to work with the command **redistribute**. When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric cannot be converted due to the incompatibility of the metric calculation mechanism of different protocols. During the conversion, therefore, it is required to redefine the metric of redistributed routes in the RIP routing domain. If there is no clear definition of metric in redistributing a routing protocol process, the RIP uses the metric defined with **default-metric**. If a clear metric is defined, this value overwrites the metric defined with **default-metric**. If this command is not configured, the default value of default-metric is 1.

Examples

In the configuration example below, the RIP routing protocol redistributes the routes learned by the OSPF routing protocol, whose initial RIP metric is set as 3.

```
DES-7210 (config)# router rip
DES-7210 (config-router)# default-metric 3
DES-7210 (config-router)# redistribute ospf 100
```

Related commands

Command	Description
redistribute	Redistribute the routes from one routing domain to another routing domain.

Platform description	

Version description	

31.1.4 default-information originate(RIP)

Use this command to generate a default route in the RIP process. The **no** form of this command deletes the generated default route.

default-information originate [**always**] [**metric** *metric-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**route-map** *map-name*]

Parameter description

Parameter	Description
always	(Optional) Enable RIP to generate the default route, no matter whether the default route exists or not.
metric *metric-value*	(Optional) The original metric value of the default route, in the range of 1-15.
route-map *map-name*	(Optional) Name of the associated route-map. Route-map is not associated by default.

Default configuration	No default route is generated by default. The metric value of the generated default value is 1.

Command mode	Routing process configuration mode.

Usage guidelines

By default, RIP will not notify the default route outside, if there is no default route in the routing table. Use the **default-information originate** routing process configuration command to notify the neighbor of the default route.

With the parameter **always** configured, no matter whether the default route exists in the RIP routing process or not, the default route will be notified to the neighbor but not shown in the local routing table. Use the **show ip rip database** command to confirm the default route generation and view the RIP routing information database.

Configure the parameter **route-map** to control the default route. For example, use the **set metric** rule to set the metric value of the default route.

The route-map **set metric** rule takes precedence over the parameter **metric** value configuration of the default route. If the parameter **metric** has not been configured, the default metric value of the default route will be adopted.

Note:

If the default route can be generated by using this command, RIP will not learn the default route notified from the neighbor.

For the default route generated by using the **ip default-network** command, the default-information originate command is still needed to add the default route to the RIP.

Examples

The configuration example below generates a default route to the RIP routing table:

```
DES-7210(config-router)# default-information originate always
```

Related commands

Command	Description
ip rip default-information	Notify the default route on an interface.
redistribute	Redistribute the routes from one routing domain to another routing domain.

Platform description

Version description

31.1.5 distance

Use this command to set the management distance of the RIP route. The **no** form of this command restores it to the default setting.

distance *distance* [*ip-address wildcard*]

no distance *distance* [*ip-address wildcard*]

Parameter description

Parameter	Description
distance	Management distance of a RIP route, an integer in the range of 1 to 255
ip-address	Prefix of the source IP address of the route
wildcard	Comparison bit of the IP address, where 0 means accurate matching while 1 means no comparison

Default

The default value is 120.

Command mode

Routing process configuration mode.

Usage guidelines

This command sets the management distance of the RIP route.

You can use this command to create several management distances with source address prefix. When the source address of the RIP route is within the range specified by the prefix, the corresponding management distance is applied; otherwise, the route uses the management distance set by the RIP.

Examples

Set the management distance of the RIP route to **160**, and specify the management distance of the route learned from 192.168.2.1 to **123**.

```
DES-7210(config)# router rip
DES-7210(config-router)# distance 160
DES-7210(config-router)# distance 123 192.168.12.1 0.0.0.0
```

31.1.6 distribute-list in (RIP)

Use this command to control route update for filtering in the routing process configuration mode. The **no** form of this command removes the configuration.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

Parameter description

Parameter	Description
access-list-number	ACL number. Only the routes on the ACL are accepted.
prefix *prefix-list-name*	Use the prefix list to filter the routes.
gateway *prefix-list-name*	Use the prefix list to filter the source of the routes.
i*nterface-type interface-number*	(Optional) Interface that the distribution list applies to

Default configuration

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

To deny some specified routes, you can process all the route update packets received by configuring the route distribute control list.

Without any interface specified, the system will process the route update packet received on all the interfaces.

Examples

In the following configuration example, the RIP controls and processes the routes received from the Fastethernet 0/0 port, only permitting the routes starting with 172.16.

```
DES-7210 (config)# router rip
DES-7210 (config-router)# network 200.168.23.0
DES-7210 (config-router)# distribute-list 10 in fastethernet 0/0
DES-7210 (config-router)# no auto-summary
DES-7210 (config-router)# access-list 10 permit 172.16.0.0
0.0.255.255
```

Related commands

Parameter	Description
access-list	Define the ACL.
prefix-list	Define the prefix of the ACL.

Platform

description	
Version description	

31.1.7 distribute-list out (RIP)

Use this command to control route update advertisement for filtering routes in the routing process configuration mode. The **no** form of this command removes this configuration.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protoco*] [*process-id* | *process-name*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol* | *process-id* | *process-name*]

Parameter description

Parameter	Description
access-list-number	ACL number. Only the routes on the ACL are permitted.
prefix *prefix-list-name*	Use the prefix list to filter the routes.
Interface	(Optional) Interface that the route update advertisement control applies to
protocol	(Optional) Routing protocol whose routes are selectively redistributed
process-id	(Optional) Set the OSPF process ID when OSPF is used.
process-name	(Optional) Set the ISIS process name when ISIS is used.

Default configuration	No route update advertisement is configured.
Command mode	Routing process configuration mode.

Usage guidelines	No optional parameters means the route update advertisement applies to all ports. Interface option means the control applies to only the specified port. Protocol option means the route update advertisement control applies to only the specific route process.

Examples	In the following configuration example, the RIP routing process only advertises the 192.168.12.0/24 route.
	`DES-7210 (config)# router rip`
	`DES-7210 (config-router)# network 200.4.4.0`
	`DES-7210 (config-router)# network 192.168.12.0`
	`DES-7210 (config-router)# distribute-list 10 out`
	`DES-7210 (config-router)# version 2`
	`DES-7210 (config-router)#access-list 10 permit 192.168.12.0 0.0.0.255`

Related commands

Parameter	Description
access-list	Define the ACL.
prefix-list	Define the prefix of the ACL.
redistribute	Configure route redistribution.

31.1.8 exit-address-family

Use this command to exit the address family configuration mode.

exit-address-family

Parameter description	N/A.
Default configuration	N/A.
Command mode	Address family configuration mode.
Usage guidelines	Use this command to exit the address family configuration mode. The abbreviation of this command is **exit** .
Examples	Following example shows how to enter or exit the address family configuration mode: `DES-7210(config-router)# address-family ipv4 vrf vpn1`

```
DES-7210(config-router-af)# exit-address-family
```

Related commands

Parameter	Description
address-family	Enter the address family configuration sub-mode

Platform description

Version description

31.1.9 ip rip authentication key-chain

Use this ocmmand to enable the RIP authentication and specify the keychain used for RIP authentication in the interface configuration mode. The **no** form of this command is used to delete the specified keychain.

ip rip authentication key-chain *name-of-keychain*

no ip rip authentication key-chain

Parameter description

Parameter	Description
name-of-keychain	Name of the keychain used for RIP authentication

Default configuration

RIP authentication is disabled by default.

Command mode

Interface configuration mode.

Usage guidelines

If the keychain is specified in the interface configuration mode but not defined with the **key chain** global configuration command, the RIP authentication will not occur.

The RIPv1 does not support authentication but the RIPv2 does.

Examples

The configuration example below enables the RIP authentication on interface serial 0 with the associated keychain is ripchain.

```
DES-7210 (config)#interface serial 0/0
DES-7210 (config-if)#ip rip authentication key-chain ripchain
```

Related commands

Command	Description
ip rip authentication mode	Define the RIP authentication mode.
ip rip receive version	Define the version of RIP packets received on the interface.
ip rip send version	Define the verion of RIP packets sent on the interface.
key chain	Define the keychain and enter into the keychain configuration mode.

Platform description

Version description

31.1.10 ip rip authentication mode

Use this command to define the RIP authentication mode in the interface configuration mode. The **no** form of this command is used to restore it to the default RIP authentication mode.

ip rip authentication mode {**text** | **md5**}

no ip rip authentication mode

Parameter description

Parameter	Description
text	Enable plaintext authentication.
md5	Enable MD5 authentication.

Default configuration

It is the plaintext authentication by default.

Command mode

Interface configuration mode.

Usage guidelines

To exchange RIP routing information directly, all devices must have the same RIP authentication mode. Otherwise, the RIP packet exchange will fail.

The RIPv1 does not support RIP authentication but the RIPv2 does.

Examples

The configuration example below configures the RIP authentication mode on the interface serial 0 as md5.

```
DES-7210 (config)#interface serial 0/0
DES-7210 (config-if)# ip rip authentication mode md5
```

Related commands

Command	Description
ip rip authentication key-chain	Enable the RIP authentication and specify the keychain used for the RIP authentication. Only the RIPv2 supports authentication.
key chain	Define the keychain and enter into the keychain configuration mode

Platform description

Version description

31.1.11 ip rip authentication text-password

Use this command to set the password string of RIP plaintext authentication. The **no** form of this command is used to remove the password string.

ip rip authentication text-password *password-string*

no ip rip authentication text-password

Parameter description

Parameter	Description
password-string	Password string of the plaintext authentication, in the length of 1-16 bytes.

Default configuration

It is the plaintext authentication by default.

Command mode

Interface configuration mode.

Usage guidelines	To enable the RIP plaintext authentication, the password string can be configured directly by using this command, or can be obtained by associating with the key chain. The latter takes the precedence over the former one. The RIPv1 does not support RIP authentication but the RIPv2 does.

Examples	The configuration example below enables the RIP plaintext authentication on the interface serial 0/0 and sets the password string as DES-7210:
	`DES-7210(config)#interface serial 0/0`
	`DES-7210(config-if)# ip rip authentication text-password dlink`

Related commands

Command	Description
ip rip authentication mode	Define the RIP authentication mode.
ip rip authentication key-chain	Enable the RIP authentication and specify the keychain used for the RIP authentication. Only the RIPv2 supports authentication.

Platform description

Version description

31.1.12 ip rip default-information

Use this command to notify a specified interface of the RIP default route. The **no** form of this command is used to cancel the notification of the default route.

ip rip default-information {**only** | **originate**} [**metric** *metric-value*]

no ip rip default-information

Parameter description

Parameter	Description
only	Notify the default route, rather than other routes.
originate	Notify the default route and other routes.
metric *metric-value*	Specify the metric value of the default route, in the range of 1-15.

Default configuration	No default route is configured by default. The default metric is 1.
Command mode	Interface configuration mode.
Usage guidelines	After configuring this command on a specified interface, a default route will be notified through this interface. If the **ip rip default-information** command in the interface configuration mode and the **default-information originate** command in the RIP process are configured at the same time, it only notifies the interface of the default route. **Note:** RIP will not learn the default route notified by the neighbor, if the **ip rip default-information** command does not configured on an interface. If the default route has been learned, it will be removed till the timer expires. The **ip rip default-information** command configuration on the interface can not be triggered and updated immediately, and will be notified on the next timed update message.

Examples	The configuration example below creates a default route which is notified on the interface ethernet0/0 only:
	`DES-7210(config)#interface ethernet 0/0`
	`DES-7210(config-if)#ip rip default-information only`

Related commands

Command	Description
default-information originate	Originate the default route in the RIP process.

Platform description	
Version description	

31.1.13 ip rip receive enable

Use this command to receive RIP packets on the interface. The **no** form of this command prohibits receiving RIP packets on the interface .

ip rip receive enable

no ip rip receive enable

Parameter description	N/A.
Default configuration	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	To prevent from receiving RIP packets on the interface, use the **no** form of this command in the interface configuration mode. To this end, you must configure this command on the interface. The **default** form of this command restores it to the default value.

Examples	Prohibit from receiving RIP packets on the Fastethernet 0/0.
	`DES-7210 (config)# interface fastethernet 0/0`
	`DES-7210 (config-if)# no ip rip receive enable`

Related commands

Parameter	Description
ip rip send enable	Enable sending RIP packets on the interface.
passive-interface	Set the interface to a passive interface.

Platform description	
Version description	

31.1.14 ip rip receive version

Use this command to define the version of RIP packets received on the interface in the interface configuration mode. The **no** form of this command is used to restore it to the default value.

ip rip receive version [**1**] [**2**]

no ip rip receive version

Parameter description

Parameter	Description
1	(Optional) Receive only RIPv1 packets.
2	(Optional) Receive only RIPv2 packets.

Default configuration

The default behavior depends on the configuration with the **version** command.

Command mode

Interface configuration mode.

Usage guidelines

This command overwrites the default configuration of the **version** command. It allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If there is no parameter when the command is configured, the receiving behavior will depend on the configuration of the version.

Examples

The configuration example below enables receiving both RIPv1 and RIPv2 packets on the fastethernet 0/0 interface.

```
DES-7210 (config)#interface fastethernet 0/0
DES-7210 (config-if)# ip rip receive version 1 2
```

Related commands

Command	Description
version	Define the default version of the RIP packets received/sent on the interface.

Platform description

Version description

31.1.15 ip rip send enable

Use this command to enable sending RIP packets on the interface. The **no** form of this command disables sending RIP packets on the interface.

ip rip send enable

no ip rip send enable

Parameter description	N/A.
Default configuration	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	To prevent from sending RIP packets on the interface, use the **no** form of this command in the interface configuration mode. To this end, you must configure this command on the interface. The **default** form of this command can restore it to the default value.

Examples	Prohibit from sending RIP packets on the Fastethernet 0/0.
	`DES-7210 (config)# interface fastethernet 0/0`
	`DES-7210 (config-if)# no ip rip send enable`

Related commands

Parameter	Description
ip rip receive enable	Enable receiving RIP packets on the interface.
passive-interface	Set the interface to a passive interface.

Platform description	
Version description	

31.1.16 ip rip send version

Use this command to define the version of the RIP packets sent on the interface in the interface configuration mode. The **no** form of this command is used to restore it to the default value.

ip rip send version [**1**] [**2**]

no ip rip send version

Parameter description

Parameter	Description
1	(Optional) Send only RIPv1 packets.
2	(Optional) Send only RIPv2 packets.

Default configuration

The default behavior depends on the configuration with the **version** command.

Command mode

Interface configuration mode.

Usage guidelines

This command overwrites the default configuration of the **version** command. It allows RIPv1 and RIPv2 packets to be sent on the interface at the same time. If there is no parameter when the command is configured, the receiving behavior will depend on the configuration of the version.

Examples

The configuration example below enables sending both RIPv1 and RIPv2 packets on the fastethernet 0/0 interface.

```
DES-7210 (config)# interface fastethernet 0/0
DES-7210 (config-if)# ip rip send version 1 2
```

Related commands

Command	Description
version	Define the default version of the RIP packets received/send on the interfaces.

Platform description

Version description

31.1.17 ip rip v2-broadcast

Use this command to send RIPv2 pakcets in broadcast form rather than in multicast form. The **no** form of this command restores it to the default setting.

ip rip v2-broadcast

no ip rip v2-broadcast

Parameter description	N/A.
Default configuration	The default depends on the configuration of the **version** command.
Command mode	Interface configuration mode.
Usage guidelines	This command overwrites the default of the **version** command. This command only affects the behavior of sending RIP packets on the interface. This command allows RIPv1 and RIPv2 packets to be sent on the interface simultaneously. Without parameters specified, which packets will be received depends on the **version** setting.

Examples	Send RIPv2 packets in the broadcast mode on the Fastethernet 0/0 interface.
	`DES-7210 (config)# interface fastethernet 0/0`
	`DES-7210 (config-if)# ip rip v2-broadcast`

Related commands

Parameter	Description
version	Define the default version of the RIP packets received and sent on the interface.

Platform description	
Version description	

31.1.18 ip split-horizon (RIP)

Use this command to enable split horizon in the interface configuration mode. The **no** form of this command disables the function.

ip split-horizon

no ip split-horizon

Parameter description	N/A.
Default configuration	Enabled.
Command mode	Interface configuration mode.
Usage guidelines	When multiple devices are connected to the IP broadcast network using a distance vector routing protocol, it is required to use the split horizon mechanism to prevent loop. The split horizon prevents the device from advertising some routing information from the interface that learns that information, which optimizes the routing information exchange between multiple devices. For non-broadcast multi-path access network (such as frame relay and X.25), however, the split horizon may cause some devices unable to learn all routing information. The split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for the split horizon issue. The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, execute the **show ip interface** command. This function makes no influence on the neighbor defined with the **neighbor** command.

Examples	The configuration example below disables the RIP split horizon function on the interface fastethernet 0/0.
	`DES-7210 (config)# interface fastethernet 0/0`
	`DES-7210 (config-if)# no ip split-horizon`

Related commands

Command	Description
neighbor (RIP)	Define a neighbor.

	validate-update-source	Enable the source address authentication of the RIP route update message.

Platform description

Version description If some command or some options are available only on a certain version, please explain it clearly here.

31.1.19 ip summary-address rip

Use this command to enable port-level convergence in the interface configuration mode. The **no** form of this command disables the convergence of the specified address or subnet.

ip summary-address rip *ip-address ip-network-mask*

no ip summary-address rip *ip-address ip-network-mask*

Parameter description

Parameter	Description
ip-address	IP addresses to be converged
ip-network-mask	Subnet mask of the specified IP address to be converged

Default configuration The RIP routes are automatically converged to the classful network edge.

Command mode Interface configuration mode.

Usage guidelines This command converges an address or subnet on a specified port. RIP routes are automatically converged to the classful network edge. The classful subnet can be configured through only port convergence.

Examples The following configuration example disables the route convergence function of the RIPv2. The port convergence is configured so that the FastEthernet 1/0 advertises the converged route 172.16.0.0/16.

```
DES-7210 (config)# interface FastEthernet 1/0
DES-7210 (config-if)# ip summary-address rip 172.16.0.0 255.255.0.0
DES-7210 (config-if)# ip address 172.16.1.1 255.255.255.0
DES-7210 (config)# router rip
```

```
DES-7210 (config-router)# network 172.16.0.0
DES-7210 (config-router)# version 2
DES-7210 (config-router)# no auto-summary
```

Related commands

Parameter	Description
auto-summary	Enable the automatic convergence of RIP routes.

Platform description

Version description

31.1.20 network (RIP)

Use this command to define the list of networks to be advertised in the RIP routing process in the routing process configuration mode. The **no** form of this command is used to delete the defined network.

network *network-number* [*wildcard*]

no network *network-number* [*wildcard*]

Parameter description

Parameter	Description
network-number	Number of the directly-connected network. This network number is a natural network number. All interfaces whose IP addresses belong to that natural network can send/receive the RIP packets.
wildcard	Define the IP address comparing bit: 0 refers to accurate matching, 1 refers to no comparing.

Command mode

Routing process configuration mode.

Usage guidelines	The *network-number* and *wildcard* parameter can be configured simultaneously to make the IP address for the interface within the address range join the RIP running. Without the *wildcard* parameter configured, DES-7200 make the interface IP address within the classful address range join the RIP running. Only when the IP address of an interface is in the network list defined for the RIP, the RIP route update messages can be received and sent on the interface.

Examples	The following example defines two network numbers associated with the RIP process.
	`DES-7210 (config)# router rip`
	`DES-7210 (config-router)# network 192.168.12.0`
	`DES-7210 (config-router)# network 172.16.0.0`

Related commands	
Platform description	
Version description	If some command or some options are available only on a certain version, please explain it clearly here.

31.1.21 neighbor (RIP)

Use this command to define a RIP neighbor in the routing process configuration mode. The **no** form of this command is used to delete the neighbor.

neighbor *ip-address*

no neighbor

Parameter description

Parameter	Description
ip-address	IP address of the neighbor.

Default configuration

N/A.

Command mode	Routing process configuration mode.
Usage guidelines	By default, the RIPv1 works with the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 works with the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, execute the **passive-interface** command in the routing process configuration mode to configure the related interfaces as passive interface and then define only some neighbor to be able to receive the routing information. This command does not affect the receiving of RIP messages. Once restart, the interface who is set to passive will not send request message.

Examples	The configuration example below defines two neighbors.
	`DES-7210 (config)# router rip`
	`DES-7210 (config-router)# network 192.168.12.0`
	`DES-7210 (config-router)# network 172.16.0.0`

Related commands	
Platform description	
Version description	

31.1.22 offset-list(RIP)

Use this command to increase the metric value of receiving or sending route. The **no** form of this command deletes the specified offset list.

offset-list *access-list-number* {**in** | **out**} *offset* [*interface-type interface-number*]

no offset-list *access-list-number* {**in** | **out**} *offset* [*interface-type interface-number*]

Parameter description

Parameter	Description
access-list-number	ACL number
in	Modify the metric of the routes received by ACL.

out	Modify the metric of the routes sent by ACL.
offset	Change of the metric value
interface-type	Interface that the ACL applies to
interface-number	Interface that the ACL applies to

Default configuration

The offset is not specified.

Command mode

Routing process configuration mode.

Usage guidelines

If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.

Examples

Increase the metric of the RIP routes by 7 in the range specified by ACL 7.

```
DES-7210 (config-router)# offset-list 7 out 7
```

Increase the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by fastEthernet 1/0.

```
DES-7210 (config-router)# offset-list 7 in 7
DES-7210 (config-router)# offset-list 8 in 7 fastEthernet 1/0
```

Related commands

Platform description

Version description

31.1.23 output-delay

Use this command to modify the delay to send the RIP update packets. The **no** form of this command removes the configuration.

output-delay *delay*

no output-delay

Parameter description

Parameter	Description
delay	Delay to send the RIP update packets in the range from 8 ms to 50 ms.

Default configuration

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

Normally, the size of a RIP update packet is 512 Kbytes including 25 routes. If the number of the update routes is larger than 25, the routes will be sent in several packets as fast as possible.

However, when a high-speed device sends a large amount of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

Examples

Set the delay to send the RIP update packets to 30 ms.

```
DES-7210(config)# router rip
DES-7210(config-router)# output-delay 30
```

Related commands

Platform description

Version description

31.1.24 passive-interface

Use this command to set an interface to a passive interface. The **no** form of this command removes this configuration.

passive-interface {**default** | *interface-type interface-num*}

no passive-interface {**default** | *interface-type interface-num*}

Parameter description

Parameter	Description
Default	Set the interface to a passive interface.
interface-type interface-num	Interface type and number

Default configuration

No ports are set to the passive mode.

Command mode

Routing process configuration mode.

Usage guidelines

The **passive-interface default** command sets all interfaces to the passive mode. You can use **no passive-interface** *intface-type interface-num* to set the specified interface to the non-passive mode.

When you enable receiving and sending RIP messages on the interface with the **ip rip send enable** and **ip rip receive enable** commands, this command sets the interface to the passive mode. Consequently, receiving RIP update messages rather than sending RIP update messages is enabled on the interface. However, the **ip rip send enable** and **ip rip receive enable** commands determine whether the messages can be sent or received.

Examples

Set all interfaces to the passive mode and then set ethernet0/0 to the non-passive mode.

```
DES-7210(config-router)# passive-interface default
DES-7210(config-router)# no passive-interface gigabitEthernet 4/1
```

Related commands

Command	Description
ip rip receive enable	Enable receiving RIP packets on the interface.
ip rip send enable	Enable sending RIP packets on the interface.

Platform description

N/A.

Version description	N/A.

31.1.25 redistribute (RIP)

Use this command to redistribute external routes in the route configuration mode. The **no** form of this command cancels the redistribution of external routes.

redistribute {**bgp**| **isis** [*process-name*] |**ospf** <*1-65535*>| **connected** | **static**} [**metric** *value*] [**route-map** *route-map-name*][**match internal** | **external** *type* | **nssa-external** *type*]

no redistribute {**bgp** | **isis** [*process-name*] | **ospf** <*1-65535*> | **connected** | **static**} [**metric** *value*] [**route-map** *route-map-name*][**match internal** | **external** *type* | **nssa-external** *type*]

Parameter description

Parameter	Description
bgp | isis | ospf | **connected** | **static**	Specify the route redistribution protocol.
metric	Set the metric of the route to be redistributed.
route-map	Set the redistribution rule.
match	Redistribute OSPF-type routes.
<*1-65535*>	Number of an OSPF instance

Default

By default:

All the routes of the sub types of the instance are redistributed when you configure redistributing OSPF.

The routes of Level-2 sub-types of the instance are redistributed when you configure ISIS redistribution.

All the routes of the protocol are redistributed for other routing protocols.

The metric of the redistributed routes is 1 by default.

The route-map is not associated.

Command mode	Routing process configuration mode.

Usage guidelines	This command redistributes external routes. It is not necessary to convert the metric of one routing protocol into that of another routing protocol for route distribution, since different routing protocols use different metric measurement methods. The RIP protocol calculates metric on hop, the OSPF on bandwidth. So their metrics are not comparable. However, a symbolic metric must be set for route redistribution. Otherwise, route redistribution will fail. When you configure ISIS routes redistribution without the **level** parameter, only level-2 routes are redistributed by default. If the redistribution configuration is initialize with **level** parameter, then all routes with **level** configured are redistributed. When you configure redistributing OSPF routes without the **match** parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The **no** form of this command restores the setting to the default value. **Note:** The redistribute command cannot redistribute the default route of other protocol to the RIP process. To this end, execute the **default-information originate** command.
Examples	Redistribute static routes. `DES-7210(config-router)# redistribute static`

Related commands

Command	Description
default-metric *metric*	Set the default metric of the route to be redistributed.

31.1.26 router rip

Use this command to create the RIP routing process and enter into the routing process configuration mode. The **no** form of this command is used to delete the RIP routing process.

router rip

no router rip

Parameter description	N/A.

Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	One RIP routing process must be defined with one network number. If a dynamic routing protocol is running on asynchronous lines, execute **async default routing** on the asynchronous interface.
Examples	The configuration example below describes how to create the RIP routing process and enter into the routing process configuration mode. `DES-7210 (config)# router rip`

Related commands

Command	Description
network (RIP)	Define the network number of the RIP process.

31.1.27 timers basic

Use this command to adjust the RIP clock in the routing process configuration mode. The **no** form of this command is used to restore it to the default.

timers basic *update invalid flush*

no timers basic

Parameter description

Parameter	Description
update	Route update time, in seconds. The *update* keyword defines the period at which the device sends route update messages. Once an update message is received, the "Invalid" and "Flush" clocks reset. By default, a route update message is sent every 30 seconds.
invalid	Route invalid period, in seconds, starting from the last valid update message. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update message is received within the route invalid period, the related route becomes invalid and

	enters into the "invalid" state. If a update message is received within the period, the clock resets. By default the Invalid period is 180s.
flush	Route flushing period, in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush period is 120 s.

Default configuration

By default, the update time is 30s, invalid time is 180s and flushing time is 120 s.

Command mode

Routing process configuration mode.

Usage guidelines

Adjusting the above clocks may speed up the routing protocol convergence and fault recovery. The devices connected with the same network must have the same RIP clock settings. The adjustment of RIP clocks is not recommended unless otherwise necessary.

To check the current RIP clock parameters, execute the **show ip rip** command.

Examples

The configuration example below enables the RIP update message to be sent every 10 seconds. If no update message is received within 30s, the related routes become invalid and enter into the invalid status. When another 90s elapses, they will be cleared.

```
DES-7210 (config)# router rip
DES-7210 (config-router)# timers basic 10 30 90
```

Note that the small settings of clocks on low-speed links may cause some risks, because numerous update messages may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2Mbps to reduce the convergence time of routes.

31.1.28 validate-update-source

Use this command to validate the source address of the received RIP route update message in the routing process configuration mode. The **no** form of the command disables the source address validation.

validate-update-source

no validate-update-source

Default configuration	Enabled.
Command mode	Routing process configuration mode.
Usage guidelines	It is possible to validate the source address of the RIP route update message. The validation aims to ensure the RIP routing process receives only the route updates from the same IP subnet neighbor. Disabling split-horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the **validate-update-source** command in the routing process configuration mode. In addition, for the **ip unnumbered** interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the routing process configuration command **validate-update-source**.

Examples	The configuration example below disables the message source address validation.
	`DES-7210 (config)# router rip`
	`DES-7210 (config-router)# no validate-update-source`

Related commands

Command	Description
ip split-horizon	Enable split horizon.
ip unnumbered	Define the IP unnumbered interface
neighbor (RIP)	Define a neighbor.

Platform description	
Version description	

31.1.29 version (RIP)

Use this command to define the RIP version in the routing process configuration mode. The **no** form of this command is used to restore it to the default.

version {**1** | **2**}

no version

Parameter description

Parameter	Description
1	Define the RIP version 1.
2	Define the RIP version 2.

Default configuration

By default, the route update messages of the RIPv1 and RIPv2 are received, but those of the RIPv1 is send only.

Command mode

Routing process configuration mode.

Usage guidelines

This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the **ip rip receive version** and **ip rip send version** commands.

Examples

The configuration example below configures the RIP version 2.

```
DES-7210 (config)# router rip
DES-7210 (config-router)# version 2
```

Related commands

Command	Description
ip rip receive version:	Define the version of RIP packets received on the interface.
ip rip send version	Define the version of RIP packets sent on the interface.
show ip rip	Show RIP information.

Platform description

Version description

31.2 Showing Related Command

31.2.1 show ip rip

Use this command to show the RIP information.

show ip rip [**vrf** *vrf-name*]

Parameter description

Parameter	Description
vrf *vrf-name*	Specify the vrf and display the basic information of the corresponding RIP instance.

Default configuration

N/A.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines

It is used to show the three timers, routing distribution, routing re-distribution status, interface RIP version, RIP interface and network range, metric, distance and so on of the RIP routing protocol process quickly. If vrf is specified, display the name of VRF and VRF-id.

Examples

In the configuration example below, the basic information of the RIP routing protocol is displayed, such as the refresh time, management distance, etc.

```
DES-7210#show ip rip
Routing Protocol is "rip"
  Sending updates every 10 seconds, next due in 4 seconds
  Invalid after 20 seconds, flushed after 10 seconds
  Outgoing update filter list for all interface is: not set
  Incoming update filter list for all interface is: not set
  Default redistribution metric is 2
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface            Send  Recv   Key-chain
    FastEthernet 1/1      2     2     ripkey1
    FastEthernet 1/0      2     2     ripkey2
  Routing for Networks:
    192.168.26.0
    192.168.64.0
  Distance: (default is 50)
```

Follwoing example specifies vrf and displays the corresponding basic information of RIP instance:

```
DES-7210(config-router)# sh ip rip vrf 1
VRF 1  VRF-id:1
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 4 seconds
  Invalid after 180 seconds, flushed after 120 seconds
  Outgoing update filter list for all interface is: not set
  Incoming update filter list for all interface is: not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 1, receive any version
  Routing for Networks:
  Distance: (default is 120)
```

31.2.2 show ip rip database

Use this command to show the summary address entries in the RIP routing database.

show ip rip database [**vrf** *vrf-name*] [*network-number* {*network-mask*}]

Parameter description

Parameter	Description
vrf *vrf-name*	(Optional) Show the RIP routing information of specified VRF.
network-number	(Optional) Network number
network-mask	Subnet maskIt if the network number is specified.

Default configuration

N/A.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines

Only when the related sub-routes are converged, the converged address entries appear in the RIP routing database. When the last sub-route information in the converged address entries becomes invalid, the converged address information will be deleted from the database.

Examples

In the configuration example below, all converged address entries in the RIP routing database are displayed.

```
DES-7210 # show ip rip database
192.168.1.0/24        auto-summary
```

```
192.168.1.0/30        directly connected, Loopback 3
192.168.1.8/30        directly connected, FastEthernet 0/0
192.168.121.0/24      auto-summary
192.168.121.0/24      redistributed
[1] via 192.168.2.22, FastEthernet 0/1
```

In the configuration example below, the converged address entries related with 192.168.121.0/24 in the RIP routing database are displayed.

```
DES-7210 # show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24       redistributed
[1] via 192.168.2.22,  FastEthernet 0/1
```

Related commands

Command	Description
show ip protocol	Show the information of the currently-running routing protocol process.

31.2.3 show ip rip external

Use this command to show the information of the external routes redistributed by the RIP protocol.

show ip rip external [**bgp** | **connected** | **isis [***process-name***] |ospf <***1-65535***>|** static] [**vrf** *vrf-name*]

Parameter description

Parameter	Description
**bgp	connected	isis	ospf	static**	Show the external route redistributed by the specified routing protocol (optional).
vrf vrf-name	Show the RIP external route of the specified VRF (optional)..
<*1-65535*>	Number of the OSPF instace

Default configuration

N/A.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Examples

The following is an example showing the direct routes redistributed by the RIP process.

```
DES-7210# show ip rip external connected
```

```
Protocol connected route:
[connected] 1.0.0.0/8 metric=0
nhop=0.0.0.0, if=2
[connected] 3.0.0.0/8 metric=0
nhop=0.0.0.0, if=16391
[connected] 4.4.0.0/16 metric=0
nhop=0.0.0.0, if=16388
[connected] 5.0.0.0/8 metric=0
nhop=0.0.0.0, if=16386
[connected] 192.168.195.0/24 metric=0
nhop=0.0.0.0, if=1
```

Related commands

Command	Description
show ip rip	Show the information of the currently running routing protocol process.

31.2.4 show ip rip interface

Use this command to show the RIP interface information.

show ip rip interface [**vrf** *vrf-name*]

Parameter description

Parameter	Description
vrf *vrf-name*	Show the RIP interface of specified VRF (optional).

Default configuration

N/A.

Command mode

Privileged mode, global configuration mode, routing process configuration mode.

Usage guidelines

Examples

The following is an example showing the RIP interface information.

```
DES-7210# show ip rip interface
FastEthernet 1/1 is down, line protocol is down
  RIP is not enabled on this interface
FastEthernet 1/0 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv2 packets only
    Send RIPv2 packets only
```

```
    Passive interface: Disabled
    Split horizon: Enabled
    V2 Broadcast: Disabled
    Multicast register: Registed
    Interface Summary Rip:
      Not Configured
    Authentication mode: Text
    Authentication key-chain: ripk1
    Authentication text-password:dlink
    Default-information: only, metric 5
    IP interface address:
      192.168.64.100/24
```

If the BFD has been configured for RIP, the result of this command is shown as follows:

```
DES-7210# show ip rip interface
Vlan 1 is up, line protocol is up
    Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 packets only
    Receive RIP packet: Enabled
    Send RIP supernet routes: Enabled
    Passive interface: Disabled
    Split horizon: Enabled
    V2 Broadcast: Disabled
    Multicast registe: Registed
    Interface Summary Rip:
      Not Configured
     IP interface address: 2.2.2.111/24
```

Related commands

Command	Description
show ip rip	Show the information of the currently running routing protocol process.

32 OSPFv2 Configuration Commands

32.1 Configuration Related Commands

32.1.1 area

Use this command to configure the specified OSPF area. The **no** form of this command removes the specified OSPF area.

area *area-id*

no area *area-id*

Parameter description

Parameter	Description
area-id	Number of the area where authentication is enabled, a decimal integer or an IP address

Default configuration

No OSPF area is configured by default.

Command mode

Routing process configuration mode.

Usage guidelines

Use the no form of this command to remove the specified OSPF area and its configuration, including the removal of the area-based configuration commands of **area authentication**、**area default-cost**、**area filter-list**、**area nssa**, ect.

Users can not remove the OSPF configuration under the following conditions:

It fails to remove all configurations for the backbone area with the virtual link configured. Now the virtual link configuration must be removed before removing the backbone area.

The corresponding **network area** command exists in any area. Now all commands added to the area must be removed before removing this OSPF area.

Examples

The following example removes the configuration of the OSPF area 2:

```
DES-7210(config)# router ospf 2
DES-7210(config-router)# no area 2
```

Related commands

Command	Description
network area	Define the OSPF on the interface and the OSPF area.

32.1.2 area authentication

Use this command to enable authentication in the OSPF area in the routing process configuration mode. The **no** form of this command disables authentication in the OSPF area.

area *area-id* **authentication** [*message-digest*]

no area *area-id* **authentication** [*message-digest*]

Parameter description

Parameter	Description
area-id	Number of the area where authentication is enabled, a decimal integer or an IP address
message-digest	(optional) MD5 (message digest 5) authentication mode

Default configuration

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

The DES-7200 software supports three authentication types: 1) 0, no authentication; when this command is not executed to enable OSPF authentication, the authentication type in the OSPF packet is 0; 2) 1, plaintext authentication mode; when this command is configured, the *message-digest* option is not used; 3) 2, MD5 authentication mode; when this command is configured, the *message-digest* option is used.

All devices in the same OSPF area must have the same authentication type. If the authentication is enabled, authentication password must be configured on the interfaces connecting neighbors. The **ip ospf authentication-key** command in the interface configuration mode can be used to configure the plaintext authentication password. The **ip ospf message-digest-key** command in the interface configuration mode can be used to configure the MD5 authentication password.

Examples

In the following configuration example, MD5 authentication is used in the OSPF routing process area 0 (backbone area), with authentication password "backbone".

```
DES-7210(config)#interface FastEthernet 0/0
DES-7210(config-if)# ip address 192.168.12.1
255.255.255.0
DES-7210(config-if)# ip ospf message-digest-key 1 md5 backbone
Configure OSPF routing protocol.
DES-7210(config)# router ospf 1
DES-7210(config-router)# network 192.168.12.0
0.0.0.255 area 0
DES-7210(config-router)# area 0 authentication
message-digest
```

Related commands

Command	Description
ip ospf *authentication-key*	Define the OSPF plaintext authentication password.
ip ospf *message-digest-key*	Define the OSPF MD5 authentication password.
area virtual-link	Define a virtual link.

32.1.3 area default-cost

Use this command to define the cost of the default aggregate route that will be advertised to the stub area or NSSA area (OSPF metric) in the routing process configuration mode. The **no** form of this command is used to restore it to the default value.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter description

Parameter	Description
area-id	Number of the stub area or NSSA area
cost	Cost of the default aggregate route that will be

		advertised to the stub area or NSSA area

Default	The default value is 1.
Command mode	Routing process configuration mode.
Usage guidelines	This command can be configured only on the area border device (ABR) and the ABR must be connected with a stub area or a NSSA area. The so-called ABR means that the device must be connected to at least one area in addition to connecting the backbone area. There are three commands to configure an OSPF area as a stub or NSSA area : **area stub**, **area nssa** and **area default-cost**. All the devices connecting to the stub area must be configured with the **area stub** command, those connecting to the NSSA area must be configured with the **area nssa** command. However, the **area default-cost** command can be executed only on the ABR.

Examples	Set the cost of the default aggregate route to 50.
	`DES-7210(config)# router ospf 1`
	`DES-7210(config-router)# network 172.16.0.0 0.0.255.255 area 0`
	`DES-7210(config-router)#network 192.168.12.0 0.0.0.255 area 1`
	`DES-7210(config-router)# area 1 stub`
	`DES-7210(config-router)# area 1 default-cost 50`

Related commands

Command	Description
area stub	Set an OSPF area as a stub area.
area nssa	Set an OSPF area as a NSSA area.

32.1.4 area filter-list

Use this command to configure the inter-area route filtering on the ABR.

area *area-id* **filter-list** [**access** *acl-name*| **prefix** *prefix-name*] [**in** | **out**]

no area *area-id* **filter-list** [**access** *acl-name* | **prefix** *prefix-name*] [**in** | **out**]

Parameter description

Parameter	Description
area-id	Area ID
acl-name	ACL name
prefix-name	Prefix-list name

	access | **prefix**	Associated prefix list or ACL
	in | **out**	Apply the ACL rule to the routes incoming/outgoing the area.

Default	N/A.
Command mode	Routing process configuration mode.
Usage guidelines	This command can be configured only on an Area Board Device (ABR) to configure inter area route filtering

Examples	Set area 1 to learn only the inter-area routes of 172.22.0.0/8.
	`DES-7210 # configure terminal`
	`DES-7210(config)# access-list 1 permit 172.22.0.0/8`
	`DES-7210(config)# router ospf 100`
	`DES-7210(config-router)# area 1 filter-list access 1 in`

32.1.5 area nssa

Use this command to set an OSPF area as an NSSA area in the routing process configuration mode. The **no** form of this command is used to delete the NSSA area or the configuration of the NSSA area.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** <*0-16777214*> | **metric-type** <*1-2*>]] [**no-summary**]

no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**]

Parameter description

Parameter	Description
area-id	NSSA area number
no-redistribution	(Optional) Import the routing information to common areas other than the NSSA area through the **redistribute** command when the device is an ABR of the NSSA area.
default-information originate	(Optional) Generate and import the default type 7 LSA to the NSSA area. This option takes effect only on the NSSA ABR or ASBR.
no-summary	(Optional) Prevent the ABR of the NSSA area from sending types 3 and 4 LSAs into the NSSA area.

Default	No NSSA area is defined by default.
Command mode	Routing process configuration mode.
Usage guidelines	The parameter **default-information-originate** is used to generate the default Type-7 LSA. This option is slightly different on the NSSA ABR and ASBR. On the NSSA ABR, the default Type-7 LSA will be generated, no matter whether there are default routes in the routing table. On the ASBR (which is not an ABR at the same time), the default Type-7 LSA is generated only when the default route exists in the routing table. The parameter **no-redistribution** prevents the OSPF from advertising the external routes imported with the **redistribute** command to the NSSA area on the ASBR. This option is generally used when the NSSA device is both an ASBR and an ABR. To further reduce the number of LSAs sent to the NSSA area, you can configure the **no-summary** parameter on the ABR to prevent it from advertising summary LSAs (Type-3 LSA) to the NSSA area. In addition, the **area default-cost** command is used on the ABR of the NSSA area to configure the cost of the default route sent to the NSSA area. By default, the cost of the default route sent to the NSSA area is 1.

Examples	Sets area 1 as the stub area on the devices in that area.
	`DES-7210(config)#router ospf 1`
	`DES-7210(config-router)#network 172.16.0.0 0.0.255.255 area 0`
	`DES-7210 (config-router)#network 192.168.12.0 0.0.0.255 area 1`
	`DES-7210(config-router)# area 1 nssa`

Related commands

Command	Description
area default-cost	Define the cost (OSPF metric) of the default aggregate route advertised to the NSSA area.

32.1.6 area range

Use this command to configure the route aggregation between OSPF areas in the routing process configuration mode. The **no** form of this command is used to delete the configured route aggregation. The **no** form with the **cost** parameter can restore the default metric of the aggregated route, but not remove route aggregation.

area *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area-id* **range** *ip-address net-mask* [**cost** *cost*]

Parameter description

Parameter	Description
area-id	ID of the area the aggreate route is injected into, a decimal integer or an IP address.
ip address	Network segment whose routes are to be aggregated
advertise | not-advertise	Whether to advertise the aggreagate range, advertise by default.
cost *cost*	Set the metric of the aggregated route.

Default

No aggregate route is configured between areas by default.

The default metric of aggregated route depends on whether the device is compatible with RFC1583 or not. If so, the default metric is the smallest cost of the aggregated route. If not, the default metric is the largest cost of the aggregated route.

Command mode

Routing process configuration mode.

Usage guidelines

This command can be executed only on the ABR to aggregate multiple routes of an area to a route and then advertise it to other areas. Route combination occurs only on the border of an area. The devices within an area see the specific routing information, but the devices outside the area only one aggregate route. The advertise and not-advertise options can be used to set whether to advertise the aggregate route, which functions as the filtering and masking purpose. The aggregate route is advertised by default.

You can define route aggregate in multiple areas to simplify the routes in the whole OSPF routing area. This improves the network forwarding performance, especially in large networks.

Examples

Aggregate the routes of area 1 into a route 172.16.16.0/20.

```
DES-7210(config)#router ospf 1
DES-7210(config-router)#network 172.16.0.0 0.0.15.255 area 0
DES-7210((config-router)#network 172.16.17.0 0.0.15.255 area 1
DES-7210(config-router)#area 1 range 172.16.16.0 255.255.240.0
```

32.1.7 area stub

Use this command to set an OSPF area as a stub area or full stub area in the routing process configuration mode. The **no** form of this command is used to delete the configuration of stub area or full stub area.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter description

Parameter	Description
area-id	STUB area number
no-summary	(Optional) Prevent the ABR from advertising network summary link to the stub area. Here the stub area is called the full stub area. Only the ABR needs this parameter.

Default

No stub area is defined by default.

Command mode

Routing process configuration mode.

Usage guidelines

All devices in the OSPF stub area must be configured with the **area stub** command. The ABR only sends three types of link state advertisement (LSA) to the stub area: 1) type 1, device LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. From the aspect of the routing table, the devices in the stub area can learn only the routes inside the OSPF routing domain, including the internal default routes generated by the ABR. The devices in the stub area cannot learn the routes outside the OSPF routing domain.

To configure a full stub area, execute **area stub** command with the no-summary keyword on the ABR. The devices in the full stub area can learn only the routes in the local area and the internal default routes generated by the ABR.

There are two commands to configure an OSPF area as a stub area: **area stub** and **area default-cost**. All devices connected to the stub area must be configured with the **area stub** command, but the **area default-cost** command can be executed only on the ABR. The **area default-cost** command defines the initial cost (i.e. metric) of the internal default route.

Examples

Set area 1 as the stub area on the devices in that area.

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# network 172.16.0.0 0.0.255.255 area 0
DES-7210 (config-router)# network 192.168.12.0  0.0.0.255 area 1
DES-7210(config-router)# area 1 stub
```

Related commands

Command	Description
area default-cost	Define the cost (OSPF metric value) of the default aggregate route advertised to the stub area.

32.1.8 area virtual-link

To define the OSPF virtual link, execute the **area virtual-link** command in the routing process configuration mode. The **no** form of this command is used to delete the virtual link.

area *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** |**null**]] [**dead-interval** *seconds*] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [[**authentication-key** *key*] | [**message-digest-key** *key-id* **md5** *key*]]

no area *area-id* **virtual-link** *router-id*

Parameter description

Parameter	Description
area-id	OSPF transition area number, a decimal integer or an IP address.
router-id	Identifier of the router neighboring to the virtual link. The router identifier can be viewed through the **show ip ospf** command.
dead-interval *seconds*	(Optional) Define the time to declare neighbor loss (in second), 40 seconds by default. This parameter must be consistent with the neighbor.
hello-interval *seconds*	(Optional)Define the interval at which the HELLO message is sent by the OSPF to the virtual link (in seconds), 10 s by default This parameter must be consistent with the neighbor.
retransmit-interval *seconds*	(Optional) OSPF LSA resend time (in second), 5 seconds by default. The setting of the time must consider the trip time of messages on the link.

transmit-delay *seconds*	(Optional) OSPF LSA send delay (in second), 1 second by default. This value adds the LSA live period. When the LSA live period reaches a certain value, the LSA will be refreshed.
authentication-key *key*	(Optional) Define the OSPF plaintext authentication key. The plaintext authentication key between neighbors must be the same. The **service password-encryption** command enables the key to be displayed in encrypted manner.
message-digest-key *key-id* **md5** *key*	(Optional) Define the OSPF MD5 authentication key identifier and key. The MD5 authentication key identifier and key between neighbors must be the same. The **service password-encryption** command enables the key to be displayed in encrypted manner.
authentication	Set the authentication type to plaintext.
message-digest	Set the authentication type to MD5.
null	Set the authentication type to no authentication

Default

dead-interval: 40s
hello-interval: 10s
retransmit-interval: 5s
transmit-delay: 1s
authentication: no authentication
N/A values for the other parameters

Command mode

Routing process configuration mode

Usage guidelines

In the OSPF routing domain, all areas must be connected with the backbone area. If an area disconnects from the backbone area, it requires to configure virtual links to connect the backbone area. Otherwise, the network communication will become abnormal. The virtual link requires the connection between two ABRs. The area that belongs to both ABRs is called the transition area. A stub Area or NSSA area cannot act as a transition area. Virtual links can also be used to connect other non-backbone areas.

The router-id is the identifier of OSPF neighbor router. If you are unsure of the router-id, check it with the **show ip ospf neighbor** command. You may configure the Loopback address as the router identifier.

The **area virtual-link** command defines only the authentication key for virtual link. To enable the OSPF message authentication for the areas connected with the virtual link, execute the **area authentication** command in the routing process configuration mode.

Examples

Set area 1 as the transition area to establish virtual link with neighbor 2.2.2.2.

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# network 172.16.0.0 0.0.15.255 area 0
DES-7210(config-router)# network 172.16.17.0 0.0.15.255 area 1
DES-7210(config-router)# area 1 virtual-link 192.1.1.1
```

Set area 1 as the transition area to establish virtual link with neighbor 1.1.1.1. This virtual link connects area 10 and backbone area, and works with the OSPF message authentication of MD5.

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# network 172.16.17.0 0.0.15.255 area 1
DES-7210(config-router)# network 172.16.252.0 0.0.0.255 area 10
DES-7210(config-router)# area 0 authentication message-digest
DES-7210(config-router)# area 1 virtual-link 1.1.1.1
message-digest-key 1 md5 hello
```

Related commands

Command	Description
area authentication	Enable the OSPF area message authentication and define the authentication mode.
show ip ospf	Show the OSPF process information, including the router identifier.

32.1.9 auto-cost

Use this command to enable the automatic cost calculating function and set the reference bandwidth. According to the reference bandwidth, you can configure the cost of the specified interface automatically.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter description

Parameter	Description
ref-bw	Reference bandwidth, in the range of 1 to 4294967 Mbps.

Default	100Mbps by default.
Command mode	Routing process configuration mode.
Usage guidelines	This command sets the reference bandwidth for automatically generating interface cost. No parameter with it enables the automatic cost function with a default for the reference bandwidth. A parameter with it enables the automatic cost calculation function with a specified reference bandwidth. Note that the "default auto-cost" and the "no auto-cost" are different: the former restores it to the default and enables the automatic cost function while the latter disables the automatic cost calculation function. If you use **ip ospf cost** command to set the cost of the interface, the cost will replace the auto-cost.

Examples	The configuration example below configures the reference bandwidth as 10M.
	`DES-7210(config)# router ospf 1`
	`DES-7210(config-router)# network 172.16.10.0 0.0.0.255 area 0`
	`DES-7210(config-router)# auto-cost reference-bandwidth 10`

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information

32.1.10 clear ip ospf process

Use this command to clear and restart the OSPF instance.

clear ip ospf (*process-id*) **process**

Parameter description

Parameter	Description
process-id	OSPF instance ID When no process ID is specified, the command clears and restarts all the running OSPF instances.

Default	Use the rule recommended in RFC 1583 by default.

Command mode	Privileged mode.
Usage guidelines	
Examples	The command below clears and restarts OSPF instance 1. `DES-7210#clear ip ospf 1 process`

32.1.11 compatible rfc1583

When the routing table includes several routes to the same destination out of the AS, you must determine the best route. Use this command to decide which rule will be taken in RFC 1583 or RFC 2328.

commpatible rfc1583

no commpatible rfc1583

Default	Use the rule recommended in RFC 1583 by default.
Command mode	Routing process configuration mode.

Examples	The configuration example below determines the best route with the rfc 2328 rule.
	`DES-7210(config)# router ospf 1`
	`DES-7210(config-router)# no commpatible rfc1583`

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information

32.1.12 default-information originate (OSPF)

Use this command to generate a default route to the OSPF routing domain in the routing process mode. The **no** form of this command disables the default route.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric** *metric*]

[**metric-type** *type*] [**route-map** *map-name*]

Parameter description

Parameter	Description
Always	(Optional) Generate the default route unconditionally, no matter whether the default route exists locally or not.
metric *metric*	(Optional) Initial metric value of the default route, 1 by default
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different devices; type 2, the same metric seens on different devices. External route of type 1 is more trustworthy than that of type 2. By default, it is type 2.
route-map *map-name*	Associated route map name, no associated route map by default

Default

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

When the **redistribute** or **default-information** command is executed, the OSPF-enabled device automatically turns into the autonomous system border device (ASBR). But the ASBR cannot generate default route automatically or advertise it to all the devices in the OSPF routing domain. The ASBR generates default routes by default. It is required to configure with the **default-information originate** routing process configuration command.

If the **always** parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route exists or not. However, the local device does not show the default route. To make sure whether the default route is generated, execute **show ip ospf database** to observe the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. The execution of the **show ip route** command on the OSPF neighbor will display the default route.

The metric of the external default route can be defined only with the **default-information originate** command instead of the **default-metric** command.

There are two types of OSPF external routes: type 1 external routes

have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, type 1 takes precedence over type 2. As a result, the **show ip route** command shows only the type 1 route.

The devices in the stub area cannot generate external default routes.

Examples

The configuration example below generates an external default route to the OSPF routing domain, with type as 1 and metric as 50.

```
DES-7210(config)#router ospf 1
DES-7210(config-router)#network 172.16.24.0 0.0.0.255 area 0
DES-7210(config-router)#default-information originate
always metric 50 metric-type 1
```

Related commands

Command	Description
show ip ospf database	Show OSPF link state database.
show ip route	Show the IP routing table.

32.1.13 default-metric

Use this command to configure the default metric of OSPF redistributed route in the routing process mode. The **no** format of this command is used to restore it to the default.

default-metric *metric*

N/A-metric

Parameter description

Parameter	Description
metric	Metric of the OSPF redistributed route

Default

The default value is 20.

Command mode

Routing process configuration mode.

Usage guidelines

The **default-metric** command must work with the **redistribute** command in the routing process configuration mode to modify the initial metric of all redistributed routes.

The configuration result of the **default-metric** command does not take effect for the external routes to the OSPF routing domain via

	default-information originate.

Examples	The configuration example below configures the initial metric of the OSPF redistributed route as 50.
	`Switch(config)# router rip`
	`DES-7210(config-router)# network 192.168.12.0`
	`Switch(config-router)# version 2`
	`DES-7210(config-router)# exit`
	`DES-7210(config)# router ospf`
	`DES-7210(config-router)# network 172.16.10.0 0.0.0.255 area 0`
	`Switch(config-router)# default-metric 50`
	`DES-7210(config-router)# redistribute rip subnets`

Related commands

Command	Description
redistribute	Redistribute the routes of other routing processes.
show ip ospf	Show the OSPF global configuration information.

32.1.14 distance ospf

Use this command to set the management distance of different types of routes.

distance ospf {**intra-area** <*1-255*> | **inter-area** <*1-255*> | **external** <*1-255*>}

no distance ospf

Parameter description

Parameter	Description
intra-area <*1-255*>	Set the management distance of the inner-area route, 110 default.
inter-area <*1-255*>	Set the management distance of the inter-area route, 110 default.
external <*1-255*>	Set the management distance of the external route, 110 default.

Default	The default value is 110.
Command mode	Routing process configuration mode.
Usage guidelines	This command is used to specify different management distances for different types of OSPF routes.

Examples

In the configuration below, the OSPF external route management distance is set as 160.

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# distance ospf external 160
```

32.1.15 distribute-list in

Use this command to configure LSA filtering.

distribute-list {*listname* | **gateway** *plist-name* | **prefix** *plist-name*} **in** [**interface-type** *num*]

no distribute-list {*listname* | **gateway** *plist-name* | **prefix** *plist-name*}| **in** [**interface-type** *num*]

Parameter description

Parameter	Description
listname	Use the acl filtering rule.
gateway *plist-name*	Use the gateway filtering rule.
prefix *plist-name*	Use the prefix-list filtering rule.
interface-type *num*	Configure the LSA route filtering on the interface.

Default

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the SPF calculation to generate the corresponding routes. It does not affect the link status database or the routing table of the neighbors. It only affects the routing entries calculated by the local OSPF. This function is generally used for the ABR or ASBR, where it can control the routes leaving the area.

Examples

```
DES-7210(config)# access-list 3 permit 172.16.0.0 0.0.127.255
DES-7210(config)# router ospf 25
DES-7210(config-router)# redistribute rip metric 100
DES-7210(config-router)# distribute-list 3 in ethernet 1/0
DES-7210(config-router)# distribute-list 3 in ethernet 1/1
```

32.1.16 distribute-list out

Use this command to configure filtering re-distribution routes, similar to the **redistribute** command.

distribute-list {l*istname* | **gateway** *plist-name* | **prefix** *plist-name*} **out** [**bgp** | **connected** | **isis** *area-tag* |**ospf** *process-id* | **rip** | **static**]

no distribute-list {l*istname* | **gateway** *plist-name* | **prefix** *plist-name* } **out** [**bgp** | **connected** | **isis** *area-tag* |**ospf** *process-id*| **rip** | **static**]

Parameter description

Parameter	Description
listname	Use the acl filtering rule.
Gateway *plist-name*	Use the gateway filtering rule.
prefix *plist-name*	Use the prefix-list filtering rule.
[**bgp** | **connected** | **isis** *area-tag* | **ospf** *process-id* |**rip** | **static**]	Source of the routes to be filtered.

Default

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

The **distribute-list ou**t and the **redistribute route-map** commands are similar. Both filter the routes that other protocols redistribute to the OSPF. However, it does not perform route redistribution by itself. Instead, it works with the **redistribute** command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration.

Examples

The example below filters the redistributed static routes.

```
DES-7210(config)# router ospf 1
DES-7210(config)# redistribute static subnets
DES-7210(config-router)# distribute-list 22 out static
DES-7210(config-router)# distribute-list prefix jjj out
static
% There already has filter configured. Please
re-configure.
```

32.1.17 enable mib-binding

Use this command to bind the MIB with the specified OSPFv2 process. Use the **no** form of this command to restore it to the default value.

enable mib-binding

no enable mib-binding

Parameter description	N/A.
Default	By default, the MIB is binded with the OSPFv2 process in the smallest number.
Command mode	Routing process configuration mode.
Usage guidelines	OSPFv2 MIB has no OSPFv2 process information, so the user operates a sole OSPFv2 process by SNMP. By default, OSPFv2 MIB is binded with the OSPFv2 process in the smallest number. The user operations take effect for this process. If the user wants to operate the specified OSPF process by SNMP, use this command to bind the MIB with this process.

Examples	The example below operates the OSPFv2 process 100 by SNMP:
	`DES-7210(config)# router ospf 100`
	`DES-7210(config-router)# enable mib-binding`

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information.
enable traps	Configure the OSPF TRAP function.

32.1.18 enable traps

OSPFv2 process supports 16 kinds of TRAP messages, which are classified into 4 categories. Use this command to enable to send the specified TRAP messages. Use the **no** form of this command to disable to send the specified TRAP messages.

enable traps [**error** [**ifauthfailure | ifconfigerror | ifrxbadpacket | virtifauthfailure | virtifconfigerror | virtifrxbadpacket**] | **lsa** [**lsdbapproachoverflow | lsdboverflow | maxagelsa | originatelsa**] | **retransmit** [**iftxretransmit | virtiftxretransmit**] | **state-change** [**ifstatechange | nbrstatechange | virtifstatechange | virtnbrstatechange**]]

no enable traps [**error** [**ifauthfailure | ifconfigerror | ifrxbadpacket | virtifauthfailure | virtifconfigerror | virtifrxbadpacket**] | **lsa** [**lsdbapproachoverflow | lsdboverflow | maxagelsa | originatelsa**] | **retransmit** [**iftxretransmit | virtiftxretransmit**] | **state-change** [**ifstatechange | nbrstatechange | virtifstatechange | virtnbrstatechange**]]

Parameter description

Parameter	Description
error	Set all traps switches related to the **error**. Use this parameter to set the following specified **error traps** switches:

ifauthfailure	Interface authentication error
ifconfigerror	Interface parameter configuration error
ifrxbadpacket	Error messages are received on the interface
virtifauthfailure	Authentication erroe on the virtual interface
virtifconfigerror	Parameter configuration error on the virtual interface
virtifrxbadpacket	Error messages are received on the virtual interface

<table>
<tr><td>isa</td><td>Set all traps switches related to the isa. Use this parameter to set the following specified isa traps switches:
<table>
<tr><td>lsdbapproachoverflow</td><td>External LSA amount has reached the 90% of the upper limit.</td></tr>
<tr><td>lsdboverflow</td><td>External LSA amount has reached the upper limit.</td></tr>
<tr><td>maxagelsa</td><td>LSA reaches the aging time</td></tr>
<tr><td>originatelsa</td><td>Generates new LSA</td></tr>
</table></td></tr>
<tr><td>retransmit</td><td>Set all traps switches related to the retransmit. Use this parameter to set the following specified retransmit traps switches:
<table>
<tr><td>iftxretransmit</td><td>Packet retransmission occurs on the interface</td></tr>
<tr><td>virtiftxretransmit</td><td>Packet retransmission occurs on the virtual interface</td></tr>
</table></td></tr>
<tr><td>state-change</td><td>Set all traps switches related to the state-change. Use this parameter to set the following specified state-change switches:
<table>
<tr><td>ifstatechange</td><td>Interface state change</td></tr>
<tr><td>nbrstatechange</td><td>Neighbor state change</td></tr>
<tr><td>virtifstatechange</td><td>State change on the virtual interface</td></tr>
<tr><td>virtnbrstatechange</td><td>State change on the virtual neighbor</td></tr>
</table></td></tr>
</table>

Default	By default, all TRAP switches are disabled.

Command mode	Routing process configuration mode.
Usage guidelines	The **snmp-server enable traps ospf** command must be configured before configuring this command, for this command is limited by the **snmp-server** command. This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.

Examples	The example below enables all TRAP switches of the OSPFv2 process 100:
	`DES-7210(config)# router ospf 100`
	`DES-7210(config-router)# enable traps`

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information.
enable mib-binding	Bind the OSPFv2 process with MIB.

32.1.19 ip ospf authentication

Use this command to configure the authentication type. Use the **no** form of the command to restore it to the default type.

ip ospf authentication [**message-digest** | **null**]

no ip ospf authentication

Parameter description

Parameter	Description
message-digest	Enable MD5 authentication on the interface.
null	Enable no authentication.

Default	No authentication mode is configured on the interface by default. Here, the authentication type of the local area applies on the interface.
Command mode	Interface configuration mode.

Usage guidelines

Plaintext authentication applies when no option is used with the command. Note that the **no** form of this command restores the setting to the default value. Whether authentication is used actually depends on the authentication mode configured for the area of the interface. If the authentication mode is configured as **null**, this enables no authentication. When both the interface and its area are configured with authentication, the one for the interface takes priority.

Examples

The configuration example below configures MD5 authentication for the OSPF on interface FastEthernet 0/0.

```
DES-7210 (config)#interface fastethernet 0/0
DES-7210(config-if)# ip address 172.16.10.0
255.255.255.0
DES-7210(config-if)# ip ospf authentication
message-digest
```

Related commands

Command	Description
area authentication	Enable authentication and define the authentication mode in the OSPF area.
ip ospf authentication-key	Configure the plaintext authentication key
ip ospf message-digest-key	Configure the MD5 authentication key

32.1.20 ip ospf authentication-key

Use this comand to configure the OSPF plaintext authentication key in the interface configuration mode. The **no** form of this command is used to delete the plaintext authentication key.

ip ospf authentication-key *key*

no ip ospf authentication-key

Parameter description

Parameter	Description
Key	Key of at most 8 characters or numerals.

Default

N/A.

Command mode

Interface configuration mode.

Usage guidelines

The **ip ospf authentication-key** command configures the key that will be inserted in all OSPF message headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key.

To enable the OSPF area authentication, execute the **area authentication** command in the routing process configuration mode.

The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in the interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes priority.

Examples

The configuration example below configures the OSPF authentication key "ospfauth" for the interface FastEthernet 0/0.

```
DES-7210 (config)#interface fastethernet 0/0
DES-7210(config-if)# ip address 172.16.10.0
255.255.255.0
DES-7210(config-if)# ip ospf authentication-key ospfauth
```

Related commands

Command	Description
area authentication	Enable authentication in the OSPF area and define the authentication mode
Ip ospf authentication	Enable authentication on the interface and define the authentication mode

32.1.21 ip ospf cost

Use this command to configure the cost (OSPF metric) of the OSPF interface for sending a packet in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf cost *cost*

no ip ospf cost

Parameter description

Parameter	Description
Cost	OSPF interface cost

Default	The default cost of the interface is 108/Bandwidth.
Command mode	Interface configuration mode.
Usage guidelines	By default, the OSPF interface cost is 108/Bandwidth, where Bandwidth is the interface bandwidth configured with the **bandwidth** command in the interface configuration mode. The default costs of different types of lines are as follows: ■ 64K serial line: 1562 ■ E1 line: 48 ■ 10M Ethernet: 10 ■ 100M Ethernet: 1 The OSPF cost configured with the **ip ospf cost** command will overwrite the default configuration.

Examples	The configuration example below configures the OSPF cost of the interface serial 1/0 as 100.
	`DES-7210(config)# interface serial 1/0`
	`DES-7210(config-if)# ip ospf cost 100`

Related commands

Command	Description
bandwidth	Specify the interface bandwidth. This setting does not affect the data transmission rate.
show ip ospf	Show the OSPF global configuration information

32.1.22 ip ospf database-filter all out

Use this command to configure not to advertise LSA messages on the interface, that is, the LSA update messages are not sent on the interface. The **no** form of the command restores it to the default.

ip ospf database-filter all out

no ip ospf database-filter

Default	This function is disabled by default. Any LSA update message can be sent on the interface.

Command mode	Interface configuration mode.
Usage guidelines	To disable sending LSA update messages on the interface, enable this function on the interface.

Examples	The configuration example below prevents the LSA update messages from being sent on the interface Gi 1/1.
	`DES-7210(config)# interface Gi 1/1`
	`DES-7210(config-if)# ip address 172.16.10.1 255.255.255.0`
	`DES-7210(config-if)# ip ospf database-filter all out`

32.1.23 ip ospf dead-interval

Use this command to configure the interval to judge the death of interface neighbor in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameter description

Parameter	Description
Seconds	Interval to judge the neighbor death (in seconds)

Default	By default it is 4 times the interval configured with the **ip ospf hello-interval** command.
Command mode	Interface configuration mode.
Usage guidelines	The OSPF death time is included in the Hello message. If the OSPF does not receive the Hello message from its neighbor within the death interval, it declares the neighbor's death and deletes its entry in the neighbor list. By default the death interval is 4 times the interval of the Hello message. The modification of the Hello interval will automatically change the death interval. This command can be used to manually change the interval to judge the death of OSPF neighbor. Note that: ■ The death interval cannot be less than the interval of Hello messages.

	■ The death intervals of all devices in the same network segment must be the same.

Examples	The configuration example below configures the interval of judging the death of the OSPF neighbor on the interface Gi 1/1 as 30s.
	`DES-7210(config)# interface GI 1/1`
	`DES-7210(config-if)# ip address 172.16.10.1 255.255.255.0`
	`DES-7210(config-if)# ip ospf dead-interval 30`

Related commands

Command	Description
ip ospf hello-interval	Specify the interval at which the OSPF sends Hello messages

32.1.24 ip ospf disable all

Use this command to specify the interface not to generate the OSPF messages.

ip ospf disable all

no ip ospf disable all

Default	
Command mode	Interface configuration mode.
Usage guidelines	The interface with this command configured will ignore whether the network area matches or not. After this command is configured, even if the interface belongs to the network, it will not generate OSPF datagram any more. So, it does not receive or send any OSPF message or participate in the OSPF calculation.

Examples	`DES-7210(config)# interface serial 1/0`
	`DES-7210(config-if)# ip address 172.16.10.1 255.255.255.0`
	`DES-7210(config-if)# ip ospf disable all`

32.1.25 ip ospf hello-interval

Use this command to configure the interval to send Hello messages in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter description

Parameter	Description
Seconds	Interval to send Hello messages (in seconds)

Default

- 10s for Ethernet
- 10s for PPP or HDLC encapsulated interfaces
- 10s for frame relay PTP interfaces
- 30s for non-frame relay PTP sub-interface and X.25 interfaces

Command mode

Interface configuration mode.

Usage guidelines

The interval of sending the Hello messages is included in the Hello message. A shorter interval means OSPF detects the topological change at a faster pace, which will aggravate network traffic. The Hello message intervals for all the devices in the same network segment must be the same. To further manually modify the interval to judge neighbor death, ensure the Hello message interval cannot be greater than the neighbor death interval.

Examples

The configuration example below configures the interval of sending the Hello message on the interface Gi 1/1 as 15.

```
DES-7210(config)# interface Gi 1/1
DES-7210(config-if)# ip address 172.16.10.1 255.255.255.0
DES-7210(config-if)# ip ospf hello-interval 15
```

Related commands

Command	Description
ip ospf dead-interval	Set the interval of judging the death of the OSPF neighbor.

32.1.26 ip ospf message-digest-key

Use this command to configure the MD5 authentication key in the interface configuration mode. The **no** form of this command is used to delete the MD5 authentication key.

ip ospf message-digest-key *key-id* **md5** *key*

no ip ospf message-digest-key

Parameter description

Parameter	Description
Key	Key of up to 16 characters or numerals

key-id	Key identifier in the range of 1 to 255

Default

N/A.

Command mode

Interface configuration mode.

Usage guidelines

The **ip ospf message-digest-key** command configures the key that will be inserted in all OSPF message headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key. For neighboring devices, the same key identifier must correspond to the same key.

To enable authentication in the OSPF area, execute the **area authentication** command in the routing process configuration mode. The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in the interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes priority.

The DES-7200 software supports smooth modification of MD5 authentication keys, which shall be added before deleted. When an MD5 authentication key of the device is added, the device will regard other devices have not had new keys and thus send multiple OSPF messages by using different keys, till it confirms the neighbors have been configured with new keys. When all devices have been configured with new keys, it is possible to delete the old key.

Examples

The configuration example below adds a new OSPF authentication key "hello5" with key ID 5 for the FastEthernet 0/0.

```
DES-7210(config)# interface fastEthernet 0/0
DES-7210(config-if)# ip address 172.16.24.2 255.255.255.0
DES-7210(config-if)# ip ospf authentication message-digest
DES-7210(config-if)# ip ospf message-digest-key 10 md5 hello10
DES-7210(config-if)# ip ospf message-digest-key 5 md5 hello5
```

When all neighbors are added with new keys, the old keys shall be deleted for all devices.

```
DES-7210(config)# interface Serial1/0
```

```
DES-7210(config-if)# no ip ospf message-digest-key 10 md5 hello10
```

Related commands

Command	Description
area authentication	Enable authentication in the OSPF area and define the authentication mode.
ip ospf authentication	Enable authentication on the interface and define the authentication mode.

32.1.27 ip ospf mtu-ignore

Use this command to disable the MTU check when an interface receives the database **description** message. The **no** form of this command is used to restore it to the default.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Default Enabled.

Command mode Interface configuration mode.

Usage guidelines After receiving the database description message, the device will check whether the MTU of neighbor interface is the same as its own MTU. If the received database description message indicates an MTU greater than the interface's MTU, the neighbor relationship cannot be established. This can be fixed by disabling the MTU check.

Examples The configuration example below disables the MTU check function on the interface serial 1/0.

```
DES-7210(config)# interface serial 1/0
DES-7210(config-if)# ip ospf mtu-ignore
```

32.1.28 ip ospf network

Use this command to configure the OSPF network type in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf network {**broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point**}

no ip ospf network {**broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point**}

Parameter description

Parameter	Description
broadcast	Set the OSPF network type as the broadcast type.
non-broadcast	Set the OSPF network type as the non-broadcast multi-path access type, i.e. NBMA network.
point-to-multipoint [**non-broadcast**]	Set the OSPF network type as the point-to-multipoint type. By default it is the point-to-multipoint broadcast type. The option non-broadcast means point-to-multipoint non-broadcast type.
point-to-point	Set the OSPF network type as the point-to-point type.

Default

- PTP network type: PPP, SLIP, frame relay PTP sub-interface, X.25 PTP sub-interface encapsulation
- NBMA network type: frame relay (except for PTP sub-interface), X.25 encapsulation (except for PTP sub-interface)
- Broadcast network type: Ethernet encapsulation
- By default, the network type is the point-to-multipoint network type.

Command mode

Interface configuration mode.

Usage guidelines

Networks are divided into three types according to the transmission feature of media:

- Broadcast network (Ethernet, token ring and FDDI)
- Non-broadcast network (frame relay and X.25)
- PTP network (HDLC, PPP and SLIP)

The non-broadcast network is further divided into two sub-types by the OSPF operation mode:

- Non-broadcast multi-path access (NBMA) type. NBMA requires all interconnected devices can directly communicate to each other, and only full mesh type connection can meet this requirement. There is no problem in case of the SVC (such as X.25) connections, but it is difficult in case of networking with PVC (such as frame relay). The OSPF on the NBMA network operates similarly to that on the broadcast network, where the

Designated Device shall be elected to advertise the link state of the NBMA network.

- The second is the point-to-multipoint network type. If the network topology is not a mesh type non-broadcast network, the OSPF requires the network type to be configured as the point-to-multipoint network type. In the point-to-multipoint network type, the OSPF regards all inter-device connections as PTP links and do not participate in the election of the designated device. The point-to-multipoint network type is further divided into broadcast type and non-broadcast type. For the non-broadcast type, it is required to manually configure the static neighbor.

Whatever the default network type of the interface, you must set it to the broadcast network type. For example, the non-broadcast multi-path access network (frame relay and X.25) can be configured as broadcast network, so that the configuration of neighbors can be omitted during the OSPF routing process configuration. The **X.25 map** and **frame-relay map** commands may enable the X.25 and frame relay networks with broadcasting capability, so that the OSPF can regard such networks as X.25 and frame relay as broadcast network.

The interface of the point-to-multipoint network can be configured with one or more neighbors. When the OSPF is configured as the point-to-multipoint network type, multiple host routes may be generated. In contrast to the broadcast network type, the point-to-multipoint network type features the following benefits:

- Easy configuration without configuration of neighbors or election of designated device
- Small cost, without needing the fully meshed topology

For the dial-up network, frame relay and X.25 network, to manually configure the IP address mapping table, the keyword "broadcast" must be specified to support broadcast.

Examples

The configuration example below configures the frame relay interface network as the broadcast type, which is applicable for the full mesh type frame relay connections.

```
DES-7210(config)# interface Serial1/0
DES-7210(config-if)# ip address 172.16.24.4
255.255.255.0
DES-7210(config-if)# encapsulation frame-relay
DES-7210(config-if)# ip ospf network broadcast
```

The configuration example below configures the frame relay interface

network as the point-to-multipoint type, which is applicable for the non-full-mesh type frame relay connections.

```
DES-7210(config)# interface Serial1/0
DES-7210(config-if)# ip address 172.16.24.4
255.255.255.0
DES-7210(config-if)# encapsulation frame-relay
DES-7210(config-if)# ip ospf network point-to-multipoint
```

The configuration example below configures the frame relay interface network as the broadcast type, with DR/RDR specified, which is applicable for the full or partial mesh type frame relay connections. The configuration below needs to be done on all branch node devices and non-designated devices (limited to become DR/BDR).

```
DES-7210(config)# interface Serial1/0
DES-7210(config-if)# ip address 172.16.24.4
255.255.255.0
DES-7210(config-if)# encapsulation frame-relay
DES-7210(config-if)# ip ospf network broadcast
DES-7210(config-if)# ip ospf priority 0
```

Related commands

Command	Description
dialer map ip	Define the map between IP address and dialing number.
frame-relay map	Define the map between IP address and frame DLCI.
neighbor (OSPF)	Define the IP address of neighbor applicable for NBMA network type and point-to-multipoint non-broadcast type only.
X25 map	Define the map between IP address and X.25 network address.

32.1.29 ip ospf priority

Use this command to configure the priority in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf priority *priority*

no ip ospf priority

Parameter description

Parameter	Description
Priority	Set the priority of the interface.

Default The default priority is 1.

Command mode	Interface configuration mode.
Usage guidelines	The interface priority is included in the Hello message. When DR/BDR (designated device/backup designated device) election occurs in the OSPF broadcast type network, the device with higher priority will become the DR or BDR. If the devices have the same priority, the one with higher ID will become the DR or BDR. The device with priority 0 cannot become DR or BDR. This command is valid for only OSPF broadcast and non-broadcast network types. Note: If the DR and BDR exist in the network, the modification of the interface priority will not take effect immediately. The new priority will not be used until the next DR and BDR election occurs.

Examples	The configuration example below configures the priority of the interface fastethernet 0/0 as 0.
	`Switch(config)#interface fastethernet 0/0`
	`DES-7210(config-if)# ip ospf priority 0`

Related commands

Command	Description
ip ospf network	Configure the network type of the interface.

32.1.30 ip ospf retransmit-interval

Use this command to define the interval to send the link state update message on the interface in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf retransmit-interval *seconds*

ip ospf retransmit-interval

Parameter description

Parameter	Description
Seconds	Interval to send the link state update message. This interval must be greater than the trip delay of packets between two neighbors. The default is 5 seconds.

Default	The default is 5 seconds.
Command	Interface configuration mode.

mode	
Usage guidelines	When the device sends an LSU message completely, the LSU message stays in the send buffer queue. If no confirmation from the neighbor is obtained in the interval defined with the **ip ospf retransmit-interval** command, the LSA will be sent once again. In serial lines or virtual links, the resend interval shall be slightly larger. The LSU message resend interval of virtual link is defined through the **area virtual-link** command followed with the keyword **retransmit-interval**.

Examples	The configuration example below configures the LSU message resend interval on the interface serial 1/0 as 10 seconds.
	`DES-7210(config)# interface serial 1/0`
	`DES-7210(config-if)# ip ospf retransmit-interval 10`

Related commands

Command	Description
area virtual-link	Define an OSPF virtual link.

32.1.31 ip ospf transmit-delay

Use this command to define the LSU message transmission delay in the interface configuration mode. The **no** form of this command is used to restore it to the default.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter description

Parameter	Description
Seconds	LSU message transmission delay (in seconds). The default is 1 second.

Default	The default is 1 second.
Command mode	Interface configuration mode.
Usage guidelines	Before the LSU message is transmitted, the Age field in all the LSAs of the message will be increased by the value defined in the interface configuration command **ip ospf transmit delay**. The configuration of

this parameter shall consider the send and line transmission delay of the interface. For low-rate lines, the transmission delay of the interface shall be slightly larger. The LSU message transmission delay of virtual link is defined through the **area virtual-link** command followed with the keyword retransmit-interval.

The DES-7200 software will resend or request resending the LSA with Age up to 3600. If no refresh is obtained in time, the aged LSA will be cleared from the link state database.

Examples

The configuration example below configures the transmission delay of serial1/ 0 as 5.

```
DES-7210(config)interface serial 1/0
DES-7210(config-if)#ip ospf transmit delay 10
```

Related commands

Command	Description
area virtual-link	Define an OSPF virtual link.

32.1.32 log-adj-changes

Use this command to enable the logging of the neighbor state changes. The **no** or **default** form of the command is used to disable it.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Parameter description

Parameter	Description
Seconds	LSU message transmission delay (in seconds). The default is 1 second.

Parameter description

Parameter	Description
detail	Record the detail of changes.

Default

Enabled. Without the **detail** parameter, the system records the logs that the neighbor enters the full state or leaves the full state.

Command mode

Routing process configuration mode.

Examples

The configuration example below logs the neighbor status change.

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# log-adj-changes
```

Related commands

Command	Description
show ip ospf	Show the OSPF global configuration information.

32.1.33 max-concurrent-dd

Use this command to specify the maximum number of DD messages that can be processed at the same time.

max-concurrent-dd *<1-65535>*

Parameter description

Parameter	Description
<1-65535>	Maximum number of DD messages

Default The default value is 5.

Command mode Interface configuration mode.

Usage guidelines When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD messages that each OSPF instance can have at the same time.

Examples In the configuration example below, the maximum number of DD messages is set as 4.

```
DES-7210(config)# router ospf 10
DES-7210(config-router)# max-concurrent-dd 4
```

32.1.34 neighbor

Use this command to define the OSPF neighbor in the routing process configuration mode. The **no** form of this command is sued to delete the specified neighbor.

neighbor *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost]*

no neighbor *ip-address*

Parameter description

Parameter	Description
ip address	IP address of the neighbor

poll-interval *seconds*	(Optional) Specify the interval of polling neighbors (in seconds), 120 s by default. Only the non-broadcast (NBMA) network type supports this option.
priority *priority*	(Optional) Configure the priority of non-broadcast network neighbors, 0 by default. Only the non-broadcast (NBMA) network type supports this option.
Cost *cost*	(Optional) Configure the cost to each neighbor in point-to-multipoint network, not defined by default, where the cost configured on the interface will be used. Only the point-to-multipoint [non-broadcast] network type supports this option.

Default

N/A.

Command mode

Routing process configuration mode.

Usage guidelines

The DES-7200 software must explicitly configure the neighbor information for every non-broadcast network neighbor. The IP address of a neighbor must be the master IP address of that neighbor interface.

In the NBMA network, if the neighbor device becomes inactive, in other words, the Hello message is not received within the device death interval, the OSPF will send more Hello messages to the neighbor. The interval at which the Hello messages are sent is called the polling interval. When the OSPF starts to work for the first time, it sends Hello messages only to the neighbor whose priority is not 0, so that the neighbor whose priority is set as 0 will not participate in the DR/BDR election. When the DR/BDR is generated, the DR/BDR sends the Hello messages to all neighbors to establish the neighbor relationship.

Since the point-to-multipoint non-broadcast network has no broadcast capability, neighbors cannot be found dynamically. So, it is required to use this command to manually configure neighbor. In addition, it is possible to configure the cost to each neighbor through the "cost" option for the point-to-multipoint network type.

Examples

The configuration example below declares an OSPF non-broadcast

network neighbor, with IP address 172.16.24.2, priority 1 and polling interval 150s.

```
DES-7210(config)# router ospf 20
DES-7210(config-router)# network 172.16.24.0 0.0.0.255 area 0
DES-7210(config-router)# neighbor 172.16.24.2 priority 1
poll-interval 150
```

Related commands

Command	Description
ip ospf priority	Set the interface priority.
ip ospf network	Set the network type

32.1.35 network area

Use this command to define which interfaces run OSPF and the OSPF areas they belong to in the routing process configuration mode. The **no** form of this command is used to delete the OSPF area definition of the interface.

network *ip-address wildcard* **area** *area-id*

no network *ip-address wildcard* **area** *area-id*

Parameter description

Parameter	Description
ip addres	IP address of the interface
wildcard	Define the comparison bits in the IP address, 0 for exact match and 1 for no comparison
area-id	OSPF area identifier. An OSPF area is always associated with an address range. For easy of management, a subnet can be used as the OSPF area identifier.

Default

There is no OSPF area configured by default.

Command mode

Routing process configuration mode.

Usage guidelines

The parameters *ip-address* and *wildcard* allow associating multiple interfaces with one OSPF area. To run OSPF on an interface, it is required to include the primary IP address and secondary IP address of the interface in the IP address range defined by **network area**. Only secondary IP address is not enough to enable OSPF on the interface.

If the IP address of the interface matches the IP address ranges

	defined by the **network** command in multiple OSPF processes, you can determine the OSPF process that the interface takes part in by the means of best match.

Examples	The configuration example below defines three areas: 0, 1 and 172.16.16.0. Define the interfaces whose IP addresses fall into the 192.168.12.0/24 range to area 1, define the interfaces whose IP addresses fall into the 172.16.16.0/20 range to area 2, and define the remaining interface to area 0.
	`DES-7210(config)# router ospf 20`
	`DES-7210(config-router)# network 172.16.16.0 0.0.15.255 area 172.16.16.0`
	`DES-7210(config-router)# network 192.168.12.0 0.0.0.255 area 1`
	`DES-7210(config-router)# network 0.0.0.0 255.255.255.255 area 0`

Related commands

Command	Description
router ospf	Create OSPF routing process

32.1.36 overflow database

Use this command to configure the maximum number of LSAs supported by the current OSPF instance.

overflow database <*0-4294967294*> **hard** | **soft**

no overflow database

Parameter description

Parameter	Description
<*1-4294967294*>	Maximum number of LSAs
hard	**soft**	hard: Shut down the OSPF instance when the number of LSAs exceeds that number. soft: Issue an alarm when the number of LSAs exceeds that number.

Command mode	Routing process configuration mode.
Usage guidelines	To shut down the OSPF instance when the number of LSAs exceeds that number, use the "hard" parameter; otherwise, use the "soft" parameter.

Examples

In the configuration below, when there are more than 10 LSAs, OSPF instance 10 will be shut down.

```
DES-7210# config terminal
DES-7210(config)# router ospf 10
DES-7210(config-router)# overflow database 10 hard
```

32.1.37 overflow database external

Use this command to configure the maximum number of external LSAs and the waiting time from overflow status to normal status.

overflow database external *max-dbsize wait-time*

no overflow database external

Parameter description

Parameter	Description
max-dbsize	Maximum number of external LSAs (the value shall be the same for all routing devices in the same AS)
wait-time	Waiting time of the routing device from the overflow status to normal status.

Default

By default the *max-dbsize* is -1 and the *wait-time* is 0 second.

Command mode

Global configuration mode.

Examples

In the configuration below, the maximum number of external LSAs is configured as 10, and it turns to the overflow status upon timeout, and the time interval attempting to restore from the overflow status to the normal status is 3 seconds.

```
DES-7210# config terminal
DES-7210(config)# router ospf 10
DES-7210(config-router)# overflow database external 10 3
```

32.1.38 overflow memory-lack

Use this command to allow the OSPF to enter the OVERFLOW state when the memory lacks. Use the **no** form of this command to disabe this function.

overflow memory-lack

no overflow memory-lack

Parameter description

Parameter	Description
no	Disable the function of entering the OVERFLOW state when the memory lacks.

Default

By default, OSPF is allowed to enter the OVERFLOW state when the memory lacks..

Command mode

Routing process configuration mode.

Usage guidelines

The action of OSPF entering the OVERFLOW state is to discard the newly-learned external route and prevent the memory from being increased effectively.

It is possible that enabling this function causes the route loop in the whole network. To reduce that occurance possibility, OSPF will generate a default route directing to the NULL port and this default route will exist in the OVERFLOW state.

Use the **clear ip ospf process** command to reset the OSPF and remove the OSPF OVERFLOW state.

Use the **no** form of this command to disallow the OSPF to enter the OVERFLOW state when the memory lacks, which may result in the constantly consume of the memory resources. If the memory is exhausted to some degree, the OSPF instance will stop and all learned routes will be removed.

Examples

The configuration example below disallows the OSPF to enter the OVERFLOW state when the memory lacks.

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# no overflow memory-lack
```

Related commands

Command	Description
clear ip ospf process	Reset the OSPF instances.
show ip protocols ospf	Show the OSPF information.

32.1.39 passive-interface

Use this command to configure the specified network interface or all interface as the passive interfaces. The **no** format of this command is used to restore it to the default.

passive-interface [**default** | **type** *number*]

no passive-interface [**default** | **type** *number*]

Parameter description

Parameter	Description
type *number*	Set the Interfaces of this type as passive interface
default	Set all the interfaces as passive interfaces.

Default

By default, no interface is configured as passive interface. All interfaces are allowed to receive/send OSPF messages.

Command mode

Routing process configuration mode.

Usage guidelines

To prevent other devices in the network from dynamically learning the routing information of the device, specify the specified network interface of this device as passive interface.

Examples

The configuration example below configures serial 1/0 as passive interface.

```
DES-7210(config)# router ospf 30
DES-7210(config-router)# passive-interface serial 1/0
```

Related commands

Command	Description
show ip ospf interface	Show the configuration information of the interface.

32.1.40 redistribute

Use this command to redistribute the external routing information.

redistribute {**bgp** | **ospf** *process-id* | **rip** | **connected** | **static**}[**metric** *value* | **match** {**internal** | **external** | **external 1** | **external 2** | **nssa-external** | **nssa-external 1** | **nssa-external 2**}**metric-type** {*1*|*2*} | **route-map** *map-tag* | **tag** <*0-4294967295*> | **subnets**]

no redistribute {**bgp** | **ospf** *process-id* | **rip** | **connected** | **static**}[**metric** *value* | **match** {**internal** | **external** | **external 1** | **external 2** | **nssa-external** | **nssa-external 1** | **nssa-external 2**}**metric-type** {*1*|*2*} | **route-map** *map-tag* | **tag** <*0-4294967295*> | **subnets**]

Parameter description

Parameter	Description
bgp | **ospf** *process-id*| **rip** | **connected** | **static**	Redistribute the routes of the specified routing protocol.
metric	Set the metric of OSPF extern2 LSA.
match	Redistribute the specific OSPF routes. By default, all the OSPF routes are redistributed.
metric-type	Set the external routing type as E-1 or E-2.
route-map	Redistribution filter rule.
tag	Set the tag value of the routes redistributed to the OSPF.
subnets	Redistribute the routes of non standard networks.

Default

N/A

Command mode

Route configuration mode.

Usage guidelines

After the command is configured, the routing device will turn to ASBR, the related routing information is imported into the OSPF domain and broadcasted to other OSPF routing device through type-5 LSAs.

For redistribution, the default metric of BGP routes is 1; the default metric of the LSAs generated by other types of routes is 20.

When you configure redistributing OSPF routes without the **match** parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The **no** form of this command restores the setting to the default value.

When you filter routes for redistribution by following the **route-map** rule, the **match** rule of the **route-map** rule is specific for the original redistribution parameters. It is only when the redistributed OSPF routes follow the **match** rule that the **route-map** rule works.

Examples

The following command redistributes static routes to the OSPF domain.

```
DES-7210(config-router)# redistribute static subnets
DES-7210(config)# router ospf 1
DES-7210(config-router)# redistribute ospf 2 subnets
DES-7210(config-router)# redistribute ospf 2 match external 1 internal
```

The following is the results of the **show run** command.

```
router ospf 1
redistribute ospf 2 match external 1 internal subnets
```

32.1.41 router ospf

Use this command to create the OSPF routing process in the global configuration mode. The **no** form of this command is used to delete the defined OSPF routing process.

router ospf *process-id* [**vrf** *vrf-name*]

no router ospf [*process-id*]

Parameter description

Parameter	Description
process-id	OSPF process ID
vrf-name	VRF name

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

On the basis of the original implementation, the R10.1 adds the routing process ID to multi-instance OSPF. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols without mutual interference.

Examples

The following example creates the OSPF routing process 10 within the specified vrf: *vpn_1*

```
DES-7210(config)# router ospf 10 vrf: vpn_1
```

Related commands

Command	Description
show ip protocols	Show the routing protocol informatin.

	show ip ospf	Show the OSPF information.

32.1.42 router-id

Use this command to set the router ID. Use the **no** form of this command to delete the setting or restore it to the default.

router-id *router-id*

no router-id

Parameter description

Parameter	Description
router-id	Router ID in IP address form

Default configuration

By default, the OSPF routing process will select the maximal interface IP address as the router ID.

Command mode

Routeing process configuration mode.

Usage guidelines

You can configure any IP address as the router ID. However, the router ID should be unique. Note that once the router ID changes, the OSPF protocol will do a large number of works. It is not recommended to change the router ID. The device can be changed only when no LSA is generated. To configure the OSPF protocol, you should execute this command to specify the ID of a device. Certainly, you can also specify it by the loopback. At this time, you should configure the router ID before configuring the OSPF protocol.

Examples

The following example modifies the router ID to 0.0.0.36

```
DES-7210(config)# router ospf 20
DES-7210(config-router)# router-id 0.0.0.36
```

Related commands

Command	Description
show ip protocols	Show the routing protocol information.

32.1.43 summary-address

Use this command to configure the converge route out of the OSPF routing domain in the routing process configuration mode. The **no** form of this command is used to delete the converged route.

summary-address *ip-address net-mask* [**not-advertise | tag** <*0-4294967295*> |]

no summary-address

Parameter description

Parameter	Description
ip address	IP address of the converged route
net-mask	Network mask of the converged route
not-advertise	Do not advertise the converged route.

Default

No converged route is configured by default.

Command mode

Routing process configuration mode.

Usage guidelines

When routes are redistributed by another routing process into the OSPF routing process, every route is advertised to the OSPF-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous border device can advertise only one converged route, reducing the scale of routing table greatly.

Unlike the **area rang** command, the former involves the convergence of routes between OSPF areas, while the latter involves the convergence of external routes of the OSPF routing domain.

For the NSSA area, the **summary-address** command is valid only on the ABR of the NSSA now, and causes the convergence for only redistributed routes.

Examples

The configuration command below generates an external converged route 100.100.0.0/16.

```
DES-7210(config)# router ospf 20
DES-7210(config-router)# summary-address 100.100.0.0 255.255.0.0
DES-7210(config-router)# redistribute static subnets
DES-7210(config-router)# network 200.2.2.0 0.0.0.255 area 1
```

```
DES-7210(config-router)# network 172.16.24.0 0.0.0.255 area 0
DES-7210(config-router)# area 1 nssa
```

Related commands

Command	Description
area-range	Configure route convergence on the OSPF area border device.

32.1.44 timers lsa-group-pacing

Use this command to configure the LSA grouping and then refresh the whole groups as well as the update interval for aged link state. The **no** form of the command restores it to the default.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing

Parameter description

Parameter	Description
seconds	This parameter is used for LSA pacing, checksum calculation, and aging interval. The range is 0 to 600s and 10 to1800s.

Default 240 seconds.

Command mode Routing process configuration mode.

Usage guidelines

The updated information in the pacing switch (LSA), checksum calculation, and aging interval are for more efficient switch use. The default is 4 minutes. This parameter needs not to be adjusted often. The optimum group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better. To configure OSPF LSA pacing, follow these steps in the privileged mode:

Examples

The configuration example below configures the pacing time as 120s.

```
DES-7210(config)# device ospf 20
DES-7210 (config-router)# timers lsa-group-pacing 120
```

Related commands

Command	Description
show ip ospf	Show the OSPF information.

32.1.45 timers spf

Use this command to configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations in the routing process configuration mode. The **no** form of this command restores it to the default.

timers spf *spf-delay spf-holdtime*

timers spf

Parameter description

Parameter	Description
spf-delay	Define the SPF calculation waiting period, in seconds. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Define the interval between two SPF calculations, in seconds. When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start.

Default

spf-delay: 5 s; spf-holdtime: 10 s.

Command mode

Routing process configuration mode.

Usage guidelines

Shorter values *of spf-delay* and *spf-holdtime* mean OSPF adapts to the topology change faster, and the network convergence period is shorter, but this will occupy more CPU of the device.

Examples

The configuration example below configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively.

```
DES-7210(config)# device ospf 20
DES-7210(config-router)# timers spf 3 9
```

Related commands

Command	Description
show ip ospf	Show the configuration information of the ospf

32.2 Showing Related Command

32.2.1 show ip ospf

Use this command to show the OSPF information in the privileged user mode.

show ip ospf [*process-id*]

Parameter description

Parameter	Description
process-id	OSPF process ID

Default N/A.

Command mode Privileged mode.

Usage guidelines This command shows the information of the OSPF routing process.

Examples

The output results of the **show ip ospf** command are as follows:

```
DES-7210# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Process uptime is 4 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This device is an ASBR (injecting external routing information)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
LsaGroupPacing: 240 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes : Enabled
Number of areas attached to this device: 1
  Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
```

```
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
Number of LSA 3. Checksum 0x0204bf
  Area 1 (NSSA)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 0
Number of fully adjacent virtual neighbors through this area is 0
Area has no authentication
SPF algorithm last executed 02:09:23.040 ago
SPF algorithm executed 4 times
Number of LSA 6. Checksum 0x028638
NSSA Translator State iselected
```

The fields in the displayed results are described as follows:

Field	Description
Router id	Router id
Process uptime	Effective time of the current OSPF process (the process does not take effect when the device-id is 0.0.0.0)
Bound to VRF	The VRF of the current OSPF
Conforms to RFC2328	The same as the RFC2328
RFC1583Compatibility flag	Whether the RFC1583 or RFC2328 is adopted for the calculation of external route. This policy is used in the selection of best ASBR and in the route comparison.
Support Tos	Only TOS0 is supported.
Supports opaque LSA	Supporting opaque-LSA
Device Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	This parameter is used for LSA pacing, checksum calculation, and aging interval.

Incomming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.
Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated
Number of LSA received	Number of LSAs received
Log Neighbor Adjency Changes	Whether the record switch for neighbor status change is enabled
Number of areas attached to this device	Total number of areas on the devices
Area type	`Area type`, including normal, stub, and nssa
Number of interfaces in this area	Number of interfaces in this area
Number of fully adjacent neighbors in this area	Number of Full neighbors of the area
Number of fully adjacent	Number of Full neighbors with

virtual neighbors through this area	virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area
NSSA Translator State	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA area.

32.2.2 show ip ospf border-devices

Use this command to show the OSPF internal routing table on the ABR/ASBR in the privileged user mode.

show ip ospf [*process-id*] **border-devices**

Parameter description

Parameter	Description
process-id	OSPF process ID

Command mode

Privileged mode.

Usage guidelines

This command shows the OSPF internal routes from the local routing device to the ABR or ASBR. The OSPF internal routing table is different from the one displayed with the **show ip route** command. The OSPF internal routing table has destination address of the router id instead of destination network.

Examples

The output results of the **show ip ospf border-devices** command are as follows:

```
DES-7210# show ip ospf border-devices
OSPF internal Routing Table
```

```
Codes: i - Intra-area route, I - Inter-area route
```

i 1.1.1.1 [2] via 10.0.0.1, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select

The fields in the displayed results are described as follows:

Field	Description
Codes	Route type code, where “i” means intra-area routes, while “I” means inter-area routes.
I	Intra-area routes
1.1.1.1	Show the OSPF ID of the border device.
[2]	Show the cost to the border device.
via 10.0.0.1	Show the next-hop gateway to the border device.
FastEthernet 0/1	Show the interface to the border device.
ABR, ASBR	Show the type of the border device, including ABR, ASBR, or both
Area 0.0.0.1	Show the area that learns the route
select	When there are multiple paths to the ASBR, the select indicates the currently selected optimal path.

32.2.3 show ip ospf database

Use this command to show the OSPF link state database information in the privileged user mode.

Different formats of the command will display different LSA information.

show ip ospf [*process-id area-id*] **database**

show ip ospf [*process-id area-id*] **database** [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**self-originate** | **max-age**]

show ip ospf [*process-id area-id*] **database** [**device**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**device**] [**adv-device**

ip address

show ip ospf [*process-id area-id*] **database** [**device**] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**network**][*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**network**] [*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**network**] [*link-state-id*] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**]

[*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**]

[*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**]

[*link-state-id*] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**external**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**external**] [*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*] **database** [**external**] [*link-state-id*] [**self-originate**]

show ip ospf [*process-id area-id*] **database** [**nssa-external**]

[*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**nssa-external**]

[*link-state-id*] [**adv-device** *ip-address*]

show ip ospf [*process-id area-id*]**database** [**nssa-external**] [*link-state-id*] [**self-originate** | **maxage**]

show ip ospf [*process-id area-id*]**database** [**database-summary**]

Parameter description

Parameter	Description
area-id	(Optional) Area ID displayed
adv-device	(Optional) Show the LSA information generated by the specified advertising device.
link-state-id	(Optional) Show the LSA information of the specified OSPF link state identifier.

self-originate	(Optional) Show the LSA information generated by the device itself.
maxage	(Optional) Display the LSAs aged.
device	(Optional) Show the OSPF device LSA information.
network	(Optional) Show the OSPF network LSA information.
summary	(Optional) Show the OSPF summary LSA information.
asbr-summary	(Optional) Show the ASBR summary LSA information.
external	(Optional) Show the OSPF external LSA information.
nssa-external	(Optional) Show the category 7 OSPF external LSA information.
opaque-area	(Optional) Show type 10 LSAs.
opaque-as	(Optional) Show type 11 LSAs.
opaque-link	(Optional) Show type 9 LSAs.
database-summary	(Optional) Show the statistics of LSAs of the link state database.

Default N/A.

Command mode Privileged mode.

Usage guidelines When the OSPF link state database is very large, you should show the information on the link state database in many ways. Proper use of these commands may help OSPF troubleshooting.

Examples The output results of the **show ip ospf database** command are as follows:

```
DES-7210# show ip ospf database
OSPF Device with ID (1.1.1.1) (Process ID 1)
Device Link States (Area 0.0.0.0)
Link ID       ADV Device     Age  Seq#      CkSum  Link count
1.1.1.1       1.1.1.1        2    0x80000011 0x6f39 2
3.3.3.3       3.3.3.3        120  0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
```

```
Link ID         ADV Device      Age  Seq#       CkSum
192.88.88.27    1.1.1.1         120  0x80000001 0x5366
Summary Link States (Area 0.0.0.0)
Link ID         ADV Device      Age  Seq#       CkSum  Route
10.0.0.0        1.1.1.1         2    0x80000003 0x350d 10.0.0.0/24
100.0.0.0       1.1.1.1         2    0x8000000c 0x1ecb 100.0.0.0/16
Device Link States (Area 0.0.0.1 [NSSA])
Link ID         ADV Device      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         2    0x80000001 0x91a2 1
         Summary Link States (Area 0.0.0.1 [NSSA])
Link ID         ADV Device      Age  Seq#       CkSum  Route
100.0.0.0       1.1.1.1         2    0x80000001 0x52a4 100.0.0.0/16
192.88.88.0     1.1.1.1         2    0x80000001 0xbb2d
192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID         ADV Device      Age  Seq#       CkSum  Route
Tag
20.0.0.0        1.1.1.1         1    0x80000001 0x033c E2
20.0.0.0/24     0
100.0.0.0       1.1.1.1         1    0x80000001 0x9469 E2
100.0.0.0/28    0
AS External Link States
Link ID         ADV Device      Age  Seq#       CkSum  Route
Tag
20.0.0.0        1.1.1.1         380  0x8000000a 0x7627 E2
20.0.0.0/24     0
100.0.0.0       1.1.1.1         620  0x8000000a 0x0854 E2
100.0.0.0/28    0
```

The fields in the displayed results of the **show ip ospf database** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Device Link States	Show the device LSA information.
Net Link States	Show the network LSA information.
Summary Net Link States	Show the summary network LSA information.
NSSA-external Link States	Show the type 7 autonomous external LSA information.
AS External Link States	Show the type 5 autonomous external LSA information.
Link ID	Link ID
ADV Device	ID of the device that advertises the LSAs
Age	Show the live period of the LSA.

Seq#	Show the sequentce number of the LSA, which is used to check aged or duplicate LSA.
Cksum	Show the checksum of the LSAs.
Link-Count	Show the number of links in the device LSA information.
Route	Show the device information included in the LSA.
Tag	Show the tag of the LSA

The output results of the **show ip ospf database asbr-summary** command are as follows:

```
DES-7210# show ip ospf database asbr-summary
     OSPF Device with ID (1.1.1.35) (Process ID 1)
        ASBR-Summary Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: ASBR-summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Device address)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
     TOS: 0  Metric: 1
```

The fields in the displayed results of the **show ip ospf database asbr-summary** command are described as follows:

Field	Description
OSPF Device with ID	Router id
AS Summary Link States	Show the summary LSA information in the AS.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.

TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.

The output results of the **show ip ospf database external** command are as follows:

```
DES-7210# show ip ospf database external
     OSPF Device with ID (1.1.1.35) (Process ID 1)
        AS External Link States
LS age: 752
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     Forward Address: 0.0.0.0
     External Route Tag: 0
```

The fields in the displayed results of the **show ip ospf database external** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Type-5 AS External Link States	Show autonomous external LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.
Metric Type	Indicate the external link type.
TOS	TOS value, which can be 0 only now.

Metric	Show the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The output results of the **show ip ospf database network** command are as follows:

```
DES-7210# show ip ospf database network
     OSPF Device with ID (1.1.1.1) (Process ID 1)


         Network Link States (Area 0.0.0.0)
LS age: 572
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.88.88.27 (address of Designated Device)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x5366
Length: 32
Network Mask: /24
     Attached Device: 1.1.1.1
     Attached Device: 3.3.3.3
```

The fields in the displayed results of the **show ip ospf database network** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Network Link States	Show the network LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.

Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the network corresponding to the LSA.
Attached Device	Show the device that is connected with the network.

The output results of the **show ip ospf database device** command are as follows:

```
DES-7210# show ip ospf database device
     OSPF Device with ID (1.1.1.1) (Process ID 1)
         Device Link States (Area 0.0.0.0)
LS age: 322
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: device-LSA
Link State ID: 1.1.1.1
Advertising Device: 1.1.1.1
LS Seq Number: 80000012
Checksum: 0x6d3a
Length: 48
Number of Links: 2

Link connected to: Stub Network
(Link ID) Network/subnet number: 100.0.1.1
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metric: 0
```

The fields in the displayed results of the **show ip ospf database device** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Device Link States	Show the device LSA information.
LS age	Show the live period of the LSA.
Options	Option
Flag	Flag
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.

Length	Show the length (in bytes) of the LSA.
Number of Links	Show the number of links associated with the device.
Link connected to	Show what the link is connected to and the network type.
(Link ID)	Link identifier
(Link Data)	Link data
Number of TOS metrics	TOS value; support TOS0 only
TOS 0 Metrics	TOS0 metric

The output results of the **show ip ospf database summary** command are as follows:

```
DES-7210# show ip ospf database summary
     OSPF Device with ID (1.1.1.1) (Process ID 1)
         Summary Link States (Area 0.0.0.0)
LS age: 499
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.0.0.0 (summary Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x330e
Length: 28
Network Mask: /24
     TOS: 0  Metric: 11
```

The fields in the displayed results of the **show ip ospf database summary** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Summary Net Link States	Show the summary network LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.

Network Mask	Show the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.

The output results of the **show ip ospf database nssa-external** command are as follows:

```
DES-7210# show ip ospf database nssa-external
     OSPF Device with ID (1.1.1.1) (Process ID 1)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 1
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x033c
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     NSSA: Forward Address: 100.0.2.1
     External Route Tag: 0
```

The fields in the displayed results of the **show ip ospf database nssa-external** command are described as follows:

Field	Description
OSPF Device with ID	Router id
NSSA-external Link States	Show the type 7 autonomous external LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.
Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequential number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.
Metric Type	Show the metric type.

TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.
NSSA:Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The output results of the **show ip ospf database external** command are as follows:

```
RDES-7210# show ip ospf database external
     OSPF Device with ID (1.1.1.1) (Process ID 1)
        AS External Link States
LS age: 1290
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     Forward Address: 0.0.0.0
     External Route Tag: 0
```

The fields in the displayed results of the **show ip ospf database external** command are described as follows:

Field	Description
OSPF Device with ID	Router id
Type-7 AS External Link States	Show the type 7 autonomous external LSA information.
LS age	Show the live period of the LSA.
Options	Option
LS Type	Show the type of the LSA.

Link State ID	Show the link ID of the LSA.
Advertising Device	Show the device advertising the LSA.
LS Seq Number	Show the sequentce number of the LSA.
Checksum	Show the checksum of the LSAs.
Length	Show the length (in bytes) of the LSA.
Network Mask	Show the network mask of the route corresponding to the LSA.
Metric Type	Show the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Show the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

Following is the display result of show ip ospf database database-summary command:

```
DES-7210# show ip ospf database database-summary
OSPF process 1:
Device Link States      : 4
Network Link States     : 2
Summary Link States     : 4
ASBR-Summary Link States : 0
AS External Link States  : 4
NSSA-external Link States: 2
```

The description of the fields displayed with the command **show ip ospf database database-summary** is as below:

Field	Description
OSPF Process	OSPF process ID
Device Link	Number of device LSAs in the area
Network Link	Number of network LSAs in the area
Summary Link	Number of summary LSAs in the area

ASBR-Summary Link	Number of ASBR summary LSAs in the area
AS External Link	Number of NSSA LSAs in the area
NSSA-external Link	Number of NSSA LSAs in the area

32.2.4 show ip ospf interface

Use this command to show the OSPF-associated interface information in the privileged user mode.

show ip ospf interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	(Optional) type of the specified interface
interface-number	(Optional) number of the specified interface

Default N/A.

Command mode Privileged mode.

Usage guidelines This command shows the OSPF information on the interface.

Examples

The output results of the **show ip ospf interface FastEthernet** *1/0* command are as follows:

```
DES-7210# show ip ospf interface fa 1/0
FastEthernet 1/0 is up, line protocol is up
Internet Address 192.88.88.27/24, Ifindex 4, Area 0.0.0.0, MTU 1500
Matching network config: 192.88.88.0/24
Process ID 1, Router id 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Device (ID) 1.1.1.1, Interface Address 192.88.88.27
Backup Designated Device (ID) 3.3.3.3, Interface Address
192.88.88.72
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
Hello due in 00:00:03
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 70784
Hello received 1786 sent 1787, DD received 13 sent 8
```

```
LS-Req received 2 sent 2, LS-Upd received 29 sent 53
LS-Ack received 46 sent 23, Discarded 1
```

The fields in the displayed results of the **show ip ospf interface serial** *1/0* command are described as follows:

Field	Description
FastEthernet 0/0 State	State of the network interface; UP means normal working and Down means faults.
Internet Address	Interface IP address
Area	OSPF area of the interface
MTU	Corresponding MTU
Matching network config	Network area configured for the corresponding OSPF
Process ID	Corresponding process ID
Router id	OSPF router id
Network Type	OSPF network type
Cost	OSPF interface cost
Transmit Delay is	OSPF interface transmit delay
State	DR/BDR state ID
Priority	Priority of the interface
Designated Device(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated device(ID)	Router id of the BRD of the interface
BDR's Interface address	Address of the BDR of the interface
Time intervals configured	The Hello, Dead, Wait, and Retransmit intervals of the interface
Hello due in	Time when the previous Hello is sent
Neighbor count	Total number of neighbors
Adjacent neighbor count	Number of **Full** neighbors
Crypt Sequence Number	The corresponding md5 authentication number of the interface
Hello received send	Statistics on the Hello packets sent and received

DD received send	Statistics on the DD packets sent and received
LS-Req received send	Statistics on the LS request packets sent and received
LS-Upd received send	Statistics on the LS update packets sent and received
LS-Ack received send	Statistics on the LS response packets sent and received
Discard	Statistics on the discarded OSPF packets

32.2.5 show ip ospf neighbor

Use this command to show the OSPF neighbor list in the privileged user mode.

show ip ospf [*process-id*] **neighbor** [[**detail**] | [[*interface-type* *interface-number*] [*neighbor-id*]]]

Parameter description

Parameter	Description
Detail	(Optional) Show the neighbor details.
interface-type *interface-number*	(Optional) Show the neighbor information of the specified interface
neighbor-id	(Optional) Show the information of the specified neighbor

Default N/A.

Command mode Privileged mode.

Usage guidelines This command shows neighbor information usually used to check whether the OSPF is running normally.

Examples The output results of the **show ip ospf neighbor** command are as follows:

```
DES-7210# show ip ospf neighbor
OSPF process 1,1 Neighbors, 1 is Full:
Neighbor ID     Pri   State              Dead Time   Address
Interface
3.3.3.3          1   Full/BDR           00:00:32    192.88.88.72
FastEthernet 1/0
```

```
DES-7210# show ip ospf neighbor detail
Neighbor 3.3.3.3, interface address 192.88.88.72
   In the area 0.0.0.0 via interface FastEthernet 1/0
   Neighbor priority is 1, State is Full, 11 state changes
   DR is 192.88.88.27, BDR is 192.88.88.72
   Options is 0x52 (*|O|-|EA|-|-|E|-)
   Dead timer due in 00:00:32
   Neighbor is up for 05:11:27
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
   Crypt Sequence Number is 0
   Thread Inactivity Timer on
   Thread Database Description Retransmission off
   Thread Link State Request Retransmission off
Thread Link State Update Retransmission off
Thread Poll Timer on
```

The fields in the displayed results of the **show ip ospf neighbor** command are described as follows:

Field	Description
Neighbor ID	Neighbor ID
Pri	Neighbor priority (for selection of DR)
State	Neighbor status
Dead Time	Remaining time for the neighbor to enter the Dead status
Address	The corresponding interface address of the neighbor
Interface	The corresponding interface of the neighbor
interface address	The interface address of the neighbor device
In the area	Show the area that learns the neighbor.
via interface	Show the interface that learns the neighbor
Neighbor priority	Priority of the neighbor OSPF

State	OSPF neighbor connection state. FULL means the stable state; DR indicates that the neighbor is the designated device; BDR indicates that the neighbor is the backup designated device; DROTHER indicates that the neighbor is not a DR/BDR. Point-to-point network type has no DR or DBR.
State changes times	Times of state changes
Dead Time	Dead time of the neighbor
DR	Interface address of the DR elected of the neighbor device (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected of the neighbor device (that is, the BDR field of the Hello packet)
Options	Hello packet E-bit option, where 0 indicates that the area is a STUB area; 2 indicates that the area is not a STUB area.
Dead timer due in	Dead time of the neighbor device
Neighbor up time	Period from when the device is discovered till now
Database Summary List	Statistics on the neighbor DD packets
Link State Request List	Statistics on the neighbor LS request packets
Link State Retransmission List	Statistics on the neighbor re-transmit packets
Crypt Sequence Number	Area MD5 authentication code
Thread Inactivity Timer	Status of invalid neighbor timer
Thread Database Description Retransmission	Status of DD packet timer of the interface
Thread Link State Request Retransmission	Status of LS request packet timer of the interface

Thread Link State Update Retransmission	Status of LS update packet timer of the interface
Thread Poll Timer	Poll Timer start status of the static neighbor

32.2.6 show ip ospf route

Use this command to show the OSPF routes.

show ip ospf [*process-id*] **route** [**count**]

Parameter description

Parameter	Description
process-id	OSPF process ID. All OSPF routes will be shown without an ID specified.
Count	Show the statistics of various OSPF routes.

Command mode

Privileged mode.

Examples

```
DES-7210# show ip ospf route
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF,
IA - OSPF inter area  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2

E2 100.0.0.0/24 [1/20] via 192.88.88.126, FastEthernet 1/0
C  192.88.88.0/24 [1] is directly connected, FastEthernet 1/0, Area 0.0.0.1
```

The description of every field shown via command show ip ospf routeis as below:

Field	Description
codes	Route type and correspond abbreviation and description
100.0.0.0/24	Route prefix
[1]	Route cost
via	Route next hop and interface

32.2.7 show ip ospf summary-address

Use this command to show the converged route of all redistributed routes in the privileged user mode.

show ip ospf summary-address

Command mode	Privileged mode.
Usage guidelines	This command is valid only on the NSSA ABR, and shows only the routes with local convergence operation.

Examples	The output results of the **show ip ospf summary-address** command are as follows:
	`DES-7210#show ip ospf summary-address`
	`Summary Address Summary Mask Advertise Status Aggregated subnets`
	`------------ ------------ ------------ -------- --------------`
	`202.101.0.0 255.255.0.0 advertise Inactive 0`
	`DES-7210#`

Parameter	Description
Summary Address	IP address to be converged
Summary Mask	Mask to be converged
Advertise	Whether to advertise the converged route
Status	The convergence range takes effect or not
Aggregated subnets	Number of external routes included in the converged route

32.2.8 show ip ospf virtual-link

Use this command to show the OSPF virtual link information in the privileged user mode.

show ip ospf [*process-id*] **virtual-link**

Command mode	Privileged mode.
Usage guidelines	If no virtual link is configured, the command only shows the neighbor status as well as other related information. The **show ip ospf neighbor** command does not show the neighbor of virtual link.

Examples

The output results of the **show ip ospf virtual-links** command are as follows:

```
DES-7210# show ip ospf virtual-links
Virtual Link VLINK0 to device 1.1.1.1 is up
Transit area 0.0.0.1 via interface FastEthernet 0/1
Local address 10.0.0.37/32
Remote address 10.0.0.27/32
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
Hello due in 00:00:05
Adjacency state Full
```

The fields in the displayed results are described as follows:

Field	Description
Virtual Link VLINK0 to device	Show the virtual link neighbors and their status.
Virtual Link State	Show the virtual link state.
Transit area	Show the transit area of the virtual link.
via interface	Show the associated interface of the virtual link.
Local address	Local interface address
Remote Address	Peer interface address
Transmit Delay	Show the transmit delay of the virtual link.
State	Interface state
Time intervals configured	The Hello, Dead, Wait, and Retransmit interval of the interface
Adjacency State	Neighbor state, where FULL means the stable state

33 BGP4 Configuration Commands

33.1 Configuration Related Commands

33.1.1 address-family ipv4

Use this command to enter " **address-faimly IPv4**" to configure the BGP configuration mode. Use the **exit-address-family** command to exit the BGP address configuration mode.

address-family ipv4 [**unicast**]

no address-family ipv4 [**unicast**]

Parameter description

Parameter	Description
unicast	Optional, detailed IPv4 unicast address prefix

Default configuration

Unicast address prefix.

Command mode

BGP configuration mode.

Usage guidelines

In the BGP address configuration mode, the standard IPv4 address can be used for the configuration.

To exit to the BGP configuration mode, run the command **exit-address-family**

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# address-family ipv4
```

Related commands

Command	Description
exit-address-family	Exit the mode.

33.1.2 address-family ipv4 vrf

Use this command to enter the address-family IPv4 VRF configuration mode to configure BGP and enable the exchange of route information of a VRF. Use the **no** form of this command to disable the exchange function or the **exit-address-family** command to exit the BGP address configuration mode.

address-family ipv4 vrf *vrf-name*

no address-family vrf *vrf-name*

Parameter description

Parameter	Description
vrf-name	VRF name

Default configuration

No vrf is defined by default.

Command mode

BGP configuration mode.

Usage guidelines

You can execute this command to configure or exit the exchange of route information between PEs and CEs.

To exit to the BGP configuration mode, run the **exit-address-family** command**.**

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# address-family ipv4 vrf vpn1
```

Related commands

Command	Description
exit-address-family	Exit the configuration mode.

33.1.3 address-family vpnv4

Use this command to enter the address-family VPN configuration mode and enable the exchange of VPN route information between PE peers. Use the **exit-address-family** command to exit the BGP address configuration mode.

address-family vpnv4 [**unicast**]

no address-family vpnv4 [**unicast**]

Parameter description

Parameter	Description
unicast	Optional, detailed IPv4 unicast address prefix

Default configuration	No VPN address family is defined by default.
Command mode	BGP configuration mode.
Usage guidelines	Execute this command to enter the address-family VPN configuration mode and enable the exchange of VPN route information between PE peers. To exit to the BGP configuration mode, run the command **exit-address-family**
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# address-family vpnv4`

Related commands

Command	Description
exit-address-family	Exit the mode.

33.1.4 aggregate-address (IPv4)

Use this command to set the aggregate IPv4 route. The **no** form of the command is used to disable this function.

aggregate-address *ip-address mask* [**as-set**] [**summary-only**]

no aggregate-address *ip-addres mask* [**as-set**] [**summary-only**]

Parameter description

Parameter	Description
ip address	IP address of the aggregate route
mask	Mask of the aggregate route
as-set	Keep the AS path information of the path in the aggregate address range.
summary-only	Advertise only the aggregate route.

Default configuration	N/A.
Command mode	BGP configuration mode, address-family IPv4 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines	By default, the BGP-enabled device will advertise all path information both before and after aggregation. If you only hope to advertise the aggregate route, use the **aggregate-address summary-only** command.
Examples	DES-7210(config)# **router bgp** *65000* DES-7210(config-router)# **aggregate-address** *10.0.0.0 255.0.0.0* **as-set**

Related commands

Command	Description
router bgp	Enable the BGP protocol.

33.1.5 auto-summary

Use this command to set BGP route auto-summary. Use the **no** form of the command to disable this function.

auto-summary

no auto-summary

Parameter description	N/A.
Default configuration	By default, this function is disabled.
Command mode	BGP configuration mode, BGP IPv4 address-family configuration mode.
Usage guidelines	Use this command to reduce the routing summary in the routing table.
Examples	DES-7210(config)# **router bgp** *65000* DES-7210(config-router)# **auto-summary**

Related commands

Command	Description
router bgp	Enable BGP.

Platform description	

33.1.6 bgp always-compare-med

Use this command to compare Multi Exit Discriminator (MED) all the time. You can use the **no** form of the command to disable this function.

bgp always-compare-med

no bgp always-compare-med

Parameter description	N/A.
Default configuration	By default, the MED of the peer path from the same AS is compared.
Command mode	BGP configuration mode.
Usage guidelines	By default, the MED value is compared for the path of the peer from the same AS. If you hope to allow comparing MED values for the paths from different ASs, this command can be used. If there are multiple valid paths to the same destination, the one with lower MED value has higher priority. Unless you are sure that the different ASs are using the same IGP and routing method, this command is not recommended.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# bgp always-compare-med`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath med confed	Compare the MED value of the path of the peer from different ASs while selecting the optimal path.
bgp bestpath med missing-as-worst	Set the priority of the path without MED attribute as the lowest while selecting the optimal path.
bgp deterministic-med	Compare the path of the peer from the same AS while selecting the optimal path.

Platform description	

33.1.7 bgp bestpath as-path ignore

Use this command to disregard the length of the AS path. You can use the **no** form of the command to disable this function.

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Parameter description	N/A.
Default configuration	By default, the AS path length is considered in choosing the optimal path.
Command mode	BGP configuration mode.
Usage guidelines	The BGP will not take the length of the AS path into account when it selects the optimal path as specified in RFC1771. In general, the shorter the length of the AS path, the higher the path priority is. Hence, we take the length of the AS path when we select the optimal path. You can determine whether it is necessary to take the length of the AS path into account when you select the optimal path according to the actual condition.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# bgp bestpath as-path ignore`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.

Platform description	

33.1.8 bgp bestpath compare-confed-aspath

Use this ocmmand to compare the AS path length of the confederation from the same external routes during selecting the optimal path, with smaller AS path in the confederation for higher path priority. You can use the **no** form of the command to disable this function.

bgp bestpath compare-confed-aspath

no bgp bestpath compare-confed-aspath

Parameter description	N/A.
Default configuration	By default, the AS path of the ebgp peer routes inside the same confederation is not compared during selecting the optimal path. Instead, the routing method is implemented.
Command mode	BGP configuration mode.
Usage guidelines	By default, during the selection of the same routing information from the peer of the internal EBGP, the AS path of the confederation is not compared. This command is used to compare the AS path of the confederation. Note that if a route does not contain the AS path of the confederation, it is not possible to implement the AS path comparison for that route.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# bgp bestpath compare-confed-aspath`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp router-id	Set the BGP Device ID.

Platform description

33.1.9 bgp bestpath compare-routerid

Use this command to compare the router ID of the same external routes during selecting the optimal path, with smaller router ID for higher path priority. You can use the **no** form of the command to disable this function.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Parameter description	N/A.
Default configuration	By default, if two paths received from different EBGP peers have the same path, the first one is considered with higher priority.
Command mode	BGP configuration mode.
Usage guidelines	By default, if two paths with full identical path attributes are received from different EBGP Peers during the selection of the optimal path, we will select the optimal path according to the sequence of receiving the paths. You can select the path with smaller Device ID as the optimal path by configuring the following commands.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# bgp bestpath compare-routerid`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp router-id	Set the BGP Device ID.

Platform description

33.1.10 bgp bestpath med confed

Use this command to compare the MED value of the path of the internal peer from AS confederation during selecting the optimal path. You can use the **no** form of the command to disable this function.

bgp bestpath med confed [missing-as-worst]

no bgp bestpath med confed [missing-as-worst]

Parameter description

Parameter	Description
missing-as-worst	Set the priority of the path without MED attribute as the lowest.

Default configuration	Disabled.
Command mode	BGP configuration mode.
Usage guidelines	The MED attribute of the path is transferred between the member ASs inside the confederation. You may set always comparing this value.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# bgp bestpath med confed`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath always-compare-med	Compare the MED value of the path of the peer from different ASs while selecting the optimal path.
bgp bestpath med missing-as-worst	Set the priority of the path without MED attribute as the lowest while selecting the optimal path.
bgp deterministic-med	Compare the path of the peer from the same AS while selecting the optimal path.

Platform description

33.1.11 bgp bestpath med missing-as-worst

Use this command to set the priority of the path without MED attribute as the lowest while selecting the optimal path. You can use the **no** form of the command to disable this function.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

Parameter description	N/A.
Default	By default, if a path without MED attribute is received, the MED value

configuration	of the path is considered as 0. This kind of routes has the highest priority according to the known rule.
Command mode	BGP configuration mode.
Usage guidelines	By default, if the path whose MED attribute is not set is received, the MED value of this path will be taken as 0. For the smaller the MED value, the higher the priority of the path is, the MED value of this path reaches the highest priority. If you hope the path without MED attribute configured has the lowest priority, this command can be used.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# bgp bestpath med missing-as-worst`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath always-compare-med	Compare the MED value of the path of the peer from different ASs while selecting the optimal path.
bgp bestpath med confed	Set the priority of the path without MED attribute as the lowest while selecting the optimal path.
bgp deterministic-med	Compare the path of the peer from the same AS while selecting the optimal path.

Platform description

33.1.12 bgp client-to-client reflection

Use this command to enalbe the route reflection function between clients on the device. The **no** form of the command disables the route reflection function between clients.

bgp client-to-client reflection

no bgp client-to-client reflection

Parameter description	N/A.
Default configuration	Enabled without the client for route reflection
Command mode	BGP configuration mode.
Usage guidelines	In general, it is not necessary to establish the connection relationship between the clients of the route reflector within the cluster, and the route reflector will reflect the route among clients. However, if the full connection relationship is established for all clients, the function for the route reflector to reflect the client route can be disabled. To disable the route reflection function, use the command **no bgp client-to-client reflection**.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# no bgp client-to-client reflection`

Related commands

Command	Description
bgp cluster-id	Configure the cluster ID of the route reflector.
neighbor route-reflector-client	Configure the client of the route reflector and configure itself as the route reflector.

Platform description

33.1.13 bgp cluster-id

Use this command to configure the cluster ID of the route reflector. Use the **no** form of the command to restore it to the default setting.

bgp cluster-id *cluster-id*

no bgp cluster-id [*cluster-id*]

Parameter description

Parameter	Description
cluster-id	Cluster ID of the route reflector, an IP address of up to four bytes or an integer

		(must be entered in form of IP address).

Default configuration

N/A.

Command mode

BGP configuration mode.

Usage guidelines

In general, one group is only configured with one route reflector. In this case, the Device ID of the route reflector can be used to identify this cluster. To increase the redundancy, you can set more than one route reflector within this cluster. In this case, you must configure the cluster ID, so that one route reflector can identify the route update from other route reflectors of this cluster.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# bgp cluster-id 10.0.0.1
```

Related commands

Command	Description
bgp client-to-client reflection	Configure the route reflection between clients.
neighbor route-reflector-client	Configure the client of the route reflector and configure itself as the route reflector.

Platform description

33.1.14 bgp confederation identifier

Use this command to configure the AS confederation identifier. Use the **no** form of the command to restore it to the default setting.

bgp confederation identifier *as-number*

no bgp confederation identifier

Parameter description

Parameter	Description
as-number	AS confederation identifier in the range of 1 to 65535

Default

N/A.

configuration	
Command mode	BGP configuration mode.
Usage guidelines	The confederation is a measure to reduce the connections of the IBGP peer within the AS. One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. For the external confederation, the whole confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information.
Examples	`DES-7210(config-router)# bgp confederation identifier 65000`

Related commands

Command	Description
bgp confederation peers	Add member AS of the AS confederation.

Platform description

33.1.15 bgp confederation peers

Use this command to configure the member AS of the AS confederation. The **no** form of the command deletes the configured member AS.

bgp confederation peers *as-number* [*as-number,…*]

no bgp confederation peers *as-number* [*as-number,…*]

Parameter description

Parameter	Description
as-number	Member AS in the confederation In the range of 1 to 65535

Default configuration	N/A.
Command mode	BGP configuration mode.
Usage guidelines	The confederation is a measure to reduce the connections of the IBGP peer within the AS. One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. For the external confederation, the whole confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information. This command is used to specify the member AS of a confederation. Note: This command can configure up to 15 members of a confederation at one time. For more members, enter them for several times.
Examples	`DES-7210(config-router)# bgp confederation peers 65000 65100`

Related commands

Command	Description
bgp confederation identifier	Configure the confederation identifier.

Platform description	

33.1.16 bgp default ipv4-unicast

Use this command to set the IPv4 unicast address as the default address family. The **no** form of the command removes the configuration.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Parameter description	N/A.
Default configuration	By default, the IPv4 unicast address is the default address family.
Command mode	BGP configuration mode.
Usage guidelines	This command is used to set the default address family of BGP as the IPv4 unicast address.
Examples	`DES-7210(config-router)# default ipv4-unicast`

Related commands

Command	Description
address-family ipv4	Enter the IPv4 address mode.

Platform description

33.1.17 bgp default local-preference

Use this command to set the default local-preference attribute value. Use the **no** form of the command to restore the defaults.

bgp default local-preference *value*

no bgp default local-preference

Parameter description

Parameter	Description
value	Local priority attribute in the range 0 to 4294967295

Default configuration	100.
Command mode	BGP configuration mode.

Usage guidelines

The BGP takes the local preference as the foundation to compare with the priority of the path learned from the IBGP peers. The larger the local preference value, the higher the priority of the path is.

The BGP speaker sends the external route received to the IBGP peers to add the local priority value.

Examples

```
DES-7210(config-router)# bgp default local-preference 200
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath always-compare-med	In electing the optimal path, allow comparing the MED value of the path of the peer from different ASs.
bgp bestpath med confed	In electing the optimal path, allow comparing the MED value of the path of the internal peer from AS community.
bgp bestpath med missing-as-worst	In electing the optimal path, allow setting the priority of the path without MED attribute as the lowest.

Platform description

33.1.18 bgp deterministic-med

This command sets comparing preferentially the MED values of peer paths from the same AS. By default, the comparison is based on the received order, and the one received the last is compared first. The **no** format of the command turns off it.

bgp deterministic med

no bgp deterministic med

Parameter description

N/A.

Default configuration

By default, the function is disabled.

Command mode

BGP CONFIGURATION MODE.

Usage guidelines	By default, they will be compared with each other according to the sequence the paths are received when the optimal path is selected. If you hope to compare with the path of the peers from the same AS firstly, execute the following operations in the BGP configuration mode:
Examples	`DES-7210(config-router)# bgp deterministic med`

Related commands

Command	Description
show ip bgp	Show the BGP route entry.
bgp bestpath always-compare-med	Compare the MED value of the path of the peer from different ASs while selecting the optimal path.
bgp bestpath med confed	Set the priority of the path without MED attribute as the lowest while selecting the optimal path.
bgp bestpath med missing-as-worst	Compare the path of the peer from the same AS while selecting the optimal path.

Platform description

33.1.19 bgp enforce-first-as

Use this command to reject the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number. The **no** format of the command disables the function.

bgp enforce-first-as

no bgp enforce-first-as

Parameter description	N/A.
Default configuration	Enabled
Command mode	BGP configuration mode.

Usage guidelines	By default, the AS number of the device is put into the path section for updating the update message.

Examples

```
DES-7210(config-router)# bgp enforce-first-as
```

Related commands

Command	Description
show ip bgp	Show the BGP route entry.

Platform description

33.1.20 bgp fast-external-fallover

When the network interface that is used in establishing the connection of the directly-connected EBGP peer fails, this command is used to establish the BGP session connection quickly. You can use the **no** form of the command to disable this function.

bgp fast-external-fallover

no bgp fast-external-fallover

Parameter description	N/A.
Default configuration	Enabled.
Command mode	BGP configuration mode.
Usage guidelines	This command takes effect only for the directly-connected EBGP neighbor.

Examples

```
DES-7210(config-router)# bgp faster-external-fallover
```

Related commands

Command	Description
router bgp	Enabled the BGP protocol.

Platform description	

33.1.21 bgp log-neighbor-changes

Use this command to log the BGP status changes without turning on **debug**. You can use the **no** form of the command to disable this function.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Parameter description	N/A.
Default configuration	Disabled.
Command mode	BGP configuration mode.
Usage guidelines	The **debug** command can also be used to log the BGP status changes. But this command may consume a great deal of resources.
Examples	`DES-7210(config-router)# bgp log-neighbor-changes`

Related commands

Command	Description
router bgp	Enabled the BGP protocol.

Platform description	

33.1.22 bgp router-id

Use this command to configure the ID-IP address of the device. The **no** form of the command restores it to the default IP address.

bgp router-id *ip-address*

no bgp router-id *ip-address*

Parameter description

Parameter	Description
ip address	IP address

Default configuration

By default, the loop-back interface of the device is selected preferentially. If it does not exist, the device ID of the device is used.

Command mode

BGP configuration mode.

Usage guidelines

This command is used to configure the ID-IP address of the device used in running the BGP protocol.

Examples

```
DES-7210(config-router)# bgp router-id 10.0.0.1
```

Related commands

Command	Description
show ip bgp dampening dampened-paths	Show the suppressed routing information.
bgp dampening	Enable the route dampening function and set the dampening parameters.

Platform description

33.1.23 clear bgp ipv4 unicast

Use this command to reset the BGP.

clear bgp ipv4 unicast {* |*address* | *as number* } [[**soft]** [**in** | **out**]]

Parameter description

Parameter	Description
*****	Reset all the current BGP sessions, and the BGP OVERFLOW state.
address	Reset the BGP session with the specified peer.
as number	Reset the sessions with all members in the specified AS.
in	Perform soft resetting for the received routing information.
out	Perform soft resetting for the

	redistributed routing information.
soft	Perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Note: This command is used to require all connected BGP devices to support the route refresh function. This product supports the route refresh function.

At any time, once the routing policy or BGP configuration changes, an effective way must be available to implement the new routing policy or configuration. Traditional measure is to close it and reestablish new BGP connection.

This product supports implementing new routing strategy without the close of the BGP session connection by the configuration of the soft reset for BGP effectively.

For the peer that does not support the route refresh function, you may run the **neighbor soft-reconfiguration inbound** command to keep a copy of original routing information of every specified BGP peer on the local BGP speaker. This will consume some resources.

You can judge whether the BGP peer supports the route refresh function by the **show ip bgp neighbors** command. If it is supported, you need to execute the **neighbor soft-reconfiguration inbound** command when the inbound routing strategy changes.

Examples

```
DES-7210# clear bgp ipv4 unicast *
```

Related commands

Command	Description
neighbor soft-reconfiguration inbound	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group).

	show ip bgp	Show the BGP route entry.

33.1.24 clear bgp ipv4 unicast dampening

Use this command to clear the dampening information and de-suppress the suppressed routes.

clear bgp ipv4 unicast dampening [*address* [*mask*]]

Parameter description

Parameter	Description
address	IP address
mask	Mask

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to clear the BGP route dampening information and de-suppress the suppressed routes. This command can be used to restart the BGP route dampening.

Examples

```
DES-7210# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Related commands

Command	Description
show ip bgp dampening dampened-paths	Show the suppressed routing information.
bgp dampening	Enable the route dampening function and set the dampening parameters.

Platform description

33.1.25 clear bgp ipv4 unicast external

Use this command to reset all EBGP connections.

clear bgp ipv4 unicast external [[**soft**] [**in | out**]]

Parameter description

Parameter	Description
in	Without soft, reset the session of the peer to establish active connection.
out	Without soft, reset the session of the local BGP speaker to establish active connection.
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to reset the specified external BGP connection.

Examples

```
DES-7210# clear ip bgp external in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp neighbors	Show the neighbor information.

Platform description

33.1.26 clear bgp ipv4 unicast flap-statistics

Use this command to clear the unsuppressed routes.

clear bgp ipv4 unicast flap-statistics [*address*[*mask*]]

Parameter description

Parameter	Description
address	IP address
mask	Mask

Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command can be used only to clear the statistics of unsuppressed routes. It does not de-suppress the suppressed routes. If you hope to clear all route statistics and de-suppress the suppressed routes, run the **clear ip bgp dampening** command.
Examples	`DES-7210# clear ip bgp flap-statistics`

Related commands

Command	Description
bgp dampening	Enable the route dampening function and set the dampening parameters.
show ip bgp	Show the BGP route entry.

Platform description

33.1.27 clear bgp ipv4 unicast peer-group

Use this command to reset the session with all members in the peer group.

clear bgp ipv4 unicast peer-group *peer-group-name* [[**soft**] [**in** | **out**]]

Parameter description

Parameter	Description
peer-group-name	Name of the peer group.
in	Without soft, reset the session of the peer to establish active connection.
out	Without soft, reset the session of the local BGP speaker to establish active connection.
soft	Perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Perform soft resetting for the received routing information.

	soft out	Perform soft resetting for the distributed routing information.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command resets the BGP session with all members in the peer group.

Examples

```
DES-7210# clear ip bgp peer-group my-group in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp	Show the BGP route entry.

Platform description

33.1.28 clear ip bgp

Use this command to reset the BGP session.

clear ip bgp {* |**ipv4 unicast***address* | *as number* } [[**soft**] [**in** | **out**]]

Parameter description

Parameter	Description
*	Reset all the current BGP sessions.
ipv4	Reset the peer of the specified IPv4 address family.
address	Reset the BGP session with the specified peer.
as number	Reset the sessions with all members in the specified AS.
in	Perform soft resetting for the received routing information.
out	Perform soft resetting for the redistributed routing information.
soft	Perform soft resetting for all routing information

	received/sent from/to the specified peer
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Note: All connected BGP devices must support the route refresh function to execute this command. This product supports the route refresh function.

At any time, once the routing policy or BGP configuration changes, an effective way must be available to implement the new routing policy or configuration. Traditional measure is to close it and reestablish new BGP connection.

This product supports implementing new routing strategy without the close of the BGP session connection by the configuration of the soft reset for BGP effectively.

For the peer that does not support the route refresh function, you may run the **neighbor soft-reconfiguration inbound** command to keep a copy of original routing information of every specified BGP peer on the local BGP speaker. This will consume some resources.

You can judge whether the BGP peer supports the route refresh function by the **show ip bgp neighbors** command. If it is supported, you need to execute the **neighbor soft-reconfiguration inbound** command when the inbound routing strategy changes.

Examples

```
DES-7210# clear bgp ipv4 unicast *
```

Related commands

Command	Description
neighbor soft-reconfiguration inbound	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group).
show ip bgp	Show the BGP route entry.

33.1.29 clear ip bgp dampening

Use this command to clear the dampening information and de-suppress the suppressed routes.

clear ip bgp [**ipv4 unicast**] **dampening** [*address mask*]

Parameter description

Parameter	Description
ipv4 unicast	IPv4 unicast
address	IP address
mask	Mask

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to clear the BGP route dampening information and de-suppress the suppressed routes. This command can be used to restart the BGP route dampening.

Examples

```
DES-7210# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Related commands

Command	Description
show ip bgp dampening dampened-paths	Show the suppressed routing information.
bgp dampening	Enable the route dampening function and set the dampening parameters.

33.1.30 clear ip bgp external

Use this command to reset all EBGP connections.

clear ip bgp external [**ipv4 unicast**] [[**soft**] [**in | out**]]

Parameter description

Parameter	Description
ipv4 unicast	IPv4 unicast session
in	Without soft, reset the session through which the peer establishes active connection.

	out	Without soft, reset the session through which the local BGP speaker establishes active connection.
	soft in	Perform soft resetting for the received routing information.
	soft out	Perform soft resetting for the distributed routing information.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command is used to reset the specified external BGP connection.

Examples

```
DES-7210# clear ip bgp external in
```

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp neighbors	Show the neighbor information.

33.1.31 clear ip bgp flap-statistics

Use this command to clear the unsuppressed routes.

clear ip bgp flap-statistics [*address*[*mask*]]

Parameter description

Parameter	Description
address	IP address
mask	Mask

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines	This command can be used only to clear the statistics of unsuppressed routes. It does not de-suppress the suppressed routes. If you hope to clear all route statistics and de-suppress the suppressed routes, run the **clear ip bgp dampening** command.
Examples	`DES-7210# clear ip bgp flap-statistics`

Related commands

Command	Description
bgp dampening	Enable the route dampening function and set the dampening parameters.
show ip bgp	Show the BGP route entry.

33.1.32 clear ip bgp peer-group

Use this command to reset the session with all members in the peer group.

clear ip bgp peer-group *peer-group-name* [**ipv4 unicast**] [[**soft**] [**in** | **out**]]

Parameter description

Parameter	Description
peer-group-name	Name of the peer group.
ipv4 unicast	ipv4 unicast session
in	Without soft, reset the session through which the peer establishes active connection.
out	Without soft, reset the session through which the local BGP speaker establishes active connection.
soft	Perform soft resetting for all routing information received/sent from/to the specified peer
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration	N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command resets the BGP session with all members in the peer group.
Examples	`DES-7210# clear ip bgp peer-group my-group in`

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp	Show the BGP route entry.

33.1.33 clear ip bgp vrf

Use this command to reset the BGP sessions of all the members of the VRF.

clear ip bgp vrf *vrf-name* [* *address* }[**soft** [**in** | **out**]]

Parameter description

Parameter	Description
vrf-name	VRF name
*	Reset all the current BGP sessions.
ipv4 unicast	Reset the BGP session of the peer of the IPv4 unicast address family.
address	Reset the BGP session with the specified peer.
in	Without soft, reset the direct session with the specific peer.
out	Without soft, reset the direct session with the BGP speaker.
soft	Perform soft resetting for all routing information received/sent from/to the specified peer.
soft in	Perform soft resetting for the received routing information.
soft out	Perform soft resetting for the distributed routing information.

Default configuration	N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command resets the BGP sessions of all the members of the VRF.
Examples	`DES-7210# clear ip bgp vrf my-vrf in`

Related commands

Command	Description
clear ip bgp	Reset the BGP session.
show ip bgp	Show the BGP route entry.

Platform description

33.1.34 default-information originate

Use this command to redistribute the default route in the process of route redistribution. The **no** form of this command is used to disable the redistribution of the default route.

[no] default-information originate

Parameter description	N/A
Default configuration	Disabled
Command mode	BGP configuration mode
Usage guidelines	This command redistributes the default route, which takes effect only when the routes to be redistributed has the default one. This **default-information originate** command is similar to the **network** command. The difference is that the former redistributes the default route. For the later command, the IGP must have the default route.

Examples

```
DES-7210(config-router)# default-information originate
```

Related commands

Command	Description
network	Configure the routes to be advertised.
redistribute	Redistribute the routes of other protocol.

Platform description

33.1.35 default-metric

Use this command to set the metric for route redistribution. The **no** form of this command is used to remove the configuration and restore it to the default value.

default-metric number

no default-metric

Parameter description

Parameter	Description
number	Metric number in the range of 1 to 4294967295

Default configuration

No metric is set by default.

Command mode

BGP configuration mode and various address-family configuration modes

Usage guidelines

This command sets the metric of the routes to be redistributed for integrity.

Note that:

The metric set with the command cannot cover the metric value set with the **redistribute metric** command.

The value is 0 when the default metric applies to the redistributed connected routes.

Examples

```
DES-7210(config-router)# default-metric 45
```

Related commands

Command	Description
redistribute	Redistribute the routes of other protocol.

Platform description

33.1.36 distance bgp

Use this command to set different management distances for different types of BGP routes. The **no** command is used to restore it to the default.

distance bgp *external-distance internal-distance local-distance*

no distance bgp [*external-distance internal-distance local-distance*]

Parameter description

Parameter	Description
external-distance	Route management distance learned from the EBGP peers in the range: 1 to 255
internal-distance	Route management distance learned from the IBGP peers in the range 1 to 255
local-distance	The management distance of route learned from the peers. However, the optimal one can be learned from the IGP. In general, these routes are indicated by the **Network Backdoor** command. Range: 1 to 255

Default configuration

The parameter defaults are as follows:

external-distance - 20

internal-distance - 200

local-distance - 200

Command mode

BGP configuration mode.

Usage guidelines

It is not recommended to change the management distance of the BGP route. If it is definitely necessary, observe the following points:

1. "*external-distance*" shall have a lower management distance than the other IGP routing protocols (OSPF, RIP, etc.);
2. *internal-distance* and *local-distance* shall have higher management distance than the other IGP routing protocols.

Examples

```
DES-7210(config-router)# distance bgp 20 20 200
```

Related commands

Command	Description
neighbor soft-reconfiguration inbound	Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group).
show ip bgp	Show the BGP route entry.

Platform description

33.1.37 exit-address-family

Use this command to exit the BGP **address-family** configuration mode.

exit-address-family

Parameter description

N/A.

Default configuration

N/A.

Command mode

BGP **address-family** configuration mode.

Usage guidelines

This command can be used to exit from various address-family modes of the BGP to the BGP configuration mode.

Examples

```
DES-7210(config-router-af)#exit-address-family
```

Related commands

Command	Description
address-family ipv4	Enter the **address-family ipv4** configuration mode.

Platform description

33.1.38 ip as-path access-list

Use this command to specify the regular expression based AS path filtering rule. The **no** command is used to delete the rule.

ip as-path access-list *path-list-num* {**permit** | **deny**}

regular-expression

no ip as-path access-list *path-list-num*

Parameter description

Parameter	Description
path-list-num	Name of the AS path control list based on the regular expression in the range of 1 to 500
permit	Permit the accesses
deny	Deny the accesses
regular-expression	Regular expression Range: 1 to 255 characters.

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

For the regular expression, see BGP Configuration in the configuration guide.

Examples

```
DES-7210(config-router)# ip as-path access-list 1 deny  ^123$
```

Related commands

Command	Description
neighbor filter-list	Apply the AS-path access control list on the specified peer.
neighbor distribute-list	Apply the distribution list on the specified peer.

Platform description

33.1.39 maximum-prefix

Use this command to limit the maximum number of prefix in the routing database in the address family. Use the **no** form of this command to restore it to the default value.

maximum-prefix *maximum*

no maximum-prefix

Parameter description

Parameter	Description
maximum	The maximum number of prefix in the routing database in the address family, in the range of 1 to 4294967295.
no	Returns to the default value.

Default configuration

In different addrses families, the default maximum numbers of prefix in the routing database are different:

The default number in the IPv4 VRF, VPNv4 address family is 1000;

The default number in the IPv4 unicast address family is 4294967295.

Command mode

BGP configuration mode, BGP IPv4 address family configuration mode, BGP IPv4 VRF configuration mode, BGP VPNv4 configuration mode.

Usage guidelines

In a BGP address family, the routing prefix may be introduced through the redistribute or the neighbor learning. Once the routing prefix in the BGP address family reaches the maximum number, this address family will enter to the overflow state.

Use the **show bgp** { *addressfamily* | **all** } **summary** command to show the state of routing database.

It is necessary to reconfigure the BGP for state clearing, or use the **clear bgp** { *addressfamily* | **all** } * command to reset the address family.

Note:

When the address family is overflow, it fails to use this command for modification.

Examples

The following example shows how to set the maximum number of prefix in the BGP routing database in the ipv4 multicast address

family:

```
DES-7210(config)# router bgp 65000

DES-7210(config-router)# address-family ipv4 unicast

DES-7210(config-router-af)# maximum-prefix 65535
```

Related commands

Command	Description
clear bgp { *addressfamily* | **all** } *****	Reset the BGP address-family.
show bgp { *addressfamily* | **all** } **summary**	Show the summary of BGP address-family.

Platform description

33.1.40 neighbor activate

Use this command to activate the neighbor or peer group in the current address mode. Use the **no** form of the command to restore it tothe default setting.

neighbor {*peer-address* | *peer-group-name*} **activate**

no neighbor {*peer-address* | *peer-group-name*} **activate**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 address or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Enabled in address-family IPv4 configuration mode

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 configuration mode,

Usage guidelines

You need to set this command in other address-family configuration modes for exchaning routes.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.0.0.1 remote-as 100
DES-7210(config-router)# address-family vpnv4
DES-7210(config-router-af)# neighbor 10.0.0.1 activate
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.41 neighbor advertisement-interval

Use this command to set the time interval to send the BGP route update message. Use the **no** form of the command to restore it to the default setting.

neighbor {*peer-address* | *peer-group-name*} **advertisement-interval** *seconds*

no neighbor {*peer-address* | *peer-group-name*} **advertisement-interval**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
seconds	Time interval to send the route update message in the range of 1 to 600 seconds

Default configuration

IBGP connection: 15seconds
EBGP connection: 30seconds

Command mode

BGP configuration mode.

Usage guidelines

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.0.0.1
advertisement-interval 10
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.42 neighbor allowas-in

Use this command to allow the PE to receive the messages of the same AS number as itself. The **no** form restores the setting to the default value.

neighbor {*peer-address* | *peer-group-name*} **allowas-in number**

no neighbor {*peer-address* | *peer-group-name*} **allowas-in**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	Number of the AS number duplication in the range of 1 to 10, 3 by default.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

A typical application is spoke-hub mode. Execute this command on the PE to enable it to receive and then send the advertised address prefix. For example, configure two VRFs on the PE. One VRF receives the routes of all PEs and advertises them to the CE; the other VRF receives the routes advertised by the CE and advertises them to all PEs.

This command applies to IBGP peers or EBGP peers.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.1.1.1 remote-as 100
DES-7210(config-router)# address-family ipv4 vrf vpn1
```

```
DES-7210(config-router-af)# neighbor 10.1.1.1 allowas-in
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.43 neighbor as-override

Use this command to allow the PE to override the AS number of a site. The **no** form restores the setting to the default value.

neighbor {*peer-address* | *peer-group-name*} **as-override**

no neighbor {*peer-address* | *peer-group-name*} **as-override**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

In general, the BGP will not receive the messages of the same AS number as its AS. This command can override the AS number, so that the BGP can receive the messages of the same AS number.

A typical application is in a VPN where two CEs have the same AS number. Usually the CEs cannot receive the messages from each other. Executing this command on a PE will override the AS number of one CE it connects. As a result, the other CE can receive the peer's route messages.

This command applies only to EBGP peers.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.1.1.1 remote-as 100
```

```
DES-7210(config-router)# address-family ipv4 vrf vpn1
DES-7210(config-router-af)# neighbor 10.1.1.1 as-override
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.44 neighbor default-originate

Use this command to allow the BGP speaker to advertise the default route to the peer (group). The **no** form of the command remove the ocnfiguration.

neighbor {*peer-address* | *peer-group-name*} **default-originate** [**route-map** *map-tag*]

no neighbor {*peer-address* | *peer-group-name*} **default-originate** [**route-map** *map-tag*]

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
map-tag	Name of the route-map of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command requires to redistribute the default route only when the default route exists locally.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command. If you set the command for a member in the peer, this command will overwrite the settings on the peer group.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.1.1.1 remote-as 80
DES-7210(config-router)# neighbor 10.1.1.1
default-originate
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.45 neighbor description

Use this command to set a descriptive sentence for the specified peer (group). The **no** form of the command removes the setting.

neighbor {*peer-address* | *peer-group-name*} **description** *text*

no neighbor {*peer*-address | *peer-group-name*} **description**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
text	Text for describing the peer (group) of up to 80 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command is used to add descriptive characters for the peer (group). This may help remember the features and characteristics of the peer (group).

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.1.1.1 remote-as 80
DES-7210(config-router)# neighbor 10.1.1.1 description xyz.com
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.46 neighbor distribute-list

Use this ocmmand to configure the ACL based on which the routing policy is implemetned to receiving/transmitting routing information from/to the BGP peer. The **no** form of the command removes the ACL configured.

neighbor {*peer-address* | *peer-group-name*} **distribute-list** *access-list-number* {**in** | **out**}

no neighbor {*peer-address* | *peer-group-name*} **distribute-list** *access-list-number* {**in** |**out**}

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
access-list-number	ACL number
in	Specify the ACL for filtering the incoming routes.
out	Specify the ACL for filtering the outgoing routes.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 configuration mode .

Usage guidelines

For the **in** rule or **out** rule, this command cannot exist at the same time with the **neighbor prefix-list** command. That is, only one of them takes effect.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command. If you set the **neighbor distribute-list** command for a member in the peer, this command will overwrite the settings on the peer group.

	You can set different filtering policies in different address-family configuration modes to control routes.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.1.1.1 remote-as 80
DES-7210(config-router)# neighbor 10.1.1.1
distribute-list bgp-filter in
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
ip access-list	Create a standard IP ACL or extended IP ACL.

Platform description

33.1.47 neighbor ebgp-multihop

Use this command to allow the BGP connection established between the EBGP peers that are not directly connected. The **no** form of the command removes the setting.

neighbor {*peer-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*peer-address* | peer-*group-name*} **ebgp-multihop**

Parameter description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
ttl	Maximum hops in the range 1 to 255

Default configuration

The BGP connection is allowed to establish only with the EBGP peer that is directly connected.

If no parameter is used with the "**ebgp-multihop**", the TTL uses 255.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage

To prevent routing loop and dampening, non-default routes that can

guidelines	reach the peer must exist between the EBGP peers where the BGP connection must be established via multiple hops. If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 remote-as 65100
DES-7210(config-router)# neighbor 10.0.0.1 ebgp-multihop
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.48 neighbor filter-list

When this command is set to specify the BGP peer to receive/transmit routing information, the same route filtering is used. The **no** form of the command cancels the filtering.

neighbor {*peer-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}

no neighbor {*peer-address* | peer-*group-name*} **filter-list** *access-list-number* {**in** | **out**}

Parameter description

Parameter	Description
peer address	IP address of the peer, IPv4 address or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
access-list-numbe	ACL number
in	as-path list is applied on the received routing information.
out	as-path list is applied on the distributed routing information.

Default configuration Disabled.

Command mode	BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 configuration mode .
Usage guidelines	If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If the **neighbor filter-list** command is set for a member of the peer, the setting will overwrite the setting for the group. You can set different filter policies in different address-family configuration modes to control routes.

Examples	`DES-7210(config)# ip as-path access-list 1 deny _123_`
	`DES-7210(config)# router bgp 65000`
	`DES-7210(config-router)# neighbor 10.0.0.1 remote-as 65100`
	`DES-7210(config-router)# neighbor 10.0.0.1 filter-list 1 out`

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
ip as-path access-list	Create an AS_PATH list.
match as-path	Match the AS_PATH list.

Platform description

33.1.49 neighbor maximum-prefix

Use this command to limit the number of prefixes received from the specified BGP peer. The **no** form of the command removes the limitation configured.

neighbor {*peer-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

no neighbor {*peer*-address | *peer-group-name*} **maximum-prefix**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
Peer-group-name	Name of the peer group of up to 32 characters
maximum	Upeer limit of the number of the received route

	entries
threshold	Percentage of the maximum when the alarm starts to be generated.
warning-only	Do not determine the BGP connection when the route entries reaches the upeer limit but produce a log entry.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

By default, the BGP connection will be torn down when the received routes exceeds the upeer limit. If you do not hope to tear down the connection, set the "**warning-only**" to control that.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1
maximum-prefix 1000
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.50 neighbor next-hop-self

Use this command to set the next-hop of the route to the local BGP speaker while specifying the routes that the BGP peer redistributes. Use the **no** form of the command to remove the configuration.

neighbor {*peer-address* | *peer-group-name*} **next-hop-self**

no neighbor {*peer-address* | *peer-group-name*} **next-hop-self**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command is mostly used in the non-full-mesh-type network, such as the Frame Relay and X.25, where the BGP speakers within the same subnet cannot completely be accessed mutually.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 next-hop-self
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.51 neighbor password

When the BGP connection with the BGP peer is established, use this command to enable the TCP MD5 authentication and set the password. The **no** form of the command disables MD5 authentication.

neighbor {*peer-address* | *peer-group-name*} **password** [0 | 7]*string*

no neighbor {*peer-address* | *peer-group-name*} **password**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
0	Display the password with encryption.
7	Display the password without encryption.
string	Password for MD5 authentication in the range of up to 80 characters

Default configuration

Disabled.

Command mode

BGP configuration mod, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command will enable the MD5 authentication of the TCP. The BGP peers must have the same password configured; otherwise, the neighbor relationship cannot be established. When this command is set, the local BGP speaker will re-establish the BGP connection with the BGP peer.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

A neighbor has only one password, not one for every address family, no matter in which mode it is configured.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 password
DES-7210
```

.Related commands

Command	Description
router bgp	Enable the BGP protocol
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.52 neighbor peer-group (assigning members)

Use this command to configure the specified peer as the member of the BGP peer group. Use the **no** form of this command to delete the specified BGP peer from the peer group.

neighbor *peer-address* **peer-group** *peer-group-name*

no neighbor *peer-address* **peer-group** *peer-group-name*

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

No peer exists in the peer group.

Command mode

BGP configuration mode.

Usage guidelines

The members of the peer group can inherit all configurations of the peer.

It is allowed to configure an individual member of the peer group to take the place of the universal configuration for the peer group, but such separate configuration does not contain the configuration information that may affect the output update. In other words, every member in the peer group will always inherit the following configurations of the peer group:

remote-as, update-source, **local-as**,**reconnect-interval** ,**times**, **advertisemet-interval**, **default-originate**, **next-hop-self**, **remove-private-as**, **send-community**, **distribute-list out**, **filter-list out**, **prefix-list out**, **route-map out**, **unsuppress-**map, **route-reflector-client**.

Do not place the neighbors in different address families into the same peer group, and also do not place the IBGP and EBGP neighbors in the same peer group.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor Red-Giant peer-group
DES-7210(config-router)# neighbor 10.0.0.1 peer-group Red-Giant
```

Related

Command	Description

commands	**router bgp**	Enable the BGP protocol.
	neighbor remote-as	Configure the BGP peer.
	neighbor peer-group (creating)	Create the BGP peer group.
	show ip bgp peer-group	Show the information of the BGP peer.

Platform description

33.1.53 neighbor peer-group (creating)

Use this command to create the BGP peer group. The **no** form of the command deletes the specified peer group and all its members.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group*-name **peer-group**

Parameter description

Parameter	Description
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

No BGP peer group is created.

Command mode

BGP configuration mode.

Usage guidelines

If multiple BGP peers use the same update policy, those peers can be configured in the same peer group, so as to simplify the configuration and boost operation efficiency.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor Red-Giant peer-group
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

	neighbor peer-group (assigning members)	Configure the specified peer as the member of the BGP peer group.
	show ip bgp peer-group	Show the information of the BGP peer.

Platform description	

33.1.54 neighbor prefix-list

Use this command to implement the routing policy based on the prefix list to receive/transmit routes from/to the BGP peer. The **no** form of the command removes the prefix-list configured.

neighbor {*peer-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}

no neighbor {*peer-address* | *peer-group-name*} **prefix-list** {**in** |**out**}

Parameter description

Parameter	Description
peer address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
prefix-lis-name	Name of the prefix-list of up to 32 characters
in	Apply the prefix list to the received routes.
out	Apply the prefix list to the redistributed routes.

Default configuration	Disabled.
Command mode	BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.
Usage guidelines	For the "**in**" rule or "**out**" rule, this command cannot exist at the same time with the **neighbor distribute-list** command. That is, only one of them takes effect. If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If the **neighbor prefix-list in** command is set for a member of the peer, the setting will overwrite the setting for the group. You can set different filter policies in different address-family

	configuration modes to control routes.

Examples

```
DES-7210(config)# ip prefix-list bgp-filter deny
10.0.0.1/16
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 prefix-list bgp-filter
in
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
ip prefix-list	Create the prefix lists.

Platform description

33.1.55 neighbor remote-as

Use this command to configure the BGP peer (group). The **no** form of the command deletes the configured peer (group).

neighbor {*peer-address* | *peer-group-name*} **remote-as** *as-number*

no neighbor {*peer-address* | *peer-group-name*} **remote-as** *as-number*

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
as-number	BGP peer (group) autonomous system number in the range of 1 to 65535

Default configuration No BGP peer is configured.

Command mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 remote-as 80
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.

Platform description

33.1.56 neighbor remove-private-as

Use this command to delete the private AS number recorded in the AS path attribute in the route sent to the specified EBGP peer. Use the **no** form of the command to remove the configuration.

neighbor {*peer-address* | *peer-group-name*} **remove-private-as**

no neighbor {*peer-address* | *peer-group-name*} **remove-private-as**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command takes effect only on the EBGP peers.

If the AS path contains the private AS number that is the AS number of the EBGP peer to be sent, the AS number is not deleted.

Private AS number range: 64512 - 65535

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1
remove-private-as
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.57 neighbor route-map

Use this command to enable route match for the received/sent routes. You can use the **no** form of the command to disable this function.

neighbor {*peer-address*|*peer-group-name* } **route-map** *map-tag* {**in** | **out**}

no neighbor {*peer-address*|*peer-group*-name } **route-map** *map-tag* {**in | out**}

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
map-tag	Name of the match rule
in	Apply the rule to the incoming routes.
out	Apply the rule to the outgoing routes.

Default configuration

N/A.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode and address-family IPv4 VPNv4 cofiguration mode.

Usage guidelines

This command can be used to filter the incoming and outgoing routes for different neighbors by using different incoming/outgoing rules. This can reach the results of purifying routes and controlling routes.

You can set different filter policies in different address-family configuration modes to control routes.

Examples

```
DES-7210(config-router)# neighbor ip-address route-map map-tag in
```

Related commands

Command	Description
neighbor soft-reconfiguration inbound	Store the routing information sent from the BGP peer.
show ip bgp	Show the BGP route entry.

Platform description

33.1.58 neighbor route-reflector-client

Use this command to configure the local device as the route reflector and specifies its client. The **no** form of the command removes the client configured.

neighbor {*ip-address* | *peer-group-name* } **route-reflector-client**

no neighbor {*ip-address* | *peer-group-name* } **route-reflector-client**

Parameter description

Parameter	Description
ip-address	IP address of the peer
peer-group-name	Name of the peer group of no more than 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

By default, all IBGP speakers in the autonomous system must establish neighbor relationship one another. The BGP speaker does not forward the routes learned from an IBGP peer to the other IBGP peers to avoid route loop.

This command can be used to set route reflector, so that there is no requirement for all IBGP speakers to establish the full neighboring relationship between each other. This will allow the route reflector to forward the learned IBGP route to the other IBGP peers.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1
route-reflector-client
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
bgp cluster-id	Configure the cluster ID of the route reflectors.
bgp client-to-client reflection	Cancel the route reflection between clients

Platform description

33.1.59 neighbor send-community

Use this command to transmit the community attributes to the specified BGP neighbor. Use the **no** form of the command to disable this function.

neighbor {*peer-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

no neighbor {*peer-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

Parameter description

Parameter	Description
peer-addres	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
both	Transmit both standard and extended communities.
standard	Transmit the standard community only.
extended	Transmit the extended community only.

Default configuration Disabled.

Command mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode and address-family IPv4 VPNv4 configuration

	mode.
Usage guidelines	This command transmits the community to the neighbor or neighbor group.
Examples	`DES-7210(config-router)# neighbor 10.1.1.1 send-community both`

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
ip community-list	Create the community list.

Platform description

33.1.60 neighbor shutdown

Use this command to disconenct the BGP connection established with the specified BGP peer. The **no** form of the command reconnects the BGP peer (group).

neighbor {*peer-address* | *peer-group-name*} **shutdown**

no neighbor {*peer-address* | *peer-group-name*} **shutdown**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration	Disabled.
Command mode	BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.
Usage guidelines	This command is used to disconnect the valid connection established with the specified peer (group), and delete all associated routing

information. However, this command still keeps the configuration information of that specified peer (group).

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.0.0.1 shutdown
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
show ip bgp summary	Show the BGP connection status.

Platform description

33.1.61 neighbor soft-reconfiguration inbound

Use this command to sotre the routing information sent from the BGP peer. Use the **no** form of the command to disable them.

neighbor {*peer-address* | *peer-group-name*} **soft-reconfiguration inbound**

no neighbor {*peer-address* | *peer-group-name*} **soft-reconfiguration inbound**

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines	This command restarts the BGP session, and keeps the unchanged routing information sent from the BGP peer (group). Executing this command will consume more memories. If both parties support the route refresh function, this command becomes unnecessary. You may run the **show ip bgp neighbors** command to judge whether the peer can support the route refresh function. If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1
soft-reconfiguration inbound
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
show ip bgp neighbors	Show the information of the BGP peer.
clear ip bgp	Reset the BGP peer session.

Platform description

33.1.62 neighbor soo

Use this command to set the SOO value of the neighbor. Use the **no** form of the command to remove the configuration.

neighbor {*peer-address* | *peer-group-name*} **soo** *soo-value*

no neighbor {*peer-address* | *peer-group-name*} **soo** *soo-value*

Parameter description

Parameter	Description
peer-addres	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
soo-value	SOO value. There are two forms of SOO value:

		as_number:nn: as_number is the public AS number and nn is defined by yourself. ip_address:nn: IP address must be global and nnis defined by yourself.

Default configuration	Disabled.
Command mode	Address-family IPv4 configuration mode
Usage guidelines	In the CE dual-home mode, execute this command to prevent the routes that a CE sends to the PEs from being sent back to the CE.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 remote-as 100
DES-7210(config-router)# address-family ipv4 vrf vpn1
DES-7210(config-router)# neighbor 10.0.0.1 soo 100:100
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
timers bgp	Configure the keepalive and holetime values globally.

Platform description

33.1.63 neighbor timers

In specifying the BGP peer to establish the BGP connection, use this command to set the *keepalive* and *holdtime* time values used for establishing the BGP connection. Use the **no** form of the command to restore it to the default setting.

neighbor [*peer-address* | *peer-group-name*] **timers** *keepalive holdtime*

no neighbor [*peer-address* | *peer-group-name*] **timers** *keepalive holdtime*

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address

peer-group-name	Name of the peer group of up to 32 characters
keepalive	Time interval to send the KEEPALIVE message to the BGP peer. Range: 0-65535 seconds.
holdtime	Time interval to consider the BGP peer alive. Range: 0-65535 seconds.

Default configuration

keepalive: 60 seconds

holdtime: 180 seconds.

Command mode

BGP configuration mode.

Usage guidelines

A reasonable *keepalive* value cannot be greater than one-third of the holdtime value.

If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 80 240
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
timers bgp	Set the *keepalive* and *holdtime* values globally.

Platform description

33.1.64 neighbor unsuppress-map

Use this command to selectively advertise the routing information that has been suppressed with the **aggregate-address** command. Use the **no** form of the command to restore it to the default setting.

neighbor {*peer-address* | *peer-group-name*} **unsuppress-map** *map-tag*

no neighbor {*peer-address* | *peer-group-name*} **unsuppress-map**

Parameter description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
map-tag	Name of the route-map of up to 32 characters

Default configuration

Disabled.

Command mode

BGP configuration mode.

Usage guidelines

This command advertises the specified routes that has been suppressed.

If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1
unsuppress-map unspress-route
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.
aggregate-address	Configure the aggregate address.
route-map	Configuring route-map

Platform description	

33.1.65 neighbor update-source

In specifying the BGP peer to establish the BGP connection, use this command to set the network interface used for establishing the BGP connection. The **no** form of the command automatically matches the optimal local interface.

neighbor {*peer-address* | *peer-group-name*} **update-source** *interface-type interface-index*

no neighbor {*peer-address* | *peer-group*-name} **update-source** *interface-type interface-index*

Parameter description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
interface-type	Interface type
interface-index	Interface index

Default configuration

Use the optimal local interface as the output interface.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

This command enables using the loopback interface to establish the BGP connection with the BGP peer.

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

If the connection is initiated by the opposite, it does not check which interface is used to establish the TCP connection.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 update-source lookback 1
```

Related

Command	Description

commands	**router bgp**	Enable the BGP protocol.
	neighbor remote-as	Configure the BGP peer.

Platform description

33.1.66 neighbor version

Use this command to show the number of the BGP protocol version used by the specific BGP neighbor. The **no** form of the command uses the default version number.

neighbor {*ip-address*|*peer-group-name*} **version** *number*

no neighbor {*ip-address*|*peer-group-name*} **version** *number*

Parameter description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	Version Number. Now only version 4 is supported.

Default configuration The default version number is 4.

Command mode BGP configuration mode.

Usage guidelines When the command is used, the BGP will lose the version negotiation function.

Examples

```
DES-7210(config-router)# neighbor 10.1.1.1 version 4
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform

description

33.1.67 neighbor weight

Use this command to set the weight for the specific neighbor. The **no** form of the command removes the setting.

neighbor {*ip-address*|*peer-group-name*} **weight** *number*

no neighbor {*ip-address*|*peer-group-name*} **weight** *number*

Parameter description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	Weight in the range of 0 to 65535.

Default configuration

No weight is configured for the specific neighbor by default. In this case, the learned neighbor weight is 0 and the locally generated weight is 32768 initially.

Command mode

BGP configuration mode.

Usage guidelines

When the command is used, the routes from the neighbor use this value as the initial weight value. The higher the weight, the higher the priority is.

Executing the **set weight** command in the route map of the neighbor will overwrite this value.

Examples

```
DES-7210(config-router)# neighbor 10.1.1.1 weight 73
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
neighbor remote-as	Configure the BGP peer.

Platform description

33.1.68 network(BGP)

Use this command to configure the network information to be advertised by the local BGP speaker. The **no** form of the command deletes the configured network information.

network *network-number* **mask** *mask* [**route-map** *map-tag*] [**backdoor**]

no network *network-number* **mask** *mask* [**route-map**] [**backdoor**]

Parameter description

Parameter	Description
network-number	Network number
mask	Subnet mask
map-tag	Name of the route-map of up to 32 characters
backdoor	The route is a backdoor route.

Default configuration

The network information is not specified.

Command mode

BGP configuration mode.

Usage guidelines

This command allows injecting the IGP route into the BGP routing table. The network information advertised can be direct route, static route and dynamic route.

The "**route-map**" can be used to modify the network information.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# network 10.0.0.1 mask
255.255.0.0
```

Related commands

Command	Description
router bgp	Enable the BGP protocol.
redistribute	Configure the route redistribution.
Network synchronization	Enalbe network synchronization.

Platform description

33.1.69 network synchronization

Use this command to advertise the network information after the local BGP speaker is synchronized with the local device. The **no** form of the command directly advertises the network information.

network synchronization

no network synchronization

Parameter description	N/A.
Default configuration	Enabled.
Command mode	BGP configuration mode.
Usage guidelines	This command is used to modify the behavior of the network during the process of advertisement. It is not recommended to turn off this switch lest route black hole is caused.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# network synchronization`

Related commands

Command	Description
router bgp	Enable the BGP protocol.
redistribute	Configure the route redistribution.
network(BGP)	Configure the route to be distributed.

Platform description

33.1.70 overflow memory-lack

Use this command to allow the BGP to enter the OVERFLOW state when the memory lacks. Use the **no** form of this command to disable this function.

overflow memory-lack

no overflow memory-lack

Parameter description

Parameter	Description
no	Disallow the BGP to enter the OVERFLOW state when the memory lacks.

Default configuration

Allow the BGP to enter the OVERFLOW state when the memory lacks.

Command mode

BGP configuration mode.

Usage guidelines

In the BGP OVERFLOW state, the newly-learned routes are discarded, which prevents the memory from being increased.

With this function enabled, if the BGP address family is in the OVERFLOW state, the newly-learned routes will be discarded, which may results in the loop in the network. To prevent that from happening and reduce the propability, BGP generates a default route directing to the NULL interface, and the default route will always exist in the OVERFLOW state.

Use the **clear bgp** {addressfamily**|all**} * command to reset the BGP and clear the OVERFLOW state in the BGP address family.

Use the no option to disallow the BGP to enter the OVERFLOW state when the memory lacks, which is possible to lead to the continuous exhausion of the memory resources. When the meory has been exhausted to a certain degree, BGP will break down all neighbors and delete all learned routes.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# no memory-lack overflow
```

Related commands

Command	Description
clear bgp { *addressfamily*|**all** } *****	Reset the BGP address family.
show bgp { *addressfamily*|**all** } **summary**	Show the summary of the BGP address family.

Platform

description

33.1.71 redistribute

Use this is to redistribute routes between the other routing protocol and the BGP. The **no** form of the command disables the function.

redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

no redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

Parameter description

Parameter	Description
protocol-type	The source protocol types for redistributing routes, including connected, static, RIP.
route-map *map-tag*	Specify the route map. No route map is associated with by default.
metric *metric-value*	Set the default metric of the routes to be redistributed, null by default.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

Note that when you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured.

The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.

Examples

```
DES-7210(config-router)# redistribute static route-map static-rmap
DES-7210(config-router)# no redistribute static
route-map static-rmap
DES-7210(config-router)# no redistribute static
```

Related commands

Command	Description
show ip protocol	Show the protocol configuration.

Platform description

33.1.72 redistribute (OSPF)

Use this is to redistribute routes between the OSPF and the BGP. The **no** form of the command disables the function.

redistribute *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [1 | 2] **nssa-external** [1 | 2]]

no redistribute *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [1 | 2] **nssa-external** [1 | 2]]

Parameter description

Parameter	Description
process-id	OSPF process ID to be redistributed
route-map *map-tag*	Specify the route map. No route map is associated with by default.
metric *metric-value*	Set the default metric of the routes to be redistributed, null by default.
match	Match the sub type of OSPF routes.
internal	Match the internal OSPF routes, the default configuration.
external [1 | 2]	Match the external OSPF rotues. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.
nssa- external [1 | 2]	Match the NSSA-external type of OSPF routes. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode.

Usage guidelines

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

Note that when you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured.

The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.

Examples

```
DES-7210(config-router)# redistribute ospf 2 route-map static-rmap
DES-7210(config-router)# no redistribute ospf 4 match external
rotue-map ospf-rmap
DES-7210(config-router)# no redistribute ospf 78
```

Related commands

Command	Description
show ip protocol	Show the protocol configuration.

Platform description

33.1.73 redistribute (ISIS)

Use this is to redistribute routes between the ISIS and the BGP. The **no** form of the command disables the function.

redistribute isis [*isis-tag*] [**route-map** *map-tag*] [**metric** *metric-value*] [**level-1** | **level-1-2** | **level-2**]

no redistribute isis [*isis-tag*] [**route-map** *map-tag*] [**metric** *metric-value*] [**level-1** | **level-1-2** | **level-2**]

Parameter description

Parameter	Description
isis-tag	(Optional)ISIS process ID to be redistributed
route-map *map-tag*	Specify the route map. No route map is associated with by default.
metric *metric-value*	Set the default metric of the routes to be redistributed, null by default.
level-1	Redistribute level-1 ISIS routes.

level-1-2	Redistribute level-1 and level-2 ISIS routes.
level-2	Redistribute level-2 ISIS routes.

Default configuration

Disabled.

Command mode

BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode.

Usage guidelines

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

Note that when you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured.

The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.

Examples

```
DES-7210(config-router)# redistribute isis route-map static-rmap
DES-7210(config-router)# no redistribute isis test route-map
isis-rmap
DES-7210(config-router)# no redistribute isis
```

Related commands

Command	Description
show ip protocol	Show the protocol configuration.

Platform description

33.1.74 router bgp

Use this command to enable the BGP protocol, configure the local autonomous system number and enter the BGP protocol configuration mode. The **no** form of the command disables the BGP protocol.

router bgp *as-number*

no router bgp *as-number*

Parameter description

Parameter	Description
as-number	AS number in the range 1 to 65535

Default configuration Disabled.

Command mode Global configuration mode.

Usage guidelines This command is used to start the BGP protocol.

Examples

```
DES-7210(config)# router bgp 65000
```

Related commands

Command	Description
ip routing	Enable IP routing.
bgp router-id	Set the ID of the device running the BGP protocol
network	Set the network information to be advertised by the local BGP speaker.

Platform description

33.1.75 synchronization

Use this command to enable the synchronization mechanism of the BGP and IGP routing information. The **no** form of the command disables the synchronization mechanism of the BGP and IGP routing information.

synchronization

no synchronization

Parameter description N/A.

Default configuration Disabled.

Command mode	BGP configuration mode.
Usage guidelines	The synchronization between BGP and IGP aims to prevent the possible route black hole. In any of the two cases below, you may cancel the synchronization mechanism to ensure fast convergence of routing information. 1. There is no the route information which pass through this AS (In general, this AS is an end AS). 2. All devices within this AS operate the BGP protocol and the full connection relationship is established among all BGP Speakers (The adjacent relationship is established between any two BGP Speakers).
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# synchronization`

Related commands

Command	Description
router bgp	Enable the BGP protocol.

Platform description

33.1.76 timers bgp

Use this command to adjust the BGP network timer. The **no** form of the command restores the default value.

timers bgp *keepalive holetime*

Parameter description

Parameter	Description
keepalive	Time interval to send the keepalive message to the BGP peer. Range: 0-65535 seconds.
holdtime	Time interval to consider the BGP peer alive. Range: 0-65535 seconds.

Default configuration

keepalive: 60 seconds

holdtime: 180 seconds.

Command mode	BGP configuration mode.
Usage guidelines	A reasonable *keepalive* value cannot be greater than one-third of the holdtime value. If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer. If the BGP peer group is specified, all members of the peer group inherit the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.
Examples	`DES-7210(config)# router bgp 65000` `DES-7210(config-router)# timers bgp 80 240`

Related commands

Command	Description
neighbor timers	Set the *keepalive* and *holdtime* values on the basis of neighbors.

Platform description

33.2 Showing Related Command

33.2.1 show ip bgp

Use this command to show the route information of BGP.

show ip bgp [{*network* | *network-mask*}] [**longer-prefixes**]

Parameter description

Parameter	Description
network	Showing the specific routing information in the routing table
network-mask	Show the routing information included in the specified network.
longer-prefixes	Show the routing information of a route, including the more specific routes included in it.

Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to view the route information of BGP.
Examples	DES-7210# **show ip bgp** Status codes: s suppressed, d damped, h history, * valid, > best, i - internal Origin codes: i - IGP, e - EGP, ? - incomplete Status Network Next Hop Metric LocPrf Path ------ -------- ------- -------- -------- ------------- *> 211.21.21.0/24 110.110.110.10 0 1000 200 300 *> 211.21.23.0/24 110.110.110.10 0 1000 200 300 *> 211.21.25.0/24 110.110.110.10 0 1000 300 *> 211.21.26.0/24 110.110.110.10 0 1000 300 *> 211.21.27.0/24 110.110.110.10 0 1000 200

33.2.2 show ip bgp cidr-only

Use this command to show unclassified routes.

show ip bgp cidr-only

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the unclassified routing information.
Examples	DES-7210# **show ip bgp cidr-only**

Related commands	Command	Description
	bgp dampening	Enable the route dampening function and set the dampening parameters.
	clear ip bgp dampening	Clear the suppressed routes.

33.2.3 show ip bgp community

Use this command to show the BGP routing information matching with the specified community.

show ip bgp community *community-number* [**exact -match**]

Parameter description	Parameter	Description
	community-number	Community number, in the form of AA:NN (autonomous system number/2-byte numeral), or any of the following predefined values: internet, no-export, local-as, no-advertise.
	exact -match	Show the routing information that fully matches the community**.**

Default configuration	N/A.

Command mode	Privileged EXEC mode.

Usage guidelines	This command is used to show the routing information with specified community value.

Examples

```
DES-7210# show ip bgp community local-as 111:12345
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network   Next Hop   Metric      LocPrf    Path
------ --------- ---------   --------  --------  -----------
*>  211.21.21.0/24  110.110.110.10  0     1000   200 300
*>  211.21.23.0/24  110.110.110.10  0     1000   200 300
*>  211.21.25.0/24  110.110.110.10  0     1000   300
*>  211.21.26.0/24  110.110.110.10  0     1000   300
*>  211.21.27.0/24  110.110.110.10  0     1000   200
```

33.2.4 show ip bgp community-list

Use this command to show the BGP routing information that matches the specified community list.

show ip bgp community-list *community-name* [**exact-match**]

Parameter description

Parameter	Description
community-name	Name of the community list
exact-match	Routing information fully matching the community list

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to view the information of the community list.

Examples

```
DES-7210# show ip bgp community-list my_comm
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network    Next Hop    Metric    LocPrf    Path
------ ----------  ----------   --------  --------  -----------
*>  211.21.21.0/24  110.110.110.10  0     1000   200 300
*>  211.21.23.0/24  110.110.110.10  0     1000   200 300
*>  211.21.25.0/24  110.110.110.10  0     1000   300
*>  211.21.26.0/24  110.110.110.10  0     1000   300
*>  211.21.27.0/24  110.110.110.10  0     1000   200
```

Related commands

Command	Description
ip community-list	Define the community list.

33.2.5 show ip bgp dampening dampened-paths

Use this command to show the suppressed path.

show ip bgp dampening dampened-paths

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the dampened path.

Examples

```
DES-7210# show ip bgp dampening dampened-paths
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
status Network          From          Reuse    Path
------ ------------ ------------ -------- --------------
*d    192.168.64.0/24   110.110.110.10  00:21:41 1000 i
*d    202.117.121.0/24  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
*d    202.117.122.0/23  110.110.110.10  00:21:43 1000 ?
```

33.2.6 show ip bgp dampening flap-statistics

Use this command to show the route dampening statistics.

show ip bgp dampening flap-statistics

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.

Usage guidelines	This command is used to show the BGP route dampening statistics.

Examples

```
DES-7210# show ip bgp dampening flap-statistics
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network        From        Flaps  Duration Reuse    Path
------ --------- ---------- ------ -------- -------- ------------
h     192.168.64.0/24   110.110.110.10    2 00:19:17      1000 i
h     201.234.1.0/24    110.110.110.10    2 00:19:17      1000 ?
h     201.234.2.0/23    110.110.110.10    2 00:19:17      1000 ?
h     201.234.2.0/23    110.110.110.10    2 00:19:17      1000 ?
h     201.234.2.0/23    110.110.110.10    2 00:19:17      1000 ?
h     201.234.2.0/23    110.110.110.10    2 00:19:17      1000 ?
```

Related commands	
Platform description	

33.2.7 show ip bgp dampening parameters

Use this command to show the route dampening parameters configured for the BGP.

show ip bgp dampening parameters

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode
Usage guidelines	This command is used to show the route dampening parameters configured for the BGP.

Examples

```
DES-7210(config-router)# bgp dampening 25 10000 10000 200
DES-7210# show ip bgp dampening parameters
```

```
dampening 25 10000 10000 200
Dampening Control Block(s):
Reachability Half-Life time    : 25 min
Reuse penalty                  : 10000
Suppress penalty               : 10000
Max suppress time              : 200 min
Max penalty (ceil)             : 29800000
Min penalty (floor)            : 5000
```

33.2.8 show ip bgp filter-list

Use this command to show the routing information that matches the filtering list.

show ip bgp filter-list *path-list-number*

Parameter description

Parameter	Description
path-list-number	Filtering list identifier

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to show the routing information that matches the filtering list.

Examples

```
DES-7210(config)# ip as-path access-list 5 permit .*
DES-7210# show ip bgp filter-list 5
BGP table version is 1, local device ID is 192.168.88.200
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop          Metric LocPrf Weight Path
*> 192.168.88.0    0.0.0.0                      32768 ?
Total number of prefixes 1
```

33.2.9 show ip bgp inconsistent-as

Use this command to show the route information of inconsistent source AS.

show ip bgp inconsistent-as

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the routing information of inconsistent source AS.
Examples	`DES-7210# show ip bgp inconsistent-as`

33.2.10 show ip bgp neighbors

Use this command to show the related information of BGP neighbor.

show ip bgp neighbors [*neighbor-address*] [**received-routes | routes | advertised-routes**]

Parameter description

Parameter	Description
neighbor-address	IP address of the neighbor
received-routes	Show all routing information received from the peer (including the received routes and rejected routes).
routes	Show all routes that come from the peer and are accepted.
advertised-routes	Show all sent route information.

Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the information of the connection with BGP neighbor.

Examples

```
DES-7210# show ip bgp neighbors
BGP neighbor                : 12.12.12.2
Remote AS                   : 100
Local AS                    : 100
```

```
Neighbor type               : internal
BGP version                 : 4
Remote ID                   : 192.168.4.2
BGP state                   : Established, up for 00:53:30
Min advertisement interval(secs): 15
Configured holdtime         : 90
Configured keepalive        : 30
Hold time                   : 90
keepalive                   : 30
Neighbor capabilities       : ignore
Address family IPv4 Unicast : advertised , recieved
Route refresh               : advertised , recieved
Connections established     : 1
Connections dropped         : 0
Last reset                  : never
Local  host                 : 12.12.12.1  Local port  : 179
Remote host                 : 12.12.12.2  Remote port : 1067
Maximum-Prefix limit        : 4294967295
Threshold for warning       : 0%
Accepted prefixes           : 0
Prefix advertised           : 6
Received messages           : 110
Sent messages               : 116
Received notifications      : 0
Sent notifications          : 0
Route refresh received      : 0
Route refresh sent          : 0
DES-7210# show ip bgp neighbors 15.15.15.5 routes
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network          Next Hop       Metric   LocPrf   Path
------ ----------- ----------- -------- -------- -----------
*>i    58.1.1.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.2.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.3.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.4.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.5.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.6.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.7.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.8.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.9.0/24      58.58.58.8          58     100 800 ?
*>i    58.1.10.0/24     58.58.58.8          58     100 800 ?
*>i    67.1.1.0/24      67.67.67.7          67     100 700 ?
*>i    67.1.2.0/24      67.67.67.7          67     100 700 ?
*>i    67.1.3.0/24      67.67.67.7          67     100 700 ?
*>i    67.1.4.0/24      67.67.67.7          67     100 700 ?
*>i    67.1.5.0/24      67.67.67.7          67     100 700 ?
```

	`*>i 67.1.6.0/24 67.67.67.7 67 100 700 ?`
Related commands	
Platform description	

33.2.11 show ip bgp paths

Use this command to show the path information in the route database.

show ip bgp paths

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the path information in the route database.
Examples	`DES-7210# show ip bgp paths`
Related commands	
Platform description	

33.2.12 show ip bgp quote-regexp

Use this command to show the BGP routing information that the AS path attribute matches the regular expression in the specified double quotation marks.

show ip bgp quote-regexp *regexp*

Parameter description

Parameter	Description
regexp	Regular expression for matching AS path attributes, with comma included.

Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the BGP routing information that the AS path attribute matches the regular expression in the specified double quotation marks. Note that the regular expression shall be enclosed with double quotation marks.
Examples	DES-7210# **show ip bgp quote-regexp** *"_300_"* Status codes: s suppressed, d damped, h history, * valid, > best, i - internal Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Path *> 211.21.21.0/24 110.110.110.10 0 1000 200 300 *> 211.21.23.0/24 110.110.110.10 0 1000 200 300 *> 211.21.25.0/24 110.110.110.10 0 1000 300 *> 211.21.26.0/24 110.110.110.10 0 1000 300
Related commands	
Platform description	

33.2.13 show ip bgp regexp

Use this command to show the BGP routing information that the AS path attribute matches the specified regular expression.

show ip bgp regexp *regexp*

Parameter description

Parameter	Description
regexp	Regular expression for matching AS path attributes

Default configuration	N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the BGP routing information that the AS path attribute matches the specified regular expression.
Examples	DES-7210# **show ip bgp regexp** *_300_* Status codes: s suppressed, d damped, h history, * valid, > best, i - internal Origin codes: i - IGP, e - EGP, ? - incomplete Status Network Next Hop Metric LocPrf Path ------ -------- --------- -------- --------- -------- *> 211.21.21.0/24 110.110.110.10 0 1000 200 300 *> 211.21.23.0/24 110.110.110.10 0 1000 200 300 *> 211.21.25.0/24 110.110.110.10 0 1000 300 *> 211.21.26.0/24 110.110.110.10 0 1000 300

33.2.14 show ip bgp summary

Use this command to show the related information of BGP.

show ip bgp summary

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the related information of BGP.
Examples	DES-7210# **show ip bgp summary** BGP device identifier 192.168.88.200, local AS number 500 BGP table version is 1 1 BGP AS-PATH entries 0 BGP community entries Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 1.1.1.1 4 200 0 0 0 0 0 never Active Total number of neighbors 1

Related	**Command**	**Description**

commands	router bgp	Enabled the BGP protocol

33.2.15 show ip bgp vpnv4

Use this command to show the VPN information of all the VRFs or RDs.

show ip bgp vpnv4 all [*network* | **neighbor** [| **address**] | **summary** | **label**]

show ip bgp vpvn4 vrf *vrf_name* [*network* | **summary** | **label**]

show ip bgp vpvn4 rd *rd_value* [*network* | **neighbor** [| **address**] | **summary** | **label**]

Parameter description

Parameter	Description
network	Network IP address
neighbor	Show neighbor information.
label	Show the label information of routes.
vrf_name	VRF name
rd_value	RD value, for example, 100:1 or 202.118.239.165:1
Summary	Show the route summary information.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to show the VPN information of all VRFs or RDs.

Examples

```
DES-7210# show ip bgp vpnv4 all
Network          Nexthop       Metric       Localprf     Weight
         Path
Route Distinguisher :  100: 2
*>i 192.168.0.1/32  192.168.0.2      0        100
0          10 ?
*>i 192.168.1.0/32  192.168.0.2      0     100
0          ?
Route Distinguisher : 100:30
*>i 192.168.0.1/32  192.168.0.2      0      100
0          10 ?
*> 192.168.4.0  192.168.4.1          0
0         20 ?
* 192.168.4.0    0.0.0.0             0
32768       ?
DES-7210# show ip bgp vpnv4 vrf vpn1 summary
BGP device identifier 192.168.0.4 , local AS num 100
```

```
BGP  VRF vrf1 Route  Distinguisher :  100 :  30
BGP table version is 1
3 BGP AS—PATH entries
0 BGP community entries
Neibhbor   V   AS   MsgRcvd Msgsend  TblVer  IntQ
OutQ   Up/Down  State/PfxRcd
192.168.4.1 4  20    15      16    1       0    0
00:10:36 3
Total number of neighbors 1
```

Related commands

Command	Description
router bgp	Enabled the BGP protocol

33.2.16 show ip community-list

Use this command to show the related information of the community list.

show ip community-list [*community-list-number*|*community-list-name*]

Parameter description

Parameter	Description
community-list-number	Number of the community list
community-list-name	Name of the community list

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to view the related information of the community list.

Examples

```
DES-7210# show ip community-list
Community-list standard local
permit local-AS
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

33.2.17 show ip as-path-access-list

Use this command to show the related information of the AS path ACL.

show ip as-path-access-list {*num*}

Parameter description

Parameter	Description
num	AS path ACL number

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to view the **as-path-access-list** information.

Examples

```
DES-7210# show ip as-path-access-list
AS path access list 30
permit ^30s
```

34 Protocol-independent Configuration Commands

34.1 Configuration Related Commands

34.1.1 distribute-list in

Use **distribute-list in** to control the route update processing in order to filter routes. Use the **no** form of this command to remove the setting.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

Parameter description

Parameter	Description
access-list-number	ACL number. Only the routes permitted in the access list can be received.
prefix *prefix-list-name*	Use the prefix list to filter routes.
gateway *prefix-list-name*	Use the prefix list to filter the sources of the routes.
interface-type interface-number	(Optional) Interface that the distribution list is applied to.

Default configuration

No distribution list is defined.

Command mode

Routing process configuration mode.

Usage

To deny some specified routes, you can configure the route

guidelines	distribution list to process all the received route update messages. This command does not apply to the OSPF routing protocol, because the OSPF receives the link state messages instead of specific routes. If no interface is specified, the route update messages received by all the interfaces will be processed.

Examples

The following example allows Fastethernet 0/0 to receive the routes beginning with 172.16 in RIP.

```
router rip
network 200.168.23.0
distribute-list 10 in fastethernet 0/0
no auto-summary
!
access-list 10 permit 172.16.0.0 0.0.255.255
```

Related commands

Command	Description
access-list	Set the access list.
prefix-list	Set the prefix list.

34.1.2 distribute-list out

Use **distribute-list out** to control the route update for the purpose of route filtering. Use the **no** form of this command to remove the setting.

distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol* | *process-id*]

no distribute-list {[*access-list-number* | *name*] | **prefix** *prefix-list-name*} **out** [*interface* | *protocol* | *process-id*]

Parameter description

Parameter	Description
access-list-number	ACL number. Only the routes permitted in the access list can be transmitted.
prefix *prefix-list-name*	Use the prefix list to filter routes.
interface	(Optional) Interface that the distribution list is applied to.
protocol	(Optional) The routes of the specified routing protocol are redistributed.

Default configuration

None.

Command mode	Routing process configuration mode.
Usage guidelines	If no optional parameter is used in this command, the route update applies to all the interfaces. If the interface option is used, the route update applies to only the interface. If other routing process parameters are used, the routes of the specified routing process are filtered for redistribution. The route update in the OSPF routing process only applies to the external routes of the OSPF AS, and no interface shall be specified.

Examples	The following example advertises 192.168.12.0/24 in RIP.
	`router rip`
	`network 200.4.4.0`
	`network 192.168.12.0`
	`distribute-list 10 out`
	`version 2`
	`!`
	`access-list 10 permit 192.168.12.0`

Related commands

Command	Description
access-list	Define the access list.
prefix-list	Define the prefix list.
redistribute	Redistribute routes.

34.1.3 ip community-list

Use this command to define a community list and control access to it. Use the **no** form of this command to remove the setting.

ip community-list {[**standard | expanded**] *community-list-name* | *community-number* } {**permit** | **deny**} [*community-number*]

no ip community-list {**standard | expanded**} {*community-list-name* | *community-number*}

Parameter description

Parameter	Description
community-list-name	Name of the community list of no more than 32 characters
standard	Set a standard community list numbered in 1 to 99.
expanded	Set an expanded community list numbered over 100.

permit	Permit access to the community list.
deny	Deny access to the community list.
community-number	Community number in the form of AA:NN(AS number/2-byte numerical) in the range of 1 to 255 characters. It may also be one of the following value: Internet: Indicates the Internet community. All paths belong to this community. no-export: Indicates that this path will not be advertised to any EBGP peers. no-advertise:Indicates that this path will not be advertised to any BGP peers. local-as:Indicates that this path will not be advertised to out of the AS. When AS confederation is configured, this path will not be advertised to other ASs or sub-ASs.

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

This command is used to define the community list for BGP.

Examples

```
DES-7210(config)# ip community-list standard 1 deny 100.20.200.20
DES-7210(config)# ip community-list standard 1 permit internet
```

Related commands

Command	Description
match community	Match the community list.

	set community-list delete	Remove the community value of the BGP path according to the community list.
	show ip community-list	Show the community list information.

34.1.4 ip default-network

Use this command to configure the default network globally. Use the **no** form of this command to remove the setting.

ip default-network *network*

no ip default-network *network*

Parameter description	**Parameter**	**Description**
	network	Default network

Default configuration	0.0.0.0/0
Command mode	Global configuration mode.
Usage guidelines	The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network. The default network always starts with an asterisk (“*”), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.

Examples	The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.
	`ip route 192.168.100.0 255.255.255.0 serial 0/1`
	`ip default-network 192.168.100.0`
	The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.
	`ip default-network 200.200.200.0`

Related commands	Command	Description
	show ip route	Show the routing table.

34.1.5 ip prefix-list

Use this command to create a prefix list or add an entry to the prefix list. Use the **no** form of this command to remove the prefix list or an entry.

ip prefix-list *prefix-lis-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

no ip prefix-list *prefix-lis-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

Parameter description

Parameter	Description
prefix-list-name	Name of the prefix list
seq-number	Sequence number of an entry in the range of 1 to 2147483647. When you execute this command to add an entry without a sequence number, the system allocates a default sequence number for the entry. The default sequence number of the first entry is 5. Every subsequential entry withtout a sequence number uses the time of 5 larger than the previous sequence number as the default sequence number.
deny	Deny the route matching the prefix list.
permit	Permit the route matching the prefix list.
ip-prefix	Network address nad mask. Network address can be any valid IP address and the mask length is in the range of 0 to 32.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
maximum-prefix-length	(Optional) Maximum length of the prefix (the ending length) Note: “le” indicates the operation of “less than” and “equivalent to”.

Default configuration	None

Command mode	Global configuration mode.
Usage guidelines	The **ip prefix-list** command configures the prefix list, with the **permit** or **deny** keyword to determine the action in case of matching. You can execute this command to define an exact match, or use “ge” or “ le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of minimum-prefix-length to 32; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “ge” and “le” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, mask length of IP prefix < minimum-prefix-length < maximum-prefix-length <=32.

Examples	The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 201.1.1.0/24.
	`DES-7210# configure terminal`
	`DES-7210(config)# ip prefix-list pre1 permit 201.1.1.0/24`
	`DES-7210(config)# router ospf`
	`DES-7210(config-router)# distribute-list prefix pre1 out rip`
	`DES-7210(config-router)# end`

34.1.6 ip prefix-list description

Use this command to add the description of a prefix list. Use the **no** form of this command to delete the description.

ip prefix-list *prefix-lis-name* **description** *description-text*

no ip prefix-list *prefix-lis-name* **description** *description-text*

Parameter description

Parameter	Description
prefix-lis-name	Name of the prefix list
description-text	Description of the prefix list

Default configuration	No description is added for a prefix list, by default.

Command mode	Global configuration mode

Examples	The example below adds the description for the prefix list:
	`DES-7210# configure terminal`
	`DES-7210(config)# ip prefix-list pre description Deny routes from Net-A`

34.1.7 ip prefix-list sequence-number

Use this command to enable sort funciton for a prefix list. Use the **no** form of this command to disable the sort function.

ip prefix-list sequence-number

no ip prefix-list sequence-number

Parameter description	None
Default configuration	No sequence number is added for a prefix list, by default.
Command mode	Global configuration mode

Examples	The example below adds a sequence number for the prefix list:
	`DES-7210# configure terminal`
	`DES-7210(config)# ip prefix-list pre description deny routes from Net-A`

Related commands

Command	Description
ip prefix-list	Configure the prefix list.

Platform

description	
Version description	

34.1.8 ip route

Use this command to configure a static route. Use the **no** form of this command to remove the prefix list or an entry.

ip route [**vrf** *vrf_name*] *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent]** [**weight** *number*] [**disable** | **enable**]

no ip route [**vrf** *vrf_name*] *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent]** [**weight** *number*] [**disable** | **enable**]

Parameter description

Parameter	Description
vrf-name	Name of the VRF
network	Network address of the destination
net-mask	Mask of the destination
ip-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
distance	(Optional) The management distance of the static route
tag	(Optional) The tag of the static route
permanent	(Optional) Permanent rotue ID
number	(Optional) Weight number of the static route
disable/enable	(Optional) Disablement or enablement ID of the static route

Default configuration	None
Command mode	Global configuration mode.
Usage guidelines	The default management distance of the static route is 1. Setting the management distance allows the learnt dynamic route to overwrite

the static route. setting the management distance of the static route can enable route backup, which is called floating route in this case. For example, the management distance of the OSPF is 110. You can set its management distance to 125. Then the data can switch over the static route when the route running OSPF fails.

You can specify the VRF that the static route belongs to. Otherwise, the static route is added to the default VRF.

The default weight of the static route is 1. To view the static route of non default weight, execute the **show ip route weight** command. The parameter weight is used to enable WCMP. When there are load-balanced routes to the destination, the switch assigns data flows by their weights. The higher the weight of a route is, the more data flows the route carries. WCMP limit is generally 32 for routers. However, WCMP limit varies by switch models for their chipsets support different weights. When the sum of the weights of load balanced routes is beyond this weight limit, the excessive ones will not take effect.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it.

When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, ip route 0.0.0.0 0.0.0.0 Fastethernet 0/0. In this case, the switch may consider that all unknown destination networks are directly connected to the Fastethernet 0/0. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not recommended to set the static route to an Ethernet interface.

Examples

The following example adds a static route to the destination network of 172.16.100.0/24 whose next hop is 192.168.12.1 and management distance is 15.

```
ip route 172.16.199.0 255.255.255.0 192.168.12.1 155
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the destination network of 172.16.100.0/24.

```
ip route 172.16.199.0 255.255.255.0 fastethernet 0/0 192.168.12.1
```

Related commands

34.1.9 ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** form of this command to disable the function.

ip routing

no ip routing

Default configuration	Enabled
Command mode	Global configuration mode.
Usage guidelines	IP routing is not necessary when the switch serves as bridge or VoIP gateway.
Examples	The following example disables IP routing `no ip routing`
Related commands	
Platform description	This command is not supported on Layer 2 devices.

34.1.10 ip static route-limit

Use this command to set the upeer threshold of the static route. Use the **no** form of this command to restore the setting to the default value.

ip static route-limit *number*

no static route-limit *number*

Parameter description

Parameter	Description
number	Upeer threshold of static routes

Default configuration	1000

Command mode	Global configuration mode.
Usage guidelines	The goal is to control the number of static routes. You can view the upeer threshold of the configured non-default static routes with the **show running config** command.
Examples	The following example sets the upeer threshold of the static routes to 900 and then restores the setting to the default value. `ip static route-limit 900`
Related commands	
Platform description	This command is not supported on Layer 2 devices.
Version description	

34.1.11 ipv6 prefix-list

Use this command to create an IPv6 prefix list or add an entry in the prefix list. Use the **no** form of this command to delete an IPv6 prefix list or an entry in the prefix list.

Ipv6 prefix-list *prefix-lis-name***[seq** *seq-number***] { deny | permit}** *ipv6-prefix* **[ge** *minimum-prefix-length***][le** *maximum-prefix- length***]**

no ipv6 prefix-list *prefix-lis-name***[seq** *seq-number***] { deny | permit}** *ipv6-prefix* **[ge** *minimum-prefix- length***][le** *maximum-prefix- length***]**

Parameter description

Parameter	Description
prefix-lis-name	Name of the prefix list

	seq-number	Sequence number of an entry in the prefix list. Its range is 1 to 4294967294. If the sequence number is not specified in this command, the system will allocate a default one for the entry. The default sequence number of the first entry is 5, and that of each subsequent one is the product of adding 5 to the sequence number of the proceeding entry.
	Permit	Permit the access to the matching result.
	deny	Deny the access to the matching result.
	Ipv6-prefix	Network address and its mask. The network address can be any valid IP address. The mask can be 0 to 32 characters.
	minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: "ge" indicates the operation of larger than and equivalent to.
	maximum-prefix- length	(Optional) Maximum length of the prefix (the ending length) Note: "le" indicates the operation of less than and equivalent to.

Default configuration	No prefix list is created.
Command mode	Global configuration mode
Usage guideline	The **ipv6 prefix-list** command configures the prefix list, with the **permit** or **deny** keyword to determine the action in case of matching. You can execute this command to define an exact match, or use “ge” or “ le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of minimum-prefix-length to 32; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length;

	"ge" and "le" indicates the range of minimum-prefix-length to maximum-prefix-length, namely, Ipv6-prefix mask length < minimum-prefix-length < maximum-prefix-length <= 128

Examples	The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 2222::/64.
	`DES-7210# configure terminal`
	`DES-7210(config)# ipv6 prefix-list pre1 permit 2222::64`
	`DES-7210(config)# ipv6 router ospf`
	`DES-7210(config-router)# distribute-list prefix pre out rip`
	`DES-7210(config-router)# end`

34.1.12 ipv6 prefix-list description

Use this command to add the description of an IPv6 prefix list. Use the **no** form of this command to delete the description.

ipv6 prefix-list *prefix-lis-name* **description** *description-text*

no ipv6 prefix-list *prefix-lis-name* **description** *description-text*

Parameter description

Parameter	Description
prefix-lis-name	Name of the ipv6 prefix list
description-text	Description of the ipv6 prefix list

Default configuration

No description is added for an IPv6 prefix list, by default.

Command mode

Global configuration mode

Examples	The example below adds the description for the prefix list:
	`DES-7210# configure terminal`
	`DES-7210(config)# ipv6 prefix-list pre description Deny routes from Net-A`

Related commands	**Command**	**Description**
	ipv6 prefix-list	Configure the IPv6 prefix list.

34.1.13 ipv6 prefix-list sequence-number

Use this command to add a sequence number for an IPv6 prefix list. Use the **no** form of this command to remove the settings.

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Parameter description	None
Default configuration	No sequence number is added for a prefix list, by default.
Command mode	Global configuration mode

Examples	The example below adds a sequence number for the prefix list:
	`DES-7210# configure terminal`
	`DES-7210(config)# ipv6 prefix-list pre description Deny routes from Net-A`

Related commands	**Command**	**Description**
	ipv6 prefix-list	Configure the IPv6 prefix list.

34.1.14 match as-path

Use this command to redistribute the routes of AS_PATH attribute permitted by the access list in the route map configuration mode. Use the **no** form of this command to remove the setting.

match as-path *as-path-acl-list-num* [*as-path-acl-list-num.....*]

no match as-path *as-path-acl-list-num* [*as-path-acl-list-num.....*]

Parameter description

Parameter	Description
as-path-acl-list-num	ACL number, in the range of 1 to 500.
access-list-name	Name of the access list

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

The **match as-path** can be followed by an access list number or name.

One or more **match** or **set** commands can be executed to configure one route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

```
!
route-map ROUTEMAP2IBGP
match as-path 20 30
```

Related commands

Command	Description
match community	Match the community.
match metric	Match the metric.
match origin	Match the source of routes.
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric.
set metric-type	Set the metric type.

34.1.15 match community

Use this command to redistribute the routes matching the Community attribute permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match community {*standard-list-number* | *expanded-list-number* | *community-list-name*} [**exact-match**] [{*standard-list-number* | *expanded-list-number* | *community-list-name*} [**exact-match**] …]

no match community {*standard-list-number* | *expanded-list-number* | *community-list-name*} [**exact-match**] [{*standard-list-number* | *expanded-list-number* | *community-list-name*} [**exact-match**] …]

Parameter description

Parameter	Description
standard-list-number	Number of the standard community list in the range 1 to 99
extended-list-number	Number of the extended community list in the range of 100 to 199
communitys-list-name	Name of the community list in the range of less than 80 characters
exact-match	Match the community list exactly.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

The **match community** can be followed by more than one community list number or name, but the total of community lists and names should not be greater than 6.

Each exact-match applies to only the previous list, not all the lists.

One or more **match** or **set** commands can be executed to configure one route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

```
ip community-list 1 permit 100:2 100:30
route-map set lopref
match community 1 exact-match
set local-preference 20
```

	Command	Description
Related commands	**match as-path**	Match the AS_PATH attribute.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set metric-type	Set the metric type.

34.1.16 match interface

Use **match interface** command to redistribute the routes whose next hop is the specified interface. Use the **no** form of this command to remove the setting.

match interface *interface-type interface-number* [*…interface-type interface-number*]

no match interface *interface-type interface-number* [*…interface-type interface-number*]

	Parameter	Description
Parameter description	*interface-type*	Interface type
	interface-number	Interface number

Default configuration	None.
Command mode	Route map configuration mode.
Usage guidelines	This command can be followed by multiple interfaces. You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example redistributes the RIP route with the next hop of fastethernet 0/0 in the OSPF routing protocol.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match interface fastethernet 0/0
```

Related commands

Command	Description
match ip address	Match the address in the access list.
match ip next-hop	Match the next-hop IP address in the access list.
match ip route-source	Match the source IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

34.1.17 match ip address

Use **match ip address** command to redistribute the routes matching the IP address permitted by the ACL or the prefix list. Use the **no** form of this command to remove the setting.

match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow **match ip address**.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type-1 external type and the default metric being 40.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 200.168.23.0

route-map redrip permit 10
```

	match ip address 10 set metric 40 set metric-type type-1!

	Command	Description
Related commands	**access-list**	Set the access list.
	match interface	Match the next-hop interface of the route.
	match ip next-hop	Match the next-hop address in the access list.
	match ip route-source	Match the route source address in the access list.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.
	set metric-type	Set the metric type.
	set tag	Set the tag.

34.1.18 match ip next-hop

Use **match ip next-hop** command to redistribute the routes whose next-hop IP address matches the access list or the prefix list. Use the **no** form of this command to remove the setting.

match ip next-hop {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip next-hop {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

	Parameter	Description
Parameter description	*access-list-number*	Number of the access list
	access-list-name	Name of the access list
	prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration	None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow **match ip next-hop**.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the next hop address of the RIP route matches the access list 10 or 20, the OSPF allows for redistribution.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 192.168.100.1
access-list 20 permit 172.16.10.1

route-map redrip permit 10
match ip next-hop 10 20
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.

match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

34.1.19 match ip route-source

Use **match ip route-source** command to redistribute the routes whose source IP address matches the access list. Use the **no** form of this command to remove the setting.

match ip route-source {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip route-source {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers may follow **match ip route-source**.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be

	performed.

Examples	In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the source IP address of the RIP route matches the access list 5, the OSPF allows for redistribution.
	`router ospf`
	`redistribute rip subnets route-map redrip`
	`network 192.168.12.0 0.0.0.255 area 0`
	
	`access-list 5 permit 192.168.100.1`
	
	`route-map redrip permit 10`
	`match ip route-source`

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

34.1.20 match ipv6 address

Use this command to redistribute the network routes permitted in the IPv6 access list or the IPv6 prfix list. Use the **no** form of this command to delete the setting.

match ipv6 address { *access-list-name*] | **prefix-list** *prefix-list-name* }

no match ipv6 address

Parameter description

Parameter	Description
access-list-name	Name of the access list.
prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration	None
Command mode	Route map configuration mode
Usage guideline	You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.
	The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type 1 external type and the default metric being 40.
	`ipv6 router ospf`
	`redistribute rip subnets route-map redrip`
	`ipv6 access-list v6acl`
	`10 permit ipv6 2620::64 any`
	
	`route-map redrip permit 10`
	`match ipv6 address v6acl`
	`set metric 30`

	Command	Description
Related commands	**ipv6 access-list**	Set the IPV6 access list.
	match interface	Match the next-hop interface of the route.
	match ipv6 next-hop	Match the next-hop address in the IPv6 access list.
	match ipvr route-source	Match the route source address in the IPv6 access list.
	match metric	Match the route metric.
	match route-type	Match the route type.
	match tag	Match the route tag.
	set metric	Set the metric for route redistribution.
	set metric-type	Set the type for route redistribution.
	set tag	Set the tag for route redistribution.

34.1.21 match ipv6 next-hop

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 next-hop { *access-list-name*] | **prefix-list** *prefix-list-name*}

no match ipv6 next hop

	Parameter	Description
Parameter description	*access-list-name*	Name of the IPv6 access list.
	prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type 1 external type and the default metric being 40.

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 2620::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 30
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.

	match ipv6 address	Match the IP address in the IPv6 access list.
	match ipv6 route-source	Match the route source address in the IPv6 access list.
	match metric	Match the route metric.
	match route-type	Match the route type.
	match tag	Match the route tag.
	set metric	Set the metric for route redistribution.
	set metric-type	Set the type for route redistribution.
	set tag	Set the tag for route redistribution.

34.1.22 match ipv6 route-source

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 route-source { *access-list-name*] | **prefix-list** *prefix-list-name* }

no match ipv6 route-source

	Parameter	**Description**
Parameter description	*access-list-name*	Name of the IPv6 access list.
	prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type 1 external type and the default metric being 40.

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 5200::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 50
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPv6 access list.
match ipv6 next-hop	Match the next hop in the IPv6 access list.

match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

34.1.23 match length

Use this command to implement the policy-based routing based on the IP packet length in the route map configuration mode. The **no** form of Use this command to remove the setting.

match length *min-length max-length*

no match length *min-length max-length*

Parameter description

Parameter	Description
min-length	Minimum length of the IP packet
max-length	Maximum length of the IP packet

Default configuration None

Command mode Route map configuration mode

Usage guideline

Policy-based routing is a packet forwarding mechanism that is more flexible than the routing based on the destination network. After the policy-based routing is used, the device will decide how to process the packets needed to route according to the route map, which decides the next-hop device of the packets.

To apply the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

To route interactive traffic and mass traffic respectively, use the packet size based policy-based routing.

Examples

In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic with packet size smaller than 500 bytes through fastethernet 1/0 interface.

```
interface fastethernet 1/0
ip policy route-map smallpak

route-map smallpak permit 10
match length 0 500
set interface fastethernet 0/0
```

Related commands

Command	Description
route-map	Define the route map
match ip address	Match the address in the access list
set default interface	Set the default packet output interface.
set interface	Set the packet output interface
set ip default next-hop	Set the default next hop of the packets.
set ip next-hop	Set the next-hop IP address of the packets

	set ip precedence	Set the priority of the packets.

34.1.24 match metric

Use **match metric** command to redistribute the routes of the specified metric. Use the **no** form of this command to remove the setting.

match metric *metric*

no match metric *metric*

Parameter description

Parameter	Description
metric	Route metric, in the range 0 to 4294967295

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes of metric 10.

```
router ospf 1
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match metric 10
```

Related

Command	Description

commands	**access-list**	Set the access list.
	match ip address	Match the IP address.
	match interface	Match the interface.
	match ip next-hop	Match the next-hop IP address.
	match ip route-source	Match the source IP address.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.
	set metric-type	Set the metric type.
	set tag	Set the tag.

34.1.25 match origin

Use this command to redistribute the routes whose source IP address is permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match origin {egp | igp | incomplete}

no match origin {egp | igp | incomplete}

	Parameter	Description
Parameter description	**egp**	Redistribute the routes from the remote EGP.
	igp	Redistribute the routes from the local IGP.
	incomplete	Redistribute the routes from an imcomplete type.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	Use this command to set the origin of the routes to be redistributed. Only one origin can be set.

Examples

```
route-map MY_MAP 10 permit
match origin egp
set community 109

route-map MAP20 20 permit
match origin incomplete
set community no-export
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set origin	Set the source.

34.1.26 match route-type

Use this command to redistribute the network routes of the specified type. Use the **no** form of this command to delete the setting.

match route-type {**local | internal** | **external** [**type-1** | **type-2**] | **level-1 | level-2**}

no match route-type {**local | internal** | **external** [**type-1** | **type-2**] | **level-1 | level-2**}

Parameter description

Parameter	Description
local	Resdistribute the local rotues.
internal	Redistribute the routes in the OSPF routing domain.
external	Redistribute the routes out of the BGP or OSPF routing domain.
type-1 | **type-2**	Redistribute the OSPF type-1 or type-2 routes.

level-1 | level-2	Redistribute the ISIS level-1 or level-2 routes.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the RIP routing protocol redistributes only the internal routes in the OSPF routing domain.

```
router rip
redistribute ospf route-map redrip
network 192.168.12.0

route-map redrip permit 10
match route-type internal
!
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.

match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the access list.
set tag	Match the IP address.

34.1.27 match tag

Use this command to redistribute the network routes with the specified tag. Use the **no** form of this command to delete the setting.

match tag *tag* […*tag*]

no match tag *tag* […*tag*]

Parameter description

Parameter	Description
tag	Route tag

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Multiple tags may follow the **match tag** command.

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the RIP routing protocol redistributes only the routes with tag 50 and 80 in the OSPF routing domain.

```
router rip
redistribute ospf 100 route-map redrip
network 192.168.12.0

route-map redrip permit 10
match tag 50 80
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the next-hop IP interface.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match ip next-hop	Match the next-hop IP address.
match route-type	Match the route type.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

34.1.28 maximum-paths

Use this command to specify the number of equivalent routes. The **no** form of this command is used to restore the setting to the default value.

maximum-paths *number*

no maximum-paths *number*

Parameter description

Parameter	Description
number	Number of equivalent routes in the range of 1 to 32

Default configuration

32 for routers. For switches, it depends on switch models.

Command mode

Route map configuration mode.

Usage guidelines

With this command executed, the number of routes for load balancing is no more than the specified number of equivalent routes. You can view the number of equivalent routes with the **show running config** command.

Examples

The following example sets the number of equivalent routes to 10 and then restore it to the default value.

```
maximum-paths 10
no maximum-paths 10
```

34.1.29 route-map

Use **route-map** to enter the route map configuration mode and define a route map. Use the **no** form of this command to remove the setting.

route-map *route-map-name* [**permit** | **deny**] [*sequence-number*]

no route-map *route-map-name* [**permit** | **deny**] [*sequence-number*]

Parameter description

Parameter	Description
route-map-name	Name of the route map. The **redistribute** command references the route map according to its name. Multiple routing policies can be

		defined in a route map, and each policy corresponds to one sequence number.
	permit	(Optional) If the **permit** keyword is defined and the rule defined by **match** is met, The **set** command controls the redistributed routes. For policy-based routing, the **set** command controls the packet forwarding, and exits the route map operation. If the **permit** keyword is defined but the rule defined by **match** is not met, the system performs the routing policy of the second route map till the **set** command is executed finally.
	deny	(Optional) If the **deny** keyword is defined and the rule defined by **match** is met, no operation will be performed. Neither route redistribution nor policy-based routing is supported in the route map. The system exits the route map operation. If the **deny** keyword is defined but the rule defined by **match** is not met, the system performs the routing policy of the second route map till the **set** command is executed finally.
	sequence-number	Sequence number of the route map. The policy with a lower sequence number is preferred, so it's noted when setting the sequence number.

Default configuration	None.
Command mode	Global configuration mode.
Usage guidelines	At present, the DES-7200 software primarily uses the route map for route redistribution and policy-based routing.

1. Route redistribution control

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

When configuring route maps, pay attention to the following when using the sequence number of a route map:

1) When you create the first route map policy, if *sequence-number* is not specified, it is 10 by default;
2) If only one route map policy exists and *sequence-number* is not specified, no new route map policy will be created, and the existing route map policy will be accessed for configuration;

If more than one route map policy is available, the sequence number of each policy shall be specified; otherwise an error message will be displayed.

2. policy-based routing

Policy-based routing refers to a routing mechanism based on user defined policies. Compared with traditional destination IP address-based routing, policy-based routing offers a flexibility for routing based on source IP address, length and port of IP packets. Policy-based routing can apply to the IP packets received on an interface or the IP packets sent from the local device.

Policy-based routing utilizes route map to define routing and forwarding policy. The **match** command defines packet filtering rule and the **set** command defines the action for the packets matching the filtering rules. The **match** command used includes **match ip address** and **match length**; the **set** command includes **set ip tos**, **set ip precedence**, **set ip dscp**, **set ip [default] nexthop**, **set ip next-hop verify-availability**, **set [default] interface**.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes with the hop count of 4. In the OSPF route domain, the route type is the external route type-1, the default metric

is 40 and the tag is 40.

```
!
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
!
route-map redrip permit 10
 match metric 4
 set metric 40
 set metric-type type-1
 set tag 40
```

Related commands

Command	Description
redistribute	Redistribute the routes.

34.1.30 set aggregator as

Use this command to specify the AS_PATH attribute for the aggregator of the routes that match the rule in the route map configuration mode. Excute the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set aggregator as *as-number ip addr*

no set aggregator as [*as-number ip addr*]

Parameter description

Parameter	Description
as-number	AS number of the aggregator
ip_address	IP address of the aggregator

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the AS_PATH attribute for the matched routes in the BGP routing domain. Only one parameter is allowed to set at a time.

Examples

```
route-map set-as-path
match as-path 1
set aggregator as 3 2.2.2.2
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the route metric.
match origin	Match the route source.
set community	Set the COMMUNITY attribute.
set metric	Set the metric.
set metric-type	Set the type.

34.1.31 set as-path prepend

Use this command to specify the AS_PATH attribute for the routes that match the rule in the route map configuration mode. Excute the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set as-path prepend *as-number*

no set as-path prepend [*as-number*]

Parameter description

Parameter	Description
as-number	AS number of the AS_PATH attribute to be configured

Default configuration

None

Command mode

Route map configuration mode

Usage guideline	Use this command to configure the AS_PATH attribute for the matched routes.

Examples	`route-map set-as-path`
	`match as-path 1`
	`set as-path prepend 100 101 102`

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the route metric.
match origin	Match the route source.
set community	Set the COMMUNITY attribute.
set metric	Set the metric.
set metric-type	Set the type.

34.1.32 set comm-list delete

Use this command to delete the COMMUNITY_LIST attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set comm-list *community-list-number* | *community-list-name* **delete**

no comm-list *community-list-number* | *community-list-name* **delete**

Parameter description

Parameter	Description
community-list-number	Number of the community list
community-list-name	Name of the community list

Default configuration	None

Command mode	Route map configuration mode
Usage guideline	Use this command to set the community list for the matched routes that will be deleted in the course of routing.

Examples

```
router bgp 100
neighbor 172.16.233.33 remote-as 120
neighbor 172.16.233.33 route-map ROUTEMAPIN in
neighbor 172.16.233.33 route-map ROUTEMAPOUT out

ip community-list 500 permit 100:10
ip community-list 500 permit 100:20

ip community-list 120 deny 100:50
ip community-list 120 permit 100:.*

route-map ROUTEMAPIN permit 10
set comm-list 500 delete
!
route-map ROUTEMAPOUT permit 10
set comm-list 120 delete
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute value.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set local-preference	Set the local priority of the route to be redistributed.
set metric-type	Set the metric type.

34.1.33 set community

Use this command to specify the community for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set community {*community-number*[community-number…] [**additive | none**}

no set community {*community-number*[community-number…] [**additive | none**}

Parameter description

Parameter	Description
community-number	Community number in the form of AA:NN or a large numeral. In addition, it can be well-known community attributes like **internet**, **local-AS**, **no-export** and **no-advertise**.
additive	Increase on the original COMMUNITY attribute.
none	Set the community attribute as blank.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the community attribute for the matched route.

Examples

```
route-map SET_COMMUNITY 10 permit
match as-path 1
set community 109:10

route-map SET_COMMUNITY 20 permit
match as-path 2
set community no-export
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.

match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set origin	Set the source.
set metric-type	Set the metric type.

34.1.34 set dampening

Use this command to specify the dampening parameters for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Parameter description

Parameter	Description
half-life	Half dampening life for the reachable or unreachable route in the range of 1 to 45 minutes, 15 minutes by default
reuse	When the route penalty is lower than this value, the route suppression is released. It is in the range 1 to 20000, 750 by default
suppress	When the route penalty is higher than this value, the route is suppressed. It is in the range 1 to 20000, 2000 by default
max-suppress-time	Maximum duration a route can be suppressed in the range 1 to 20000 minutes, 4* half-life by default.

Default configuration None

Command mode Route map configuration mode

Usage guideline	Use this command to set the dampening parameter for the matched routes.

Examples

```
route-map tag
match as path 10
set dampening 30 1500 10000 120

router bgp 100
neighbor 172.16.233.52 route-map tag in
```

Related commands

Command	Description
match as-path	Match the AS_PATH value.
match community	Match the community.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of the route to be redistributed.

34.1.35 set default interface

Use this command to specify the default interface for forwarding the packets whose route matches the rule but without an egress in the route map configuration mode. Use the **no** form of this command to remove the setting.

set default interface *interface-type interface-number* [*…interface-type interface-number*]

no set default interface *interface-type interface-number* [*…interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.

Default	None

Command mode	Route map configuration mode

Usage guideline

Multiple interfaces may follow the **set default interface** command.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the device will determine how to process the packets to be routed according to the route map, which determines the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

If the first defined interface becomes **down**, the interface set by the second **set** command will be attempted. A route-map policy may contain multiple **set** operations.

Examples

In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic whose packet size is less than 500 bytes and the route is not defined through fastEthernet 1/0 interface.

```
interface serial 1/0
ip policy route-map smallpak

route-map smallpak permit 10
match length 0 500
set default interface fastethernet 1/0
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
match length	Match the packet length.

set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop of the packets.
set ip next-hop	Set the next-hop IP address of the packets.
set ip precedence	Set the priority of the packets.

34.1.36 set extcommunity

Use this command to specify the extended COMMUNITY attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set extcommunity {**rt** *extend-community-value* | **soo** *extend-community-value*}

no set extcommunity {**rt** | **soo** }

Parameter description

Parameter	Description
rt	Specify the extended community value in the form of RT.
soo	Specify the extended community value in the form of SOO.
extend-community-value	Extended community value.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the extended community attribute for the matched route.

Examples

```
access-list 2 permit 192.168.78.0 255.255.255.0
route-map MAP NAME permit 10
match ip-address 2
set extcommunity rt 100:2
```

Related commands	**Command**	**Description**
	match as-path	Match the AS_PATH value
	match community	Match the community.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set metric-type	Set the metric type.

34.1.37 set interface

Use this command to specify the interface for forwarding the packets matching the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set interface *interface-type interface-number* [*…interface-type interface-number*]

no set interface *interface-type interface-number* [*…interface-type interface-number*]

Parameter description	**Parameter**	**Description**
	interface-type	Interface type.
	interface-number	Interface ID

Default	None
Command mode	Route map configuration mode
Usage guideline	Multiple interfaces may follow the **set interface** command. Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the device will determine how to process the packets to be routed according to the route map, which determines the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

If the first defined interface becomes **down**, the interface set by the second **set** command will be attempted. A route-map policy may contain multiple **set** operations.

If the interface is set as null 0, the packets will be discarded.

Examples

In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic whose packet size is less than 500 bytes through fastethernet 0/0 interface.

```
interface serial 1/0
ip policy route-map smallpak

route-map smallpak permit 10
match length 0 500
set interface fastethernet 0/0
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
match length	Match the packet length.
set default interface	Set the default outgoing interface when there is no route in the routing table.
set ip default next-hop	Set the default next hop of the packets when there is no route in the routing table.
set ip next-hop	Set the next-hop IP address of the packets.
set ip precedence	Set the priority of the packets.

34.1.38 set ip default next-hop

Use this command to specify the default next-hop IP address for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip default next-hop *ip-address* [*weight*] […*ip-address*[*weight*]]

no set ip default next-hop *ip-address* [weight] […*ip-address*[*weight*]]

Parameter description

Parameter	Description
ip-address	IP address of the next hop.
weight	Weight of the next hop.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline	This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight inputted. Up to 32 IP addresses may follow the set ip default next-hop command. If a weight follows ip address, up to 4 next hop IP addresses can be configured. Note: If a weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In this mode, the weight of those next hop IP addresses whose weight is not configured is 1 by default. Differences between set ip next-hop and set ip default next-hop: After the set ip next-hop command is configured, the policy-based routing takes precedence over the routing table; while after the set ip default next-hop command is configured, the routing table takes precedence over the policy-based routing. Use this command to customize a default route for a specified user. If the software fails to find the forwarding route, the packet will be forwarded to the nexthop set with this command. To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded through the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy. A route-map policy may contain multiple **set** operations.

Examples	The following example forwards the packets from two different nodes through different routes.
	For the messages received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding route, they are forwarded to device 6.6.6.6. For the messages received from 2.2.2.2, if the software cannot find the forwarding route, they are forwarded to device 7.7.7.7. The other messages will be discarded if the software cannot find the forwarding route.
	`access-list 1 permit ip 1.1.1.1 0.0.0.0`
	`access-list 2 permit ip 2.2.2.2 0.0.0.0`
	
	`interface async 1`

```
ip policy route-map equal-access

route-map equal-access permit 10
match ip address 1
set ip default next-hop 6.6.6.6
route-map equal-access permit 20
match ip address 2
set ip default next-hop 7.7.7.7
route-map equal-access permit 30
set default interface null0
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

34.1.39 set ip dscp

Use this command to specify the DSCP value for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip dscp *dscp-value*

no set ip dscp

Parameter description

Parameter	Description
dscp-value	DSCP value

Default configuration

None

Command mode	Route map configuration mode
Usage guideline	
Examples	

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

34.1.40 set ip next-hop

Use this command to specify the next-hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop *ip-address* [weight] […*ip-address* [*weight*]]

no set ip next-hop *ip-address* [weight] […*ip-address*[*weight*]]

Parameter description

Parameter	Description
ip-address	IP address of the next hop.
weight	Weight of the next hop.

Default configuration	None

Command mode	Route map configuration mode
Usage guideline	This command supports two operation modes: **WCMP** load balancing mode and **non-WCMP** load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user. Multiple IP addresses may follow **set ip next-hop** and the number of addresses should be less than 32. If **weight** follows **ip address**, up to 4 next hop addresses can be configured. Note: If **weight** follows any **next-hop**, the operation mode of this command will be automatically switched to the **WCMP** load balancing mode. In the WCMP load balancing mode, for the **nexthop address** without configuring the corresponding **weight**, the **weight** is 1 by default. This command can be used to set different routes for the traffic that meets different **match** rule. If multiple IP addresses are configured, they can be used in turn. Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. After the policy-based routing is used, the device will decide how to process the packets that need be routed according to the route map, which decides the next-hop device of the packets. To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy. A route-map policy may contain multiple **set** operations.
Examples	The following example enables policy-based routing on serial 1/0. When the interface receives the packets from

10.0.0.0/8, they will be sent to 192.168.100.1; when the interface receives the packets from 172.16.0.0/16, they will be sent to 172.16.100.1; all other packets will be discarded.

```
interface serial 1/0
ip policy route-map load-balance

access-list 10 permit 10.0.0.0 0.255.255.255
access-list 20 permit 172.16.0.0 0.0.255.255

route-map load-balance permit 10
 match ip address 10
 set ip next-hop 192.168.100.1

route-map load-balance permit 20
match ip address 20
set ip next-hop 172.16.100.1

route-map load-balance permit 30
set interface Null0
```

Related commands

Command	Description
Route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

34.1.41 set ip next-hop verify-availability

Use this command to verify the availability of the next hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop verify-availability *ip-address* **track** *track-object-num*

no set ip next-hop verify-availability

Parameter description

Parameter	Description
ip-address	IP address of the next hop
Track-object-num	Number of the object to be tracked

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

None

Examples

The following example enables policy-based routing on serial 1/0. When the interface receives the packets from 10.0.0.0/8, they will be sent to 192.168.100.1; when the interface receives the packets from 172.16.0.0/16, they will be sent to 172.16.100.1; all other packets will be discarded.

```
interface serial 1/0
ip policy route-map load-balance

access-list 10 permit 10.0.0.0 0.255.255.255
access-list 20 permit 172.16.0.0 0.0.255.255

route-map load-balance permit 10
 match ip address 10
 set ip next-hop 192.168.100.1

route-map load-balance permit 20
match ip address 20
set ip next-hop 172.16.100.1

route-map load-balance permit 30
set interface Null0
```

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

34.1.42 set ip precedence

Use this command to set the precedence of the IP head of the packet matching the rule in the route map configuratio mode. Use the **no** form of this command to remove the configured precedence setting.

set ip precedence {*<0-7>* | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

no set ip precedence {*<0-7>* | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

Default configuration N/A

Command mode Route map configuration mode

Usage guideline With different precedence values for the IP packet head configured, the IP packets matching the PBR routing are sent accoding to the different precedence values.

Multiple **set ip precedence** commands can be executed in the route map configuration rule, but only the last one takes effect, and the precedence will be specified for the head of the IP packet matiched the PBR.

Examples The following example sets the precedence of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:

```
DES-7210(config)#access-list 1 permit 192.168.217.68
0.0.0.0
DES-7210(config)#route-map name
DES-7210(config-route-map)#match ip address 1
DES-7210(config-route-map)#set ip precedence 4
DES-7210(config)#interface FastEthernet 0/0
DES-7210(config-if)#ip policy route-map name
```

Related commands

Command	Description
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip tos	Set the tos for the IP packet head.

34.1.43 set ip tos

Use this command to set the tos of the IP head of the packet matching the rule in the route map configuratio mode. Use the **no** form of this command to remove the configured tos setting.

set ip tos {*<0-15>* | *max-reliability* | *max-throughput* | *min-delay* | *min-monetary-cost* | *normal* }

no set ip tos {*<0-15>* | *max-reliability* | *max-throughput* | *min-delay* | *min-monetary-cost* | *normal* }

Default configuration	N/A
Command mode	Route map configuration mode
Usage guideline	With different TOS values for the IP packet head configured, the IP packets matching the PBR routing are transmitted with different service qualities. The TOS value will be specified for the head of the IP packet matiched the PBR.

Examples	The following example sets the TOS value of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:
	`DES-7210(config)#access-list 1 permit 192.168.217.68 0.0.0.0`
	`DES-7210(config)#route-map name`
	`DES-7210(config-route-map)#match ip address 1`
	`DES-7210(config-route-map)#set ip tos 4`
	`DES-7210(config)#interface FastEthernet 0/0`
	`DES-7210(config-if)#ip policy route-map name`

Related commands

Command	Description
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.

match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip precedence	Set the precedence for the IP packet head.

34.1.44 set level

Use this command to set the level of the area where the routes matching the rule are redistributed in the route map configuration command. Use the **no** form of this command to remove the setting.

set level {level 1| level 2 | level 1-2 | stub-area | backbone}

no set level

Default configuration	None

Command mode	Route map configuration mode

Examples

In the example below, the OSPF routing protocol redistributes the RIP protocol to the backbone area.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
set level backbone
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.

match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

34.1.45 set local-preference

Use this command to set the **LOCAL_PREFERENCE** value for the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting. **set local-preference** *number*

no set local-preference

Parameter description	**Parameter**	**Description**
	number	Local priority metric ranging 1 to 4294967295

Default configuration	None
Command mode	Route map configuration mode
Usage guideline	Use this command to set the local preference for the matched routes. Only one local preference can be set.

Examples

```
route-map SET_PREF permit 10
match as-path 1
set local-preference 6800

route-map SET_PREF permit 20
match as-path 2
set local-preference 50
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

34.1.46 set metric

Use **set metric** to set the metric for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric [+ *metric-value* | **-** *metric-value* | *metric-value*]

no set metric

Parameter description

Parameter	Description
+	Increase based on the metric of the original route
-	Decrease based on the metric of the original route
metric-value	Metric for the route to be redistributed

Default configuration

The default metric for route redistribution varies with the routing protocol.

Command mode

Route map configuration mode

Usage guideline

You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attentions should be paid to the upeer and lower limits of the routing protocols when you execute the **set metric**, **+ metric** or **– metric** commands. When the RIP protocol redistributes the routes of other protocols, the range of the metric after increase or decrease is 1 to 16.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more **match** or **set** commands can be executed to configure a route map. If the **match** command is not used, all the routes will be matched. If the **set** command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes and sets the default metric to 40.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0


route-map redrip permit 10
set metric 40
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.

match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

34.1.47 set metric-type

Use **set metric-type** to set the type of the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric-type *type*

no set metric-type

Parameter description

Parameter	Description
type	Type of the routes to be redistributed. At present, you can set the type of the routes that the OSPF protocol redistributes. type-1: Type-1 external route; type-2: Type-2 external route.

Default configuration

Type-2

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands

can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the type as type-1.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
set metric-type type-1
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set tag	Set the tag.

34.1.48 set next-hop

Use this command to specify the next-hop IP address for the routes that match the rule. Use the **no** form of this command to remove the setting. This command is only used to configure routing policies.

set next-hop *ip-address*

no set next-hop *ip-address*

Parameter description

Parameter	Description
ip-address	IP address of the next hop.

Default configuration	None
Command mode	Route map configuration mode
Usage guideline	You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The following example enables the OSPF routing protocol to redistribute the RIP route and sets the next-hop to 192.168.1.2.
	`route-map redrip permit 10`
	`match ip address 1`
	`set next-hop 192.168.1.2`

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.

	set tag	Set the tag.

34.1.49 set origin

Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set origin {egp | igp | incomplete}

no set origin {egp | igp | incomplete}

Parameter description	**Parameter**	**Description**
	egp	Redistribute the routes from the remote EGP.
	igp	Redistribute the routes from the local IGP.
	Incomplete	Redistribute the routes from an unknown device.

Default configuration	None
Command mode	Route map configuration mode
Usage guideline	Use this command to set the source of the routes to be matched. Only one route source attribute can be set.

Examples	`route-map SET_ORIGIN 10 permit`
	`match as-path 1`
	`set origin igp`
	`route-map SET_ORIGIN 20 permit`
	`match as-path 2`
	`set origin egp`

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of redistributed routes.

34.1.50 set originator-id

Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set originator-id *ip-addr*

no originator-id [*ip-addr*]

Parameter description

Parameter	Description
ip-addr	IP address of the originator.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the source of the routes to be matched.

Examples

```
route-map SET_ORIGIN 10 permit
match as-path 1
set originator-id 5.5.5.5
route-map SET_ORIGIN 20 permit
match as-path 2
set originator-id 5.5.5.6
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of redistributed routes.

34.1.51 set tag

Use this command to set the tag for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set tag *tag*

no set tag

Parameter description

Parameter	Description
tag	Tag of the route to be redistributed

Default configuration

The original routing tag remains unchanged.

Command mode

Route map configuration mode

Usage guideline	This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the tag as 100.

```
router ospf 1
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0
route-map redrip permit 10
set tag 100
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.

34.1.52 set weight

Use this command to set the weight for the BGP routes matching filtering rules. Use the **no** form of this command to remove the setting.

set weight *number*

no set weight

Parameter description

Parameter	Description
number	Weight in the range of 0 to 65535

Default configuration	None
Command mode	Route map configuration mode
Usage guideline	This command can only be used modify the weight of a BGP route. By default, the weight of the route learned from a neighbor is the one configured with the **neighbor weight** command. The weight of the locally generated route is fixed 32768.

Examples	The following example sets the weight for the BGP route learned from the neighbor 1.1.1.1 at the inbound direction to 100.
	`router bgp 1`
	`neighbor 1.1.1.1 route-map nei-rmap-in in`
	`route-map nei-rmap-in permit 10`
	`set weight 100`

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match community	Match the route community.
match metric	Match the route metric.
match origin	Match the source.
set community	Set community of the redistributed route.
set metric	Set the metric of the redistributed route.
set metric type	Set the metric type of the redistributed route.

34.1.53 ip ref ecmp load-balance source

The hardware forwarding table includes not only ECMP/WCMP route but also load balancing policy. When there is more than one next hop of a route, the hardware can select one of them according to defined policy expressed by HASH(KEY(SIP,[DIP] [TCP/UDP Port] [UDF])).

This expression means that the hardware selects the next hop based on the Hash operation of a keyword. You can define the policy in two ways: Hash algorithm and key. The hardware offers two Hash algorightms-CRC32_Upper and CRC32_Lower. You can select some fields of a packet to form a key. By default, only source IP address is selected. Meanwhile, port number, destionation IP address, and customized value of TCP/UDP packet are available.

ip ref ecmp load-balance {[**crc32_lower** | **crc32_upper**] [**dip**] [**port**] [**udf number**]}

no ip ref ecmp load-balance{[**crc32_lower** | **crc32 upper**] [**dip**] [**port**] [**udf number**]}

Command mode	Global configuration mode
Usage guideline	You can use any combination of DIP, port, and UDF to form a key, and select CRC32_Lower or CRC32_Upper as Hash algorithm. This command can only be used modify the weight of a BGP route. The no form will remove the keywords it carries with as the components of a key from the saved setting. For example, if the system saves the setting of SIP, DIP and Port. After the **no ip ref ecmp route dip port** is executed, only SIP is available for the key. If the no form has the keywords not in the saved settings, the command runs properly.

Examples	The following example sets the Hash algorithm for the load balanced route.
	`DES-7210(config)# ip ref ecmp load-balance crc32_upper`
	The following example sets the keyword for the load balanced route.
	`DES-7210(config)# ip ref ecmp load-balance dip port`

34.2 Show Related Command

34.2.1 show route-map

Use the command to view the configuration of the route map in the privileged mode.

show route-map [*route-map-name*]

Parameter description

Parameter	Description
route-map-name	(Optional) Show the configuration information of the specified the route map.

Default configuration

The configuration information of all the route maps is displayed.

Command mode

Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

If no route map is specified, the configurations of all the route maps will be displayed, otherwise only the configuration of the specified route map is displayed.

Examples

```
DES-7210# show route-map
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
```

Field	Description
route-map	Name of the route map.
Permit	The route map contains the **permit** keyword.
sequence 10	Sequence number of the route map.
Match clauses	Set the matching rule. Whether to perform the **set** operation depends on the **permit** or **deny** keyword in the route map.
Set clauses	Setsthe operation when the rule is matched.

34.2.2 show ip community-list

Use **show ip community-list** command to view the community list.

show ip community-list [*community-list-number* | *community-list-name*]

Parameter description

Parameter	Description
community-list-number	Number of the community list.
community-list-name	Name of the community list.

Default configuration

None

Command mode

Privileged EXEC mode

Usage guidelines

This command shows the information on the community list.

Examples

```
DES-7210# show ip community-list
Community-list standard local
permit local-AS
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

34.2.3 show ip prefix-list

Use **show ip prefix-list** to view the prefix list or the entries.

show ip prefix-list [*prefix-name* [**seq** *seq-num* | *ip-prefix*]]

Parameter description

Parameter	Description
prefix-name	Name of the prefix list.

Default configuration

The configuration information of all the prefix lists is displayed by default.

Command mode

Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines	If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
DES-7210# show ip prefix-list
ip prefix-list name : test
seq pre: 2 entries
    seq 5 permit 192.168.564.0/24
    seq 10 permit 192.2.2.0/24
```

34.2.4 show ip route

Use the command to view the configuration of the IP routing table.

show ip route [[**vrf** *vrf_name*] [*network* [*mask*] | **count** | **protocol** [*process-id*] | **weight**]]

Parameter description

Parameter	Description
vrf *vrf_name*	(Optional) Show the route information of the VRF.
network	(Optional) Show the route information to the network.
mask	(Optional)Show the route information to the network of this mask.
count	(Optional)Show the number of existent routes.
protocol	(Optional) Show the route information of specific protocol.
process-id	(Optional) Routing protocol process ID.
weight	(Optional) Show the route information of non deault weight.

Default configuration	All routes are displayed by default.
Command mode	Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.
Usage guidelines	This command can show route information flexibly.

Examples

```
DES-7210# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN
1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
```

Field	Description
O	Source routing protocol, which ma C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route ia: IS-IS area internal route
20.0.0.0/8	Network address and mask destination network
[1/0]	Manage metric
Via 20.0.0.1	Next hop IP address.
VLAN 1	Forwarding interface of next hop

```
DES-7210# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
*192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF,
extern 2
```

Field	Description
Routing Descriptor Blocks	Next hop IP address, source, upd forwarding interface, source protocol and type of route informa

```
DES-7210# show ip route count
--------- route info ----------
the num of active route: 5

DES-7210# show ip route weight
------------[distance/metric/weight]-----------
S    23.0.0.0/8 [1/0/2] via 192.1.1.20
S    172.0.0.0/16 [1/0/4] via 192.0.0.1
```

34.2.5 show ipv6 prefix-list

Use this command to show the information about the IPv6 prefix list or its entries.

show ipv6 prefix-list [prefix-name]

Parameter description

Parameter	Description
prefix-name	Name of the IPv6 prefix list.

Default configuration

The configuration information of all the IPv6 prefix lists is displayed.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, route protocol configuration mode, route map configuration mode

Usage guideline

If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
DES-7210# show ipv6 prefix-list
Ipv6 prefix-list p6 : 2 entries
permit 13::/20
```

34.2.6 show ip ref

Use the command to view the statistics of RFE, including number of routes, number of adjacent devices, number of load balancing tables, and number of weighted nodes.

show ip ref

Command mode Privileged mode

Usage guidelines This command shows the route information of the REF.

Examples

```
DES-7210# show ip ref
-----------statistic information-----------:
current    routes: 5
alloc weight_nodes: 5
alloc  bal_tables: 0
alloc   adj_nodes: 5
alloc     res_adj: 0
----------------------------------------:
```

Field	Description
routes	Number of routes in the REF table
weight_nodes	Number of weighted nodes
bal_tables	Number of load balance tables r the route map.
adj_nodes	Number of adjacent nodes
res_adj	Number of resolved nodes

35 PBR Configuration Commands

35.1 Configuration Related Commands

35.1.1 ip policy route-map

Use this command to enable the policy-based routing on an interface in the interface configuration mode. The **no** format of this command disables the function.

ip policy route-map *route-map*

no ip policy route-map

Parameter description	**Parameter**	**Description**
	route-map	Name of the route map

Default	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	The policy-based routing must be applied on the specified interface. That interface performs only the policy-based routing for the received packets, while the packets sent by the interface will be forwarded normally according to the routing table. To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy. Due to the function restriction, when using the policy-based routing

on the switch, the route map will have a restriction used by policy-based routing: the configured ACL must be a type of numerical value in stead of name-configured ACL. There is no this restriction on the device.

Note that up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Examples

In the example below, when the fast Ethernet interface FE0 receives datagram, if the source address of the datagram is 10.0.0.1, it sets the next-hop as 196.168.4.6; if the source address is 20.0.0.1, it sets the next-hop as 196.168.5.6; otherwise, otherwise, the general forwarding will be performed.

```
access-list 1 permit 10.0.0.1
access-list 2 permit 20.0.0.1
route-map lab1 permit 10
match ip address 1
set ip next-hop 196.168.4.6
exit
route-map lab1 permit 20
match ip address 2
set ip next-hop 196.168.5.6
exit
interface FastEthernet 0/0
ip policy route-map lab1
exit
```

Related commands

Command	Description
access-list	Define the access list rule.
route-map	Define the route map.
set ip next-hop	Set the next hop of the policy-based routing.
set ip default next-hop	Set the default next hop of the policy-based routing.
set ip dscp	Set the DSCP of the IP packet.
match ip address	Set the IP address.
match length	Match the packet length.

Note: For the commands on route-map, refer to *Protccol Independent Commands*.

35.1.2 ip policy

Use this command to set the policy applied for the **set ip nexthop** command in the global configuration mode. The **no** form restores the forwarding mode of policy-based routing.

ip policy {**load-balance|redundance**}

no ip policy

Parameter description

Parameter	Description
load-balance | redundance	Specify the policy: load balancing or redundant backup.

Default Redundant backup is adopted by default.

Command mode Global configuration mode.

Usage guidelines When you configure the **set ip next-hop** command in the sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first hop of the policy-based routing can be parsed. When the load balancing is set, multiple hops of the policy-based routing can be parsed. The WCMP can be set up to four next hops, and the ECMP can be set up to 32 next hops. The parsed next hop refers to the learned next hop of ARP message.

Examples

In the example below, there are multiple next hops configured in the route map. After the redundant backup is set in the global configuration mode, only the first next hop among the sub-route map of the policy-based routing applied on the EF0 takes effect and performs forwarding.

```
access-list 1 permit 10.0.0.1
access-list 2 permit 20.0.0.1
route-map lab1 permit 10
match ip address 1
set ip next-hop 196.168.4.6
set ip next-hop 196.168.4.7
set ip next-hop 196.168.4.8
exit
route-map lab1 permit 20
match ip address 2
set ip next-hop 196.168.5.6
set ip next-hop 196.168.5.7
set ip next-hop 196.168.5.8
exit
interface FastEthernet 0/0
ip policy route-map lab1
exit
ip policy redundance
```

36 IPv6 Configuration Commands

36.1 Configuration Related Commands

The IPv6 configuration includes following related commands:

- **ping ipv6**
- **ipv6 address**
- **ipv6 enable**
- **ipv6 hop-limit**
- **ipv6 neighbor**
- **ipv6 source-route**
- **ipv6 route**
- **ipv6 ns-linklocal-src**
- **ipv6 nd ns-interval**
- **ipv6 nd reachable-time**
- **ipv6 nd prefix**
- **ipv6 nd ra-lifetime**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-hoplimit**
- **ipv6 nd ra-mtu**
- **ipv6 nd managed-config-flag**
- **ipv6 nd dad attempts**
- **ipv6 nd suppress-ra**
- **ipv6 redirects**
- **clear ipv6 neighbors**
- **tunnel destination**
- **tunnel mode ipv6ip**
- **tunnel source**
- **tunnel ttl**

36.1.1 ping ipv6

Use this command to diagnose the connectivity of the IPv6 network.

ping ipv6 [*ipv6-address*]

Parameter description

Parameter	Description
ipv6-address	Destination IP address to be diagnosed.

Command mode

Privileged mode.

Usage guidelines

If no destination address is entered in the command, the user interaction mode is entered, and you can specify the parameters. The following table shows the meanings of symbols returned by the **ping** command:

Signs	Meaning
!	The response to each request sent is received.
.	The response to the request sent is not received within a regulated time.
U	The device has no route to the destination host.
R	Parameter error.
F	No system resource is available.
A	The source IP address of the packet is not selected.
D	The network interface is in the **Down** status, or the IPv6 function is disabled on the the interface (for example, IP address collision is detected).
?	Unknown error

Examples

```
DES-7210# ping ipv6 fec0::1
```

36.1.2 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to delete the configured address.

ipv6 address *ipv6-prefix/prefix-length* [**eui-64**]

no ipv6 address [*ipv6-prefix/prefix-length*] [**eui-64**]

Parameter description

Parameter	Description
ipv6-prefix	IPv6 address in the format defined in RFC2373. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
prefix-length	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of DES-7200 is 0 to 64 or 128 to 128.
eui-64	The generated IPV6 address consists of the address prefix and the 64 bit interface ID.

Command mode

Interface configuration mode

Usage guidelines

When using **eui-64**, the length of the prefix must be 64 bits. When an IPv6 interface is created and the link status is up, the system will automatically generate a local IP address for the interface.

If no deleted address is specified when using **no ipv6 address**, all the manually configured addresses will be deleted.

no ipv6 address *ipv6-prefix*|*prefix-length* **eui-64** can be used to delete the addresses configured with **ipv6 address** *ipv6-prefix*|*prefix-length* **eui-64**.

Examples

```
DES-7210(config-if)# ipv6 address 2001:1::1/64
DES-7210(config-if)# no ipv6 address 2001:1::1/64
DES-7210(config-if)# ipv6 address 2002:1::1/64 eui-64
DES-7210(config-if)# no ipv6 address 2002:1::1/64 eui-64
```

36.1.3 ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the **no** form of this command to disable this function.

ipv6 enable

no ipv6 enable

Default configuration

Disabled.

Command mode	Interface configuration mode.
Usage guidelines	The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface. Note: If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with **no ipv6 enable**.
Examples	DES-7210(config-if)# **ipv6 enable**

Related commands

Command	Description
show ipv6 interface	Show the related information of an interface.

36.1.4 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.

ipv6 hop-limit *value*

no ipv6 hop-limit

Default configuration	The default is 64.
Command mode	Global configuration mode.
Usage guidelines	This command takes effect for the unicast messages only, not for multicast messages.
Examples	DES-7210(config)# **ipv6 hop-limit** *100*

36.1.5 ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to remove the setting.

ipv6 neighbor *ipv6-address interface-id hardware-address*

no ipv6 neighbor ipv6-address interface-id

Parameter description

Parameter	Description
ipv6-address	IPv6 address of the neighbor. It must follow the address format defined in RFC2373.
interface-id	Network interface of the neighbor (including routed Port, L3 AP interface, or SVI interface).
hardware-address	Hardware address of the neighbor. It shall be a 48-bit MAC address in the format of XXXX.XXXX.XXXX, where “X” is a hexadecimal number.

Default configuration

No static neighbor is configured.

Command mode

Global configuration mode.

Usage guidelines

Similar to the ARP command, the static neighbor can only be configured on an IPv6 interface.

If the neighbor to be configured has been learned through NDP and has been stored in the neighbor list, the dynamically generated neighbor will be automatically switched to a static one. The configured static neighbor is always in the **Reachable** status.

Use **clear ipv6 neighbors** to clear all the neighbors dynamically learned through NDP.

Use **show ipv6 neighbors** to view the neighbor information.

Examples

```
DES-7210(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related commands

Command	Description
show ipv6 interface	Show the neighbor information.
clear ipv6 neighbors	Clear the neighbors learned dynamically.

36.1.6 ipv6 source-route

Use this command to forward the IPv6 packet with route header. The **no** form of this command disables the forwarding.

ipv6 source-route

no ipv6 source-route

Parameter description	None.
Default configuration	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Because of the potential security of the header of type 0 route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.
Examples	`DES-7210(config)# no ipv6 source-route`
Related commands	None.

36.1.7 ipv6 route

Use this command to configure an IPv6 static route. Use the **no** form of this command to remove the setting.

ipv6 route *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-id* [*ipv6-address*]}

no ipv6 route *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-id* [*ipv6-address*]}

	Parameter	Description
Parameter description	*ipv6-prefix*	IPV6 network number following the format specified in RFC2373. prefix-length: Length of the IPv6 prefix. "/" must be added in front of the prefix. Note: The prefix length range of the static routes of DES-7200 is 0 to 64 or 128 to 128.

	ipv6-address	Next-hop IP address to the destination address. It shall be in the format defined in RFC2373. The next-hop IP address and the next-hop outgoing interface can be specified at the same time. Note that if the next-hop IP address is a link-local address, the outgoing interface must be specified.
	interface-id	The outgoing interface toward the destination network. If the static route is configured with the outgoing interface but no next-hop address is specified, the destination address will be considered on the link connected with the outgoing interface; that is to say, the static route will be treated as a directly-connected route. Note that if the destination network or next-hop address is a link-local address, the outgoing interface must be specified.

Command mode	Global configuration mode.
Usage guidelines	Note: If the destination IP address or next-hop IP address is a link-local IP address, the outgoing interface must be specified; if the destination address is a link-local IP address, the next-hop must be also a link-local IP address. When configuring a route, the destination IP address and the next-hop IP address shall not be a multicast address. If both the next hop IP address and the outgoing interface are specified, the outgoing interface of the direct route that matches the next hop shall be the same as the configured outgoing interface.
Examples	`DES-7210(config)# ipv6 route 2001::/64 vlan 1 2005::1`

Related commands

Command	Description
show ipv6 route	Show the IPv6 route information.

36.1.8 ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests. When **no ipv6 ns-linklocal-src** is executed, the global IP address will be taken as the source address to send neighbor requests.

ipv6 ns-linklocal-src

no ipv6 ns-linklocal-src

Default configuration	The local address of the link is always used as the source address to send neighbor requests.
Command mode	Global configuration mode.
Usage guidelines	None.
Examples	`DES-7210(config)# no ipv6 ns-linklocal-src`

36.1.9 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the **no** form of this command to restore it to the default setting.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Parameter description

Parameter	Description
milliseconds	Interval for retransmitting NS in the range of 1000 to 429467295 milliseconds

Default configuration	The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000ms(1s).
Command mode	Interface configuration mode.
Usage guidelines	The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.
Examples	`DES-7210(conifg-if)# ipv6 nd ns-interval 2000`

Related

Command	Description

commands	**show ipv6 interface**	Show the interface information**.**

36.1.10 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the **no** form of this command to restore it to the default setting.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Parameter description	**Parameter**	**Description**
	milliseconds	Reachable time for the neighbor in the range 0 to 3600000 milliseconds.

Default configuration	The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30000ms(30s) when the device discovers the neighbor.
Command mode	Interface configuration mode.
Usage guidelines	The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time. The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used. According to RFC4861, the actual time to reach neighbor is not consistent with the configured value, ranging from 0.5*configured value to 1.5*configured value.
Examples	`DES-7210(config-if)# ipv6 nd reachable-time 1000000`

Related commands	**Command**	**Description**
	show ipv6 interface	Show the interface information.

36.1.11 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the **no** form of this command to delete the set prefix or restore it to the default setting.

ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise**]] [**off-link**] [**no-autoconfig**]

no ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** { [**off-link**] [**no-autoconfig**] | [**no-advertise**] }

Parameter description

Parameter	Description
ipv6-prefix	IPv6 network ID following the format defined in RFC2373
prefix-length	Length of the IPv6 prefix. “/” shall be added in front of the prefix
valid-lifetime	Valid lifetime of the RA prefix received by the host
preferred-lifetime	Preferred lifetime of the RA prefix received by the host
at *valid-date preferred-date*	Set the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
infinite	Indicate that the prefix is always valid.
default	Set the default perfix.
no-advertise	The prefix will not be advertised by the device.
off-link	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
no-autoconfig	Indicate that the RA prefix received by the host cannot be used for auto address configuration.

Default configuration

By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:

valid-lifetime: 2592000s (30 days)

preferred-lifetime: 604800s (7 days),

The prefix is advertised and is used for on-link judgment and auto address configuration.

Command mode	Interface configuration mode.
Usage guidelines	This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command. **ipv6 nd prefix default** Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command. **at** *valid-date preferred-date* The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

Examples	The following example adds a prefix for SVI 1.
	`DES-7210(conifg)# interface vlan 1`
	`DES-7210(conifg-if)# ipv6 nd prefix 2001::/64 infinite 2592000`
	The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):
	`DES-7210(conifg)# interface vlan 1`
	`DES-7210(conifg-if)# ipv6 prefix default no-autoconfig`
	If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related commands

Command	Description
show ipv6 interface	Show the RA information of an interface.

36.1.12 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Parameter description	**Parameter**	**Description**
	seconds	Default life time of the device on the interface, 0-9000.

Default configuration	1800s.
Command mode	Interface configuration mode.
Usage guidelines	The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval).
Examples	`DES-7210(conifgf)# interface vlan 1` `DES-7210(conifg-if)# ipv6 nd ra-lifetime 2000`

Related commands	**Command**	**Description**
	show ipv6 interface	Show the interface information.
	ipv6 nd ra-interval	Set the interval of sending the RA.
	ipv6 nd ra-hoplimit	Set the hopcount of the RA.
	ipv6 nd ra-mtu	Set the MTU of the RA.

36.1.13 ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-interval {*seconds* | **min-max** *min_value max_value*}

no ipv6 nd ra-interval

Parameter description	**Parameter**	**Description**
	seconds	Interval of sending the RA message in seconds, 3-1800s.

	min-max	Maximum and minimum interval sending the RA message in seconds
	min_value	Minimum interval sending the RA message in seconds
	max_value	Maximum interval sending the RA message in seconds

Default configuration	200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.
Command mode	Interface configuration mode.
Usage guidelines	If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value. If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

Examples	`DES-7210(conifgf)# interface vlan 1`
	`DES-7210(conifg-if)# ipv6 nd ra-interval 110`
	`DES-7210(config-if)# ipv6 nd ra-interval min-max 110 120`

Related commands	**Command**	**Description**
	show ipv6 interface	Show the interface information.
	ipv6 nd ra-lifetime	Set the lifetime of the device.
	ipv6 nd ra-hoplimit	Set the hopfcount of the RA message.
	ipv6 nd ra-mtu	Set the MTU of the RA message.

36.1.14 ipv6 nd ra-hoplimit

Use this command to set the hopcount of the RA message. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-hoplimit *value*

no ipv6 nd ra-hoplimit

Parameter description	**Parameter**	**Description**
	value	Hopcount

Default configuration	The default value is 64.
Command mode	Interface configuration mode.
Usage guidelines	It is used to set the hopcount of the RA message.
Examples	`DES-7210(config)# interface vlan 1` `DES-7210(config -if)# ipv6 nd ra-hoplimit 110`

Related commands	**Command**	**Description**
	show ipv6 interface	Show the interface information.
	ipv6 nd ra-lifetime	Set the lifetime of the device.
	ipv6 nd ra-interval	Set the interval of sending the RA message.
	ipv6 nd ra-mtu	Set the MTU of the RA message.

36.1.15 ipv6 nd ra-mtu

Use this command to set the MTU of the RA messag. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-mtu *value*

no ipv6 nd ra-mtu

Parameter description	**Parameter**	**Description**
	value	MTU value, 0-4294967295.

Default configuration	IPv6 MTU value of the network interface.

Command mode	Interface configuration mode.
Usage guidelines	If it is specified as 0, the RA will not have the MTU option.
Examples	DES-7210(config)# **interface vlan** *1* DES-7210(config -if)# **ipv6 nd ra-mtu** *1400*

Related commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd ra-lifetime	Set the lifetime of the device.
ipv6 nd ra-interval	Set the interval of sending the RA message.
ipv6 nd ra-hoplimit	Set the hopcount of the RA message.

36.1.16 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag of the RA message. Use the **no** form of this command to remove the setting.

ipv6 nd managed-config-flag

no ipv6 managed-config-flag

Default configuration	None.
Command mode	Interface configuration mode.
Usage guidelines	This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it does not be used.
Examples	DES-7210(config)# **int vlan** *1* DES-7210(config)# **ipv6 nd managed-config-flag**

	Command	Description
Related commands	**show ipv6 interface**	Show the interface information.
	ipv6 nd other-config-flag	Set the flag for obtaining all information except IP address through stateful auto configuration.

36.1.17 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts

	Parameter	Description
Parameter description	*value*	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

Default configuration	1.
Command mode	Interface configuration mode.
Usage guidelines	When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the ”tentative” status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

Examples	DES-7210(conifgf)# **interface vlan** *1* DES-7210(conifg-if)# **ipv6 nd dad attempts** *3*

Related commands	**Command**	**Description**
	show ipv6 interface	Show the interface information.

36.1.18 ipv6 nd suppress-ra

Use this command to disable the interface from sending the RA message. Use the **no** form of this command to enable the function.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Default configuration	The RA message is not sent on the IPv6 interface by default.
Command mode	Interface configuration mode.
Usage guidelines	This command suppresses the sending of the RA message on an interface.
Examples	DES-7210(config)# **interface vlan** *1* DES-7210(config-if)# **ipv6 nd suppress-ra**

Related commands	**Command**	**Description**
	show ipv6 interface	Show the interface information.

36.1.19 ipv6 redirects

Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the **no** form of this command to disable the function.

ipv6 redirects

no ipv6 redirects

Default configuration	The ICMPv6 redirect message is permitted to be sent on the IPV6 interface.

Command mode	Interface configuration mode.
Usage guidelines	The transmission rate of any ICMPv6 error message is limited. By default, it is 100pps.
Examples	DES-7210(config)# **interface vlan** *1* DES-7210(config-if)# **ipv6 redirects**

Related commands

Command	Description
show ipv6 interface	Show the interface information.

36.1.20 clear ipv6 neighbors

Use this command to clear the dynamically learned neighbors.

clrear ipv6 neighbors

Command mode	Privileged mode.
Usage guidelines	This command can be used to clear all the neighbors dynamically learned by the RDP. Note that the static neighbors will not be cleared.
Examples	DES-7210# **clear ipv6 neighbors**

Related commands

Command	Description
ipv6 neighbor	Configure the neighbor.
show ipv6 neighbors	Show the neighbor information.

36.1.21 tunnel mode ipv6ip

Use this command to configure static IPv6 tunnel mode. Use the **no** form of this command to restore it to the default IPv6 tunnel mode.

tunnel mode ipv6ip [**6to4 | isatap**]

no tunnel mode

Parameter description

Parameter	Description
6to4	Configure the tunnel as the auto 6to4 tunnel.
isatap	Configure the tunnel as an auto ISATAP tunnel.

Default configuration

The type of the configured IPv6 tunnel is a tunnel configured manually.

Command mode

Interface configuration mode.

Usage guidelines

After a tunnel is created, it is considered to be manual tunnel by default. You can also use **tunnel mode ipv6ip** without any parameter to set a tunnel to manual tunnel. For an auto tunnel, no destination address is specified.

Examples

The following example configures a 6to4 tunnel.

```
DES-7210(config)# interface tunnel 1
DES-7210(config-if)# tunnel mode ipv6ip 6to4
DES-7210(config-if)# tunnel source vlan 1
```

Related commands

Command	Description
tunnel source	Configure the source address of the tunnel.
tunnel destination	Configure the destination address of a tunnel.
Tunnel ttl	Configure the TTL of the tunnel.

36.1.22 tunnel destination

Use this command to specify the destination address for the tunnel. Use the **no** form of this command to remove the setting.

tunnel destination *ipv4-address*

no tunnel destination

Parameter description

Parameter	Description
ipv4-address	Destination address of the tunnel, namely the IPv4 address in the other side of the tunnle..

Default

The destination address encapsulated by the tunnel is not configured

configuration	by default.
Command mode	Interface configuration mode.
Usage guidelines	A device shall not be configured multiple tunnels with the same encapsulation type, source address and destination address. Note: For auto tunnel (6to4 and isatap), the destination address shall not be configured.

Examples	The following example configures an IPv6 manual tunnel.
	`DES-7210(config)# interface tunnel 1`
	`DES-7210(config-if)# tunnel mode ipv6ip`
	`DES-7210(config-if)# tunnel source vlan 1`
	`DES-7210(config-if)# tunnel destination 192.168.5.1`

Related commands

Command	Description
tunnel source	Configure the source IP address of the tunnel.
tunnel mode	Configure the mode of a tunnel.
Tunnel ttl	Configure the TTL of the tunnel.

36.1.23 tunnel source

Use this command to specify the source IP address for the tunnel. Use the **no** form of this command to remove the setting.

tunnel source {*ipv4-address* | *interface-type interface-number*}

no tunnel source

Parameter description

Parameter	Description
ipv4-address	Source IPv4 address of the tunnel used as the source IP address of the packets to be transmitted through the tunnel.
interface-type interface-number	Interface referenced by the tunnel, which will be used as the source IPv4 address of the packets to be transmitted through the tunnel.

Default configuration	No tunnel source address is configured by default.

Command mode	Interface configuration mode.
Usage guidelines	The source IP address of a tunnel can be a specified IPv4 address or an IPv4 address of an interface. When you configure an auto tunnel (for example, 6to4 and isatap), it is recommended to specify the source address. A device shall not be configured multiple tunnels with the same encapsulation type, source address and destination address. If there are multiple auto tunnels, their source addresses shall be different.

Examples	The following example configures an IPv6 manual tunnel.
	`DES-7210(config)# interface tunnel 1`
	`DES-7210(config-if)# tunnel mode ipv6ip`
	`DES-7210(config-if)# tunnel source vlan 1`
	`DES-7210(config-if)# tunnel destination 192.168.5.1`

Related commands

Command	Description
tunnel mode	Configure the mode of a tunnel.
tunnel destination	Configure the destination address of a tunnel.
Tunnel ttl	Configure the TTL of the tunnel.

36.1.24 tunnel ttl

Use this command to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages. The **no** form of this command restores it to the default.

tunnel ttl *value*

no tunnel ttl

Parameter description

Parameter	Description
value	TTL value

Default configuration	The default value is 128.
Command mode	Interface configuration mode.

Usage guidelines	This command is used to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages.

Examples

```
DES-7210(config)# interface tunnel 1
DES-7210(config-if)# tunnel ttl 64
```

Related commands

Command	Description
tunnel mode	Configure the mode of a tunnel.
tunnel source	Configure the source IP address of the tunnel.
tunnel destination	Configure the destination IP address of a tunnel.

36.2 Show Related Command

36.2.1 show ipv6 route

Use this command to show the IPv6 route information.

show ipv6 route [**static**] [**local**] [**connected**]

Parameter description

Parameter	Description
static	Show the static routes.
local	Show the local routes.
connected	Show the directly-connected routes.

Command mode	Privileged mode.
Usage guidelines	Use this command to view the routing table.

Examples

```
DES-7210# show ipv6 route
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
L    ::1/128
      via ::1, loopback 0
C    fa::/64
      via ::, vlan 1
L    fa::1/128
```

```
     via ::, loopback 0
C    2001::/64
     via ::, vlan 2
L    2001::1/128
     via ::, loopback 0
L    fe80::/10
     via ::1, Null0
C    fe80::/64
     via ::, vlan 1
L    fe80::200:ff:fe00:1/128
     via ::, loopback 0
C    fe80::/64
     via ::, vlan 2
```

Related commands

Command	Description
ipv6 route	Configure a static route.

36.2.2 show ipv6 neighbors

Use this command to show the IPv6 neighbors.

show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]

Parameter description

Parameter	Description
verbose	Show the neighbor details.
interface-id	Show the neighbors of the specified interface.
ipv6-addres	Show the neighbors of the specified IPv6 address.

Command mode

Privileged mode.

Usage guidelines

Show the neighbors on the SVI 1 interface:

```
DES-7210# show ipv6 neighbors vlan 1
IPv6 Address Linklayer Addr   Interface
fa::1        00d0.0000.0002   vlan 1
fe80::200:ff:fe00:2  00d0.0000.0002  vlan 1
```

Show the neighbor details:

```
DES-7210# show ipv6 neighbors verbose
IPv6 Address  Linklayer Addr Interface
2001::1      00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1    00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
```

Field	Meaning
IPv6 Address	IPv6 address of the Neighbor
Linklayer Addr	Link address, namely, MAC address. If it is not available, **incomplete** is displayed.
Interface	Interface the neighbor locates.
State	State of the neighbor: state/H(R) The values of **STATE** are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3). ?: Unknown state. /R—indicate the neighbor is considered as a device /H: The neighbor is a host.

	Age	The reachable time of the neighbor. '-' indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. 'expired' indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.
	Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

Examples

```
DES-7210# show ipv6 neighbors
```

Related commands

Command	Description
ipv6 neighbor	Configure a neighbor.

36.2.3 show ipv6 interface

Use this command to show the IPv6 interface information.

show ipv6 interface [*interface-id*] [**ra-info**]

Parameter description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregateport, or SVI)
ra-info	Show the RA information of the interface.

Command mode

Privileged mode.

Usage guidelines

Use this command to show the address configuration, ND configuration and other information of an IPv6 interface.

Examples

```
DES-7210# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
ff01:1::1
```

```
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND device advertisements live for 1800 seconds
```

The following line is included in the above information: 2001::1, subnet is 2001::/64 [**TENTATIVE**]. The flag bit in the [ ] following the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	Indicate that the address is an anycast address.
TENTATIVE	Indicate that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	Indicate that a duplicate address exists.
DEPRECATED	Indicate that the preferred lifetime of the address expires.
NODAD	Indicate that no DAD is implemented for the address.
AUTOIFID	Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.

```
DES-7210# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
```

```
ND device advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime: 2592000, pltime: 604800, flags:
LA)
```

Description of the fields in **ra-info**:

Field	Meaning
RA timer is stopped (on)	Indicate whether the RA timer is started.
waits	Indicate that the RS is received but the number of the responses is not available.
initcount	Indicate the number of the RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: Indicate the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M | M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O | O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

Field	Meaning
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.

Def	Indicate that the interfaces use the default prefix.
Auto | CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
!Adv	Indicate that the prefix will not be advertised.
vltime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.
L | !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
A | !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

37 OSPFv3 Configuration Commands

37.1 Configuration Related Commands

37.1.1 area default-cost

Use this command to set the cost of the default route for the ABR in the stub area. Use the **no** form of this command to restore it to the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter description

Parameter	Description
area-id	Area ID of the stub area. It can be an integer or an IPv4 prefix.
cost	Cost of the default route of the stub area in the range 1 to 16777214.

Default configuration

By default, the cost of the default route is 1.

Command mode

OSPFv3 configuration mode.

Usage guidelines

This command can only work in the ABR connected to the stub area.

Examples

The following example sets the cost of the default route of stub area 50 to 100.

```
ipv6 router ospf 1
area 50 stub
area 50 default-cost 100
```

	Command	Description
Related commands	**area stub**	Set a stub area.
	show ipv6 ospf area	Show the OSPFv3 area information.

37.1.2 area-range

Use this command to set the range of the converged inter-area addresses. Use the **no** form of this command to remove the setting or restore it to the default setting.

area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise|not-advertise**]

no area *area-id* **range** *ipv6-prefix*/*prefix-length*

	Parameter	Description
Parameter description	*area-id*	ID of the area in which the addresses are converged. It can be an integer or an IPv4 prefix.
	ipv6-prefix/prefix-length	Range of the converged addresses.
	not-advertise	The range of the converged addresses is not advertised. By default, the function is enabled.

Default configuration	No converged inter-area address range is defined.
Command mode	OSPFv3 configuration mode.
Usage guidelines	This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. In this way, the number of the routes in the OSPF AS is reduced. Use **no area** *area-id* to delete the area including all the configuration of the area.

Examples	The following example converges the routes in area 1.
	`ipv6 router ospf 1`
	`area 1 range 2001:abcd:1:2::/64`

	Command	Description
Related		

commands	**discard-route**	Add the discard route generated by the OSPF process to the core routing table.
	summary-prefix	Set the range of the external routes to be converged.

37.1.3 area stub

Use this command to create a stub area or set its attributes. Use the **no** form of this command to restore the stub area to an ordinary area or delete its configuration.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

	Parameter	Description
Parameter description	*area-id*	ID of the stub. It can be an integer or an IPv6 prefix.
	no-summary	This option applies only to the ABR in the stub area, indicating that the ABR only advertises the type 3 LSA indicating the default route to the stub area, not other type 3 LSAs.

Default configuration	None.
Command mode	OSPFv3 configuration mode.
Usage guidelines	Use **no area** *area-id* **stub** command to restore the area as a common area. Use **no area** *area-id* to delete the area including all the configuration of the area. By default, the ABR in the stub area only generates and then advertises the type 3 LSA indicating the default route to the stub area. While the ABR in the NSSA area generates and then advertises the type 3 LSA indicating the default route to the NSSA area only after **no-summary** is used.
Examples	The following example enables the ABR in stub area 10 to advertise the default route to the stub area. `ipv6 router ospf 1`

```
area 10 stub
area 10 stub no-summary
```

Related commands

Command	Description
area default-cost	Set the cost of the default route in the stub area.
show ipv6 ospf area	Show the OSPFv3 area information.

37.1.4 area virtual-link

Use this command to create a virtual link or set its parameters. Use the **no** form of this command to delete the virtual link or restore it to the default setting.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*]

no area *area-id* **virtual-link** *router-id* [**hello-interval**] [**dead-interval**][**retransmit-interval**] [**transmit-delay**] [**instance**]

Parameter description

Parameter	Description
area-id	ID of the area in which the virtual link is located. It can be an integer or an IPv6 prefix.
Router-id	Neighbor router ID of the virtual link.
hello-interval *seconds*	Set the interval to send the hello message on the local virtual link interface in the range from 1 to 65535s. The default value is 10s.
dead-interval *seconds*	Interval for the local interface of the virtual link to wait before considering that the neighbor fails. Its range is 1 to 65535s, and the default value is four times the value of **hello-interval**.
retransmit-interval *seconds*	Specify the interval for the local interface of the virtual link to retransmit LSA. The range is from 1 to 65535s, and the default value is 5s.
transmit-delay *seconds*	Specify the delay for the local interface of the virtual link to wait before sending LSA. The range is from 1 to 65535s, the default value is 1s.
instnace *instance-id*	Specify the instance corresponding to the virtual like.

Default configuration	No virtual link is defined.
Command mode	OSPFv3 configuration mode.
Usage guidelines	In the OSPF AS, all the areas must be connected with the backbone area to ensure that they can learn the routes of the whole OSPF AS. If an area cannot be directly connected with the backbone area, it can connect it through a virtual link. Note: ■ The virtual link shall not be in the stub or NSSA area. ■ **hello-interval**, **dead-interval** and **instance** shall be configured consistently on both sides of the virtual link, otherwise neighboring relationship cannot be set up between the virtual neighbors. ■ Use **no area** *area-id* to delete the area including all the configuration of the area.

Examples	The following example configures a virtual link.
	`ipv6 router ospf 1`
	`area 1 virtual-link 192.1.1.1`

Related commands

Command	Description
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.
show ipv6 ospf virtual-links	Show the OSPFv3 virtual link information.

37.1.5 auto-cost

The metric of the OSPF protocol is the interface-based bandwidth. Use this command to enable the bandwidth-based interface metric calculation or modify the reference bandwidth. Use the **no** form of this command to disable the bandwidth-based interface metric calculation or restore it to the default reference bandwidth.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter description

Parameter	Description
reference-bandwidth *ref-bw*	Specify the reference bandwidth In the range 1 to 4294967 Mbps. The default value is 100Mbps.

Default configuration

The interface metric is calculated based on the reference bandwidth, which is 100Mbps.

Command mode

OSPFv3 configuration mode.

Usage guidelines

Use **no auto-cost reference-bandwidth** to restore it to the default reference bandwidth.

You can use **ipv6 ospf cost** in the interface configuration mode to set the cost of the specified interface, and it takes precedence over the metric calculated based on the reference bandwidth.

Examples

The following example changes the reference bandwidth to 10M.

```
ipv6 router ospf 1
auto-cost reference-bandwidth 5
```

Related commands

Command	Description
ipv6 ospf cost	Set the cost of the interface.
show ipv6 ospf	Show the OSPFv3 routing process information.

37.1.6 clear ipv6 ospf process

Use this command to clear and restart the OSPF process.

clear ipv6 ospf {**process** | *process-id*]

Parameter description

Parameter	Description
process-id	OSPF process ID ranging from 1 to 65535

Command mode

Privileged mode.

Usage guidelines

In normal case, it is not necessary to use this command.

Examples	The example below restarts the OSPF process.
	`en`
	`clear ipv6 ospf process`

37.1.7 default-information originate

Use this command to generate a default route to the OSPF routing domain in the routing process mode. The **no** form of this command disables the default route.

default-information originate [always] [metric *metric***] [metric-type** *type***] [route-map** *map-name***]**

no default-information originate [always] [metric] [metric-type] [route-map *map-name***]**

Parameter settings

Parameter	Description
always	(Optional) Generate the default route unconditionally, no matter whether the default route exists locally or not.
metric *metric*	(Optional) Initial metric value of the default route, 1 by default
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different routers; type 2, the same metric sees on different routers. External route of type 1 is more trustworthy than that of type 2. By default, it is type 2.
route-map *map-name*	Associated route-map name, no associated route-map by default

Default	None
Command mode	Routing process configuration mode
Usage guideline	When the **redistribute** or **default-information** command is executed, the OSPF-enabled router automatically turns into the autonomous system border router (ASBR). But the ASBR cannot generate default route automatically or advertise it to all the routers in the OSPF routing domain. The ASBR generates default routes by default. It is required to configure with the **default-information**

originate routing process configuration command.

If the **always** parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route exists or not. However, the local router does not show the default route. To make sure whether the default route is generated, execute **show ipv6 ospf database** to observe the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. The execution of the **show ipv6 route** command on the OSPF neighbor will display the default route.

The metric of the external default route can be defined only with the **default-information originate** command instead of the **default-metric** command.

There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, type 1 takes precedence over type 2. As a result, the **show ipv6 route** command shows only the type 1 route.

The routers in the stub area cannot generate external default routes.

Examples

The configuration example below generates a default route.

```
default-information originate always
```

Related commands

Command	Description
redistribute	Redistribute routes.
show ipv6 ospf	Show the OSPFv3 route information.
show ipv6 ospf database	Show OSPFv3 link state database

37.1.8 default-metric

Use this command to set the default metric for the routes to be redistributed. Use the **no** form of this command to restore it to the default setting.

default-metric *metric-value*

no default-metric

Parameter description

Parameter	Description
metric-value	Default metric for the routes to be redistributed. Its range is 1 to 16777214, and the default value is 20.

Default configuration

20.

Command mode

OSPFv3 configuration mode.

Usage guidelines

This command can be used with **redistribute** together to set the default metric for the routes to be redistributed. But this command does not appliy to two types of routes:

1. The default route generated with **default-information originate**;
2. The redistributed direct route, which always uses 20 as the default metric value.

Examples

The following example sets the default metric for the routes to be redistributed to 10.

```
default-metric 10
```

Related commands

Command	Description
redistribute	Redistribute the routes.
show ipv6 ospf	Show the OSPFv3 routing process information.

37.1.9 ipv6 ospf area

Use this command to enable the interface to participate in the OSPFv3 routing process. Use the **no** form of this command to disable this function.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

Parameter description

Parameter	Description
process-id	OSPF process ID.
area *area-id*	OSPFv3 area in which the interface participates in. It can be an integer or an IPv6 prefix.

	instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to enable the interface to participate in the OSPFv3 routing process. If **ipv6 router ospf** is not used to start the OSPFv3 routing process, it will be automatically started after this command is used.

Use **no ipv6 ospf area** to disable the specified interface from participating in the OSPFv3 routing process.

Use **no ipv6 router ospf** to disable all the interfaces from participating in the OSPFv3 routing process.

Only the routers with the same instance ID can establish neighbor relationship one another.

After this command is configured, all the prefix information on the interface will be used in the operation of the OSPFv3.

Examples

The following example starts the **OSPFv3** process on **int fastethernet 0/0** for the specified area of the specified instance.

```
int fastethernet 0/0
ipv6 ospf 1 area 2 instance 2
```

Related commands

Command	Description
ipv6 ospf prefix-filter	Set the prefix information not to be advertised on the interface.
ipv6 router ospf	Start the OSPFv3 routing process.
passive-interface	Set the passive interface.
show ipv6 ospf interface	Show the OSPFv3 interface information.

37.1.10 ipv6 ospf cost

Use this command to set the cost of the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf cost *cost*[**instance** *instance-id*]

no ipv6 ospf cost[**instance** *instance-id*]

Parameter description

Parameter	Description
Cost	Cost of the interface. Its range is 1 to 65535, and the default value is 10.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration

10.

Command mode

Interface configuration mode.

Usage guidelines

By default, the cost of the interface is automatically calculated based on the bandwidth of the interface.

You can also use this command to modify the cost of the interface, and it takes precedence over the metric value based on the reference bandwidth.

Examples

The following example sets the cost of the interface to 1:

```
ipv6 ospf cost 1
```

Related commands

Command	Description
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

37.1.11 ipv6 ospf dead-interval

Use this command to set the interval for the interface to consider that the neighbor fails. If the interface does not receive the hello message from the neighbor, it considers that the neighbor fails. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter description

Parameter	Description
seconds	Interval of the neighbor fails. Its range is 1 to 65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration

Four times the value of **ip ospf hello-interval**.

Command mode

Interface configuration mode.

Usage guidelines

The dead time of neighbors shall be the same. Otherwise they cannot establish normal adjacency.

By default, the dead interval is four times the hello interval. If the hello interval changes, the dead interval changes accordingly.

It's not recommended to modify the parameters directly. If needed, note that:

1. The dead interval shall be larger than the hello interval sent by the neighbor.
2. The same dead interval shall be set for the neighbors.

Examples

The following example sets the dead interval of the local interface to 60s.

```
ipv6 ospf dead-interval 60
```

Related commands

Command	Description
ipv6 ospf hello-interval	Set the interval for the interface to send the Hello message.
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface

37.1.12 ipv6 ospf hello-interval

Use this command to set the interval for the interface to send the Hello message. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameter description

Parameter	Description
seconds	Interval for sending the Hello message. Its range is 1-65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration

10 seconds.

Command mode

Interface configuration mode.

Usage guidelines

The same hello interval must be set for the neighbors, otherwise they cannot establish normal adjacency.

Examples

The following example sets the interval for the interface to send the Hello message to 20s.

```
ipv6 ospf hello-interval 20
```

Related commands

Command	Description
ipv6 ospf dead-interval	Set the interval for the interface to consider that the neighbor fails.
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

37.1.13 ipv6 ospf neighbor

Use this command to set the OSPFv3 neighbor manually. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [**poll-interval** <0-4294967295> | **priority** <0-255>]] [**instance** *instance-id*]

no ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [**poll-interval** <0-4294967295> | **priority** <0-255>]] [**instance** *instance-id*]

Parameter description	**Parameter**	**Description**
	cost <*1-65535*>	(Optional) Configure the cost to each neighbor in point-to-multipoint network. It is not defined by default, where the cost configured on the interface will be used. Only the point-to-multipoint type network supports this option.
	poll-interval <*0-4294967295*>	(Optional) Interval to poll the neighbors (in seconds), 120 s by default. Only the non-broadcast (NBMA) type network supports this option.
	priority <*0-255*>	(Optional) Configure the priority of non-broadcast network neighbors, 0 by default. Only the non-broadcast (NBMA) type network supports this option.
	instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Command mode	Interface configuration mode.
Usage guidelines	You can set relevant parameters for the neighbors depending on the actual network type.

37.1.14 ipv6 ospf network

Use this command to set the network type of the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf network {**broadcast | non-broadcast** | **point-to-point | point-to-multipoint** [**non-broadcast**]} [**instance** *instance-id*]

no ipv6 ospf network [**broadcast | non-broadcast** | **point-to-point | point-to-multipoint** [**non-broadcast**]] [**instance** *instance-id*]

Parameter description	**Parameter**	**Description**
	broadcast	Specify the broadcast network type.
	non-broadcast	Specify the non-broadcast network type.
	point-to-point	Specify the point-to-point network type.
	point-to-multipoint	Specify the point-to-multipoint network type.

	point-to-multipoint non-broadcast	Specify the point-to-multipoint non-broadcast network type.
	instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration	Broadcast network type.
Command mode	Interface configuration mode.
Usage guidelines	You can set the network type of the interface according to the actual link type and the topology.
Examples	The following example sets the network type of the interface that participates in the OSPFv3 to point-to-point. `ipv6 ospf network point-to-point`

Related commands	**Command**	**Description**
	ipv6 ospf priority	Set the interface priority.
	show ipv6 ospf interface	Show the OSPFv3 interface information.
	instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

37.1.15 ipv6 ospf priority

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

ipv6 ospf priority *number-value* [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameter description	**Parameter**	**Description**
	number-value	The priority of the interface. Its range is 0 to 255, and the default value is 1.
	instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration	1.
Command mode	Interface configuration mode.
Usage guidelines	In the broadcast type, it is necessary to elect the DR/BDR. In electing the DR/BDR, the device of the highest priority is preferred. If several devices are of the same priority, the one with the largest router-ID is preferred. The device with the priority level of 0 does not participate in the election of DR/BDR. If the DR and BDR are available in the network, modifying the interface priority will not take effect immediately. The interface will participate in the election of the DR/BDR at the next time.
Examples	The following example disables the interface from being elected as the DR/BDR. `ipv6 ospf priority 0`

Related commands

Command	Description
ipv6 ospf network	Set the network type of the interface.
router-id	Set the ID of the router.
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

37.1.16 ipv6 ospf retransmit-interval

Use this command to set the interval for the interface to retransmit the LSA. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf retransmit-interval [**instance** *instance-id*]

Parameter description

Parameter	Description
seconds	Interval for retransmitting the LSA. Its range is 1 to 65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration

5 seconds.

Command mode

Interface configuration mode.

Usage guidelines

To ensure the reliable transmission of routing information, the LSA sent to the neighbor shall be acknowledged by the neighbor. You can use this command to set the interval for waiting for the acknowledgement from the neighbor. If no acknowledgement is received within the specified period, the LSA information will be retransmitted.

Examples

The following example sets the interval for retransmitting the LSA to 10s.

```
ipv6 ospf retransmit-interval 10
```

Related commands

Command	Description
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

37.1.17 ipv6 ospf transmit-delay

Use this command to set the delay for the interface to sending the LSA. Use the **no** form of this command to restore it to the default setting.

ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]

no ipv6 ospf transmit-delay [**instance** *instance-id*]

Parameter description

Parameter	Description
seconds	The delay time for sending LSA.

		Its range is 1 to 65535(s).
	instance *instance-id*	Configure the specific OSPFv3 instance on the interface,0-255.

Default configuration	1 second.
Command mode	Interface configuration mode.
Usage guidelines	Use this command to set the delay for the interface to transmit the LSA.
Examples	The following example sets the delay for the interface to transmit the LSA. `ipv6 ospf transmit-delay 2`

Related commands	**Command**	**Description**
	show ipv6 ospf interface	Show the OSPFv3 interface information.

37.1.18 ipv6 router ospf

Use this command to start OSPFv3 routing process. Use the **no** form of this command to disable the OSPFv3 routing process.

ipv6 router ospf *process-id*

no ipv6 router ospf *process-id*

Parameter description	**Parameter**	**Description**
	process-id	OSPF process number

Default configuration	Disabled.
Command mode	Global configuration mode.

Usage guidelines	After the OSPFv3 process is started, the OSPFv3 configuration mode is entered.
Examples	The following example starts the OSPFv3 process. `ipv6 router ospf 1`

Related commands

Command	Description
ipv6 ospf area	Configure the interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Show the OSPFv3 routing process information.

37.1.19 log-adj-changes

Use this command to enable the logging of the neighbor state changes. The **no** or **default** form of the command is used to disable it.

log-adj-changes

no log-adj-changes

Parameter settings	None
Default	By default, Disabled
Command mode	Routing process configuration mode

Examples	The configuration example below turns on the log for neighbor status change.
	`DES-7210(config)# router ospf 1`
	`DES-7210(config)# log-adj-changes detail`

Related commands

Command	Description
show ipv6 ospf	Show the OSPF global configuration information

37.1.20 max-concurrent-dd

Use this command to set the maximum number of DD packets that can be processed simultaneously.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter description	**Parameter**	**Description**
	number	Maximum number of DD packets that can be processed simultaneously, 1-65535.

Default configuration	None.
Command mode	OSPFv3 configuration mode.

Examples	The following example set max-concurrent-dd to 4, allowing exchanging DD packet with 4 neighbors at the same time:
	`router ipv6 ospf 1`
	`max-concurrent-dd 4`

37.1.21 passive-interface

Use this command to set the passive interface. Use the **no** form of this command to remove the configuration .

passive-interface {**default** | *interface-type interface-number* }

no passive-interface {**default** | *interface-type interface-number* }

Parameter description	**Parameter**	**Description**
	default	Set all the interfaces to passive ones.
	interface-type interface-number	Set the specified interface to passive one.

Default configuration	None.
Command mode	OSPFv3 configuration mode.

Usage guidelines	After an interface is set to passive one, it no longer receives or sends the hello message. This command applies to the interfaces participating in the OSPF but not to the virtual links.

Examples	The following example enables only VLAN1 to participate in the OSPFv3 process.
	`passive-interface default`
	`no passive-interface vlan 1`

Related commands

Command	Description
ipv6 ospf area	Configure the interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.

37.1.22 redistribute

Use this command to start the route redistribution in order to import the routing information of other routing protocols to the OSPFv3 routing process. Use the **no** form of this command to disable this function or modify the redistribution parameters.

redistribute *protocol* [**metric** *metric-value*] [**metric-type** *type-value*][**route-map** *map-tag*] [**level-1** | **level-1-2** | **level-2**] [**match** [**internal** I **external** | **nssa-external** ([1|2)]]]]]]]

no redistribute *protocol* **[metric][metric-type][route-map]** [**level-1** | **level-1-2** | **level-2**] [**match** [**internal** I **external** | **nssa-external** [1|2)]]]]]]]

Parameter description

Parameter	Description
protocol	Routing protocol that is redistributed, including static, connected, rip, and bgp.
metric *metric-value*	Specify the metric for the route to be redistributed. Its range is 0 to 16777214, and the default value is **default-metric**.
metric-type *type-value*	Specify the type for the route to be redistributed. The default value is 2.

	route-map *map-tag*	Specify the routing policy for route redistribution. The name of **map-tag** can be up to 32 characters. By default, **route-map** is not set.
	match [**internal** | **external** | **nssa-external**] [1|2)]	Redistribute the OSPF routes of the specific type: internal: inter-area and intra-area routes external [1|2]: E1, E2 or all external routes nssa-external [1|2): N1, N2 or all external NSSA routes.

Default configuration

Disabled.

Command mode

OSPFv3 configuration mode.

Usage guidelines

When a device supports multiple routing protocols, the coordination between these protocols becomes an important task. The device can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

When redistributing OSPF routes, you can configure match to redistribute the corresponding routes. All types of OSPF routes are redistributed by default.

The match parameter of route-map is specific the source of routes. The parameters *tag*, *metric* and *metric-type* of the set rule of route-map take precedence over the ones configured for the redistribute command.

Examples

The following example redistributes the direct route and associates route-map test (the corresponding rule is match metric 20 and set metric 20).

```
redistribute connect metric 10 route-map test
```

Related commands

Command	Description
default-information	Set the default route to be redistributed.

	originate	
	default-metric	Set the default metric for the route to be redistributed.
	summary-prefix	Set the converged address range of the external route.
	show ipv6 ospf	Show the OSPFv3 routing process information.
	show ipv6 ospf database	Show the OSPFv3 LSA information.

37.1.23 router-id

Use this command to set the router ID (device ID). Use the **no** form of this command to remove the setting or restore it to the default router ID.

router-id *router-id*

no router-id

Parameter description

Parameter	Description
router-id	ID of the device in the IPv4 address format.

Default configuration

The best interface address is automatically selected as the router ID.

Command mode

OSPFv3 configuration mode.

Usage guidelines

Each device that runs the OSPFv3 process shall be identified with a router ID. Router ID is in the format of IPv4 address.

Unlike the OSPFv2, the OSPFv3 process will automatically acquire an IPv4 address to use it as the router ID. After the device starts the OSPFv3 process, a user must use the **router-id** command to configure the router ID for the OSPFv3 process. Otherwise, the OSPFv3 process will not be able to start.

The router ID shall be unique.

At present, after the OSPFv3 routing process starts, the Router ID shall be set before the interface participates in the OSPFv3. That is to say, after the interface runs OSPFv3 routing process, the router ID cannot be modified. Otherwise the OSPFv3 routing process and the whole OSPF AS will be greatly affected.

	If the router ID needs to be reconfigured, shut down and restarts the OSPFv3 process, and then configure router ID.
Examples	The following example sets the ID of the device that participates in the OSPFv3 process to 1.1.1.1. `router-id 1.1.1.1`

Related commands

Command	Description
ipv6 ospf priority	Set the interface priority.
show ipv6 ospf	Show the OSPFv3 routing process information.

37.1.24 timers spf

Use this command to set the dalay and interval for the OSPFv3 to calculate SPF after receiving the topology change. The **no** format of this command is used to restore it to the default.

timers spf *delay holdtime*

no timers spf

Parameter description

Parameter	Description
delay	Delay from determining the topology change to calculating SPF. Its range is 0 to 214748364s, and the default value is 5s.
holdtime	Delay from determining the topology change to calculating SPF. Its range is 0 to 214748364s, and the default value is 5s.

Default configuration	*spf-delay*: 5 seconds. *spf-holdtime:* 10 seconds.
Command mode	OSPFv3 configuration mode.
Usage guidelines	The smaller the *spf-delay* and *spf-holdtime*, the shorter time the OSPF takes to adapt to the topology change, but the more system

space will be occupied.

Examples

```
timers spf 2 4
```

Related commands

Command	Description
clear ipv6 ospf	Restart part function of the OSPFv3.
show ipv6 ospf	Show the OSPFv3 routing process information.

37.2 Show Related Command

37.2.1 show ipv6 ospf

Use this command to show the information of the OSPFv3 process.

show ipv6 ospf [*process-id*]

Parameter description

Parameter	Description
process- id	OSPF process number, 1-65535.

Command mode

Privileged mode.

Examples

The following example shows the information about the OSPFv3 process.

```
DES-7210# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 11
 Number of LSA received 4
 Log Neighbor Adjency Changes : Enabled
 Number of areas in this device is 2
 Area BACKBONE(0)
 Number of interfaces in this area is 1(1)
 SPF algorithm executed 4 times
 Number of LSA 3.  Checksum Sum 0x1DDF1
 Number of Unknown LSA 0
```

With the BFD for OSPFv3 configured, the content of “BFD is enabled” is added to the displaying information of the command **show ipv6 ospf**. For example:

```
DES-7210# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 11
 Number of LSA received 4
 Log Neighbor Adjency Changes : Enabled
 Number of areas in this device is 2
 BFD is enabled
 Area BACKBONE(0)
 Number of interfaces in this area is 1(1)
 SPF algorithm executed 4 times
 Number of LSA 3.  Checksum Sum 0x1DDF1
 Number of Unknown LSA 0
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
default-information originate	Set the default route to be redistributed.
default-metric	Set the default metric for the route to be redistributed.
router-id	Router ID
timers spf	Set the delay and interval for the OSPFv3 to perform SPF calculation after receiving the topology change.

37.2.2 show ipv6 ospf database

Use this command to show the database information of the OSPFv3 process

show ipv6 ospf [*process- id*] **database** [**lsa-type** [**adv-router** *router-id*]]

Parameter description

Parameter	Description
process- id	OSPF process number, 1-65535
lsa-type	LSA type. There are the following types:

	external, link, inter-prefix, inter-router, intra-prefix, network, router, te If this parameter is not specified, all LSA information will be shown.
adv-router *router-id*	Show the LSA information generated by the specified router.

Command mode

Privileged mode.

Examples

The following example shows the information about the OSPFv3 process database.

```
DES-7210# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface FastEthernet 1/0)

Link State ID   ADV Router     Age  Seq#      CkSum  Prefix
0.0.0.2         1.1.1.1        197 0x80000001 0x7cd8     0
0.0.0.5         2.2.2.2        206 0x80000001 0x8c86     0
              Link-LSA (Interface Loopback 1)
Link State ID   ADV Router     Age  Seq#      CkSum  Prefix
0.0.64.1        1.1.1.1         82 0x80000001 0xb760     0
              Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router     Age  Seq#      CkSum   Link
0.0.0.0         1.1.1.1      17 0x80000006 0x62a1     1
0.0.0.0         2.2.2.2        156 0x80000003 0x8653     1
              Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router     Age  Seq#      CkSum
0.0.0.5         2.2.2.2        157 0x80000001 0xf8f6
              Router-LSA (Area 0.0.0.1)
Link State ID   ADV Router     Age  Seq#      CkSum   Link
0.0.0.0         1.1.1.1         17 0x80000002 0x0529     0
              Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router     Age  Seq#      CkSum
0.0.0.1         1.1.1.1         77 0x80000002 0x83b4
AS-external-LSA
Link State ID   ADV Router     Age  Seq#      CkSum
0.0.0.1         1.1.1.1         1 0x80000001 0x6035 E2
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.

37.2.3 show ipv6 ospf interface

Use this command to show the OSPFv3 interface information.

show ipv6 ospf interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and interface number.

Command mode

Privileged mode.

Examples

The following commands show the information about the OSPFv3 interface.

```
DES-7210# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit
5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

If the BFD has been enabled for the neighbor on the interface, the content of “BFD enabled” is added to the displaying information of the command **show ipv6 ospf interface**. For example:

```
DES-7210# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
```

```
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit
5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
ipv6 ospf area	Enable the interface to participate in the OSPFv3 process.

37.2.4 show ipv6 ospf neighbor

Use this command to show the neighbor information of the OSPFv3 process.

show ipv6 ospf [*process- id*] **neighbor** [**interface-type** *interface-number* [**detail**]| *neighbor-id* |**detail**]

Parameter description

Parameter	Description
process- id	OSPFv3 process number, 1-65535
detail	Show details about the neighbor.
interface-type interface-number	Interface type And interface number
neighbor-id	Neighbor ID

Command mode

Privileged mode.

Examples

The following command shows the brief information about the OSPF neighbor.

```
DES-7210# show ipv6 ospf neighbor
OSPFv3 Process (1), Neighbores, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:33    FastEthernet 1/0
0
```

The following command shows the details of neighbors:

```
DES-7210# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c
    In the area 0.0.0.0 via interface FastEthernet 1/0
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 2.2.2.2 BDR is 1.1.1.1
    Options is 0x000013 (-|R|-|-|E|V6)
    Dead timer due in 00:00:36
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
```

If the BFD detection has been enabled for the forwarding path of neighbor on the interface, the content of “BFD session state up” is added to the displaying information of the command **show ipv6 ospf neighbor detail**. For example:

```
DES-7210# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c
    In the area 0.0.0.0 via interface FastEthernet 1/0
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 2.2.2.2 BDR is 1.1.1.1
    Options is 0x000013 (-|R|-|-|E|V6)
    Dead timer due in 00:00:36
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    BFD session state up
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
ipv6 ospf area	Enable the interface to participate in the OSPFv3 process.
area virtual-link	Configure the OSPFv3 virtual link.
show ipv6 ospf interface	Show the OSPFv3 interface information.

37.2.5 show ipv6 ospf route

Use this command to show the OSPFv3 route information.

show ipv6 ospf [*process- id*] **route** [**count**]

Parameter description

Parameter	Description
process- id	OSPFv3 process number, 1-65535.
count	Number of OSPFv3 routes

Command mode	Privileged mode.

Examples

The following example shows the information about OSPF routes.

```
DES-7210# show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area,
E1 - OSPF external type 1, E2 - OSPF external type 2
Destination                              Metric
Next-hop
E2 2222::/64                                    1/20
via fe80::c800:eff:fe84:1c, FastEthernet 1/0
O  3333::/64                                     11
via fe80::c800:eff:fe84:1c, FastEthernet 1/0, Area 0.0.0.0
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.

37.2.6 show ipv6 ospf topology

Use this command to show the topology of each area of OSPFv3.

show ipv6 ospf [*process- id*] **topology** [**area** *area-id*]

Parameter description

Parameter	Description
process- id	OSPFv3 process number, 1-65535
area-id	Area ID

Command mode	Privileged mode.

Examples

The following command shows the topology of each area of OSPFv3.

```
DES-7210# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID       Bits  Metric    Next-Hop
Interface
1.1.1.1          EB  --
2.2.2.2          E   1         2.2.2.2
FastEthernet 1/0

OSPFv3 paths to Area (0.0.0.1) routers
Router ID       Bits  Metric    Next-Hop
Interface
1.1.1.1          B   --
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
area range	Configure the address range of the OSPF area.

37.2.7 show ipv6 ospf virtual-links

Use this command to show the virtual link information of the OSPFv3 process.

show ipv6 ospf [*process- id*] **virtual-links**

Parameter description

Parameter	Description
process- id	OSPFv3 process number, 1.65535

Command mode

Privileged mode.

Examples

The following command shows the information about the OSPFv3 virtual link.

```
DES-7210# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 2.2.2.2 is down
  Transit area 0.0.0.1 via interface FastEthernet 1/0, instance ID
0
  Local address *
  Remote address 3333::1/128
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in inactive
    Adjacency state Down
```

	Command	Description
Related commands	**ipv6 router ospf**	Start the OSPFv3 routing process.
	area virtual-link	Configure the OSPFv3 virtual link.
	show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.

38 IGMP Configuration Commands

38.1 IGMP Configuration Task List

Use the following commands to configure the routing protocol to manage multicast groups:

- **clear ip igmp group**
- **clear ip igmp interface**
- **ip igmp access-group**
- **ip igmp join-group**
- **ip igmp static-group**
- **ip igmp immediate-leave group-list**
- **ip igmp last-member-query-count**
- **ip igmp last-member-query-interval**
- **ip igmp limit (interface configuration mode)**
- **ip igmp query-interval**
- **ip igmp query-max-response-time**
- **ip igmp querier-timeout**
- **ip igmp robustness-variable**
- **ip igmp version**
- **ip igmp limit (global configuration mode)**
- **ip igmp proxy-service**
- **ip igmp mroute-proxy**
- **ip igmp ssm-map enable**
- **ip igmp ssm-map static**
- **show ip igmp groups**
- **show ip igmp interface**
- **show ip igmp ssm-mapping**

38.1.1 clear ip igmp group

Use this command to clear dynamic group member information obtained from the response messages in the IGMP buffer.

Command Syntax	**clear ip igmp group**[*group-address* | *interface-type interface-number*]

Parameter description

Parameter	Description
N/A	Delete all group information.
group-address	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
interface-type	Interface type.
interface-number	Interface number.

Command mode	Privileged mode.
Usage guidelines	The IGMP buffer includes a list that contains the multicast groups that the hosts in the direct subnet join. If the device joins a group, this group will be included in this list. To delete all the entries from the IGMP buffer, use the **clear ip igmp group** command without parameters.
Examples	Delete all group entries: `DES-7210# clear ip igmp group`

Related commands	**show ip igmp groups** **show ip igmp interface**

38.1.2 clear ip igmp interface

Use this command to clear the IGMP entry for the interface.

Command syntax	**clear ip igmp interface** *ifname*

Parameter description

Parameter	Description
ifname	Name of the interface

	N/A	All interfaces

Default N/A.

Command mode Privileged mode.

Usage guidelines This command is used to clear the information on the interface that is generated when IGMP is configured. The *ifname* parameter can be ignored.

Examples

```
DES-7210# clear ip igmp interface gigabitEthernet 4/1
```

38.1.3 ip igmp access-group

Use this command to control a multicast group on the interface. The **no** form of this command disables this function.

Command syntax

ip igmp access-group *access-list*

no ip igmp access-group

Parameter description

Parameter	Description
access-list	Name of access control list within the range of 1 to 199, 1300 to 2699, or characters.

Default Filtering conditions are not set.

Command mode Interface configuration mode.

Usage guidelines You can add some interfaces of the host in a subnet to multiple multicast groups. These multicast groups can be controlled using **ip igmp access-group**.

Examples In the following example, the host service can only add the interface GigabitEthernet 4/1 to the group 225.2.2.2 .

```
DES-7210# configure terminal
DES-7210(config)# access-list 1 permit 225.2.2.2 0.0.0.0
```

```
DES-7210(config)# interface GigabitEthernet 4/1
DES-7210(config-if)# ip igmp access-group 1
```

38.1.4 ip igmp join-group

Use this command to configure the interface of the switch with host activities and adds it to a multicast group, so that the sub-switch can learn the corresponding group information. You can use this command to add an interface to a group. The **no** form of this command removes the setting.

Command Syntax

ip igmp join-group *group-address*

no ip igmp join-group *group-address*

Parameter description

Parameter	Description
group-address	Multicast group IP address

Default configuration

The interface is not manually added to the multicast group.

Command mode

Interface configuration mode.

Usage guidelines

This command enables the host activities for the IGMP interface. When the host function is enabled, the interface can initiate the report message and respond to the query message.

If the IGMP function is enabled on the interface, the interface can initiate the report message, so that the interface can learn the configured group members.

You can use this command to add an interface to a group.

Examples

Following example is to add a host group member manually:

```
DES-7210# configure terminal
DES-7210(config)# interface fast 0/1
DES-7210(config-if)# ip igmp join-group 233.3.3.3
```

38.1.5 ip igmp static-group

Use this command to directly add an interface to a group. You can use this command to add an interface to a group. Use the **no** form of this command to remove the setting.

Command Syntax	**ip igmp static-group** *group-address* **no ip igmp static-group** *group-address*

Parameter description

Parameter	Description
group-address	Multicast group IP address.

Default configuration	The switch is not added to the multicast group manually.
Command mode	Interface configuration mode.
Usage guidelines	This command directly adds an interface to a multicast group. The difference from **join-group** is that it directly adds an interface to the group without interacting with a report message. You can use this command to add an interface to a group.

Examples	Following example is to add a host group member manually:
	`DES-7210# configure terminal`
	`DES-7210(config)# interface fast 0/1`
	`DES-7210(config-if)# ip igmp static-group 233.3.3.3`

38.1.6 ip igmp immediate-leave group-list

In the IGMPversion2 and IGMPversion3 versions, use this command to shorten the delay of leaving a group. This command is used when a single receiving host is connected to a single interface. The **no** form of this command is used to disable this function.

Command syntax	**ip igmp immediate-leave group-list** *access-list* **no ip igmp immediate-leave group-list**

Parameter description

Parameter	Description
access-list	Name of access control list.

Default	Disabled.

Command mode	Interface configuration mode.
Usage guidelines	If this command is not configured, the device will send a particular group query message upon receiving the leaving message from the interface. When the host response is timeout, the device stops forwarding packets to this interface. The length of timeout depends on the query interval of the last member and IGMP robustness variable. The default value is 2s. If this command is configured, the device does not send a particular group query message upon receiving the leaving message from the interface. Instead, it directly removes this interface from the IGMP buffer and notifies the IGMP protocol. This will shorten the time significantly.

Examples	The following example demonstrates how to provide the immediate leaving function for some multicast groups. Certainly, you must make sure each interface of these multicast groups have one group member only.
	`DES-7210# configure terminal`
	`DES-7210(config)# access-list 1 permit 225.192.20.0 0.0.0.255`
	`DES-7210(config)# interface ethernet 0/1`
	`DES-7210(config-if)# ip igmp immediate-leave group-list 1`
	`DES-7210(config-if)# exit`

Related commands	**ip igmp last-member-query-interval.**

38.1.7 ip igmp last-member-query-count

last-member-query-count means the number of query packets that the multicast device will send continuously upon receiving the leave message. Use this command to configure the value of **last-member-query-count**. Use the **no** command to restore it to the default value.

Command syntax	**ip igmp last-member-query-count** *number* **no ip igmp last-member-query-count**

Parameter description

Parameter	Description
number	Value of the last member query count in the

		range 2 to 7.

Default The default value of **last member query count** is 2.

Command mode Interface configuration mode.

Usage guidelines When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **ip igmp last-member-query-count** plus a half of the response time. The device will delete information about this group member if no member report is received within the waiting time.

Examples Set the value of last member query count to 3.

```
DES-7210# configure terminal
DES-7210(config)# interface ethernet 0
DES-7210(config-if)# ip igmp last-member-query-count 3
```

38.1.8 ip igmp last-member-query-interval

Use this command to set the time interval of sending the group query message. Use the **no** form of this command to restore it to the default.

Command syntax

ip igmp last-member-query-interval *interval*

no ip igmp last-member-query-interval

Parameter description

Parameter	Description
Interval	The interval sending the group query message in the range1 to 255(in the unit of 0.1 second).

Default 1s.

Command mode Interface configuration mode.

Usage guidelines When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **ip igmp last-member-query-count** plus a half of the response time. The device will delete information about this group member if no

	member report is received within the waiting time.

Examples	The following example sets the interval of sending the group query message to 20 seconds:
	`DES-7210# configure terminal`
	`DES-7210(config)# interface eth 0`
	`DES-7210(config-if)# ip igmp last-member-query-interval 200`

Related commands	**ip igmp immediate-leave.**

38.1.9 ip igmp limit (interface configuration)

Use this command to set the maximum number of IGMP states on the interface. Use the **no** form of this command to remove the setting.

Command syntax

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit

Parameter description

Parameter	Description
number	Maximum number of IGMP states, depending on devices, 1-16384
except	(Optional) Prevent the groups of the access list from taking part in calculation, which is not limited by maximum number..
access-list	(Optional) Access list

Default

1024

Command mode

Interface configuration mode.

Usage guidelines

This command in global configuration mode limits the number of the IGMP group members. The messages of the members over the limit are not recorded and processed.

This command can be configured globally or on the interface The messages of the members will be ignored if they exceed the interface or global configuration.

Examples

The following example sets the limitation to 300:

```
DES-7210(config-if)# ip igmp limit 300
```

38.1.10 ip igmp query-interval

Use this command to configure the query interval of an ordinary member. Use the **no** form to set the query interval of ordinary member to the default value.

Command syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

Parameter description

Parameter	Description
seconds	Query interval of ordinary member, in second. The range is 1 to 18000s.

Default

125 seconds.

Command mode

Interface configuration mode.

Usage guidelines

The time to query an ordinary member can be changed by configuring the query interval of the ordinary member.

Examples

Configure the query interval of ordinary member to 120s on the interface Ethernet 0.

```
DES-7210(config-if)# ip igmp query-interval 120
```

Configure the query interval of ordinary member to the default value on the interface Ethernet 0.

```
DES-7210(config-if)# no ip igmp query-interval
```

38.1.11 ip igmp query-max-response-time

Use this command to configure the maximum response interval. The **no** form of this command to set the maximum response interval to the default value.

Command syntax

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Parameter description

Parameter	Description
seconds	The maximum response interval, in second. The

		range is 1 to 25s.

Default 10s.

Command mode Interface configuration mode.

Usage guidelines This command works only when IGMPv2 is being used. This command controls the interval for the respondent to respond the query message before the device deletes the group information.

Examples Configure the maximum response interval to 20s on the interface Ethernet 0.

```
DES-7210(config-if)# ip igmp query-max-response-time 20
```

Configure the maximum response interval to the default value on the interface Ethernet 0.

```
DES-7210(config-if)# no ip igmp query-max-response-time
```

38.1.12 ip igmp query-timeout

Use this command to configure the time the device waits before it takes over as the querier. Use the **no** form to restore it to the default.

Command syntax **ip igmp query-timeout** *seconds*
no ip igmp query-timeout

Parameter description

Parameter	Description
seconds	Time the device waits before it takes over as the querier. The range is 60 to 300s.

Default 255s.

Command mode Interface configuration mode.

Usage guidelines IGMPv2 should be run for this command to work. By default, Cisco sets the waiting time of the device to two times of the query interval of **ip igmp query-interval**. In DES-7210, the default value is set to

255s. This device becomes the querier if no query packet is received in this duration.

Examples

Configure the time the device waits before it takes over as the querier to 200s on the interface Ethernet 0.

```
DES-7210(config-if)# ip igmp query-timeout 200
```

Configure the time the device waits before it takes over as the querier to the default value on the interface Ethernet 0.

```
DES-7210(config-if)# no ip igmp query-timeout
```

38.1.13 ip igmp robustness-variable

Use this command to change the value of the robustness variable. Use the **no** form of this command to restore it to the default value.

Command syntax

ip igmp robustness-variable *number*

no ip igmp robustness-variable

Parameter description

Parameter	Description
number	The value of robustness variable ranging 2 to 7.

Default

The default value is 2.

Command mode

Interface configuration mode.

Examples

The following example sets the value of robustness variable to 3:

```
DES-7210# configure terminal
DES-7210(config)# interface ethernet 0
DES-7210(config-if)# ip igmp robustness-variable 3
```

38.1.14 ip igmp version

Use this command to set the version number of IGMP to be used on the interface. Use the **no** form of this command to restore it to the default value.

Command syntax

ip igmp version {**1** | **2** | **3**}

no ip igmp version

Parameter description

Parameter	Description
{**1** | **2** | **3**}	Three version numbers, ranging 1 to 3.

Default

The version number is 2 by default.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to globally configure the IGMP version. It should be noted that IGMP will reset after configuration.

Examples

The following example sets the version number to 2:

```
DES-7210# configure terminal
DES-7210(config)# interface ethernet 0
DES-7210(config-if)# ip igmp version 2
```

Related commands

ip igmp access-group
ip igmp limit
ip multicast rate-limit

38.1.15 ip igmp limit (global configuration)

Use this command to globally set the maximum number of IGMP group records. Use the **no** form of this command to remove the setting.

Command syntax

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit *number* [**except** *access-list*]

Parameter description

Parameter	Description
number	Maximum number of IGMP states, depending on devices
except	(Optional) Prevent the groups of the access list from taking part in calculation.
access-list	(Optional) Acdess list name

Default

65530

Command mode	Global configuration mode.
Usage guidelines	Use this command to globally configure the maximum number of IGMP group records. The messages of the members exceeding the threshold will not be saved in the IGMP buffer and will not be forwarded. This command can be configured globally or on the interface The messages of the members will be ignored if they exceed the interface or global configuration.
Examples	The following example sets the maximum number to 300: `DES-7210(config) # ip igmp limit 300`

38.1.16 ip igmp proxy-service

Use this command to enable the service function of all downlink **mroute-proxy** ports. If you run this command on an interface, the interface becomes the uplink port of the corresponding **mroute-proxy** that associates its downlink ports and maintains the group information reported by the downlink ports.

ip igmp proxy-service

no ip igmp proxy-service

Default configuration	All interfaces are not in the **proxy-serice** status.
Command mode	Interface configuration mode.
Usage guidelines	The command can configure at most 32 interfaces. Each proxy-service port can associate with the maximum of 255 downlink ports. When receiving a query message, the **proxy-service** port responds according to the member information maintained by the port itself. The member information maintained by the **proxy-service** port is collected from the interface configured with **mroute-proxy**. Therefore, if a port is configured with proxy-server, the port performs the host activities, but not the device activities. If **switchport** operation is performed on an interface, the **ip igmp mroute-proxy interface** command configured on the associated downlink ports is automatically deleted.

Examples

Configure an interface to the **proxy-service** module:

```
DES-7210(config-if)# ip igmp proxy-service
```

38.1.17 ip igmp mroute-proxy

Use this command to configure an interface as a mroute-proxy interface that can transmit messages to its uplink ports.

ip igmp mroute-proxy *interfname*

no ip igmp mroute-proxy

Parameter description

Parameter	Description
Interfname	Name of the relevant uplink interface.

Default configuration

N/A.

Command mode

Interface configuration mode.

Usage guidelines

After an uplink interface is configured as **proxy-service** interface, the interface can forward the IGMP messages sent by its members.

Examples

Configure an interface to **mroute-proxy** interface:

```
DES-7210(config-if)# ip igmp mroute-proxy fa 0/1
```

38.1.18 ip igmp ssm-map enable

Use this command to enable the **igmp ssm-map** function in the global configuration mode. Use the **no** form of this command to disable the function.

ip igmp ssm-map enable

no ip igmp ssm-map enable

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines	If this command is configured, the dynamically learned group information is added forcibly to the associated source record. This command is usually used together with the **ip igmp ssm-map static** command.
Examples	Enable the **igmp ssm-map** function in the global configuration mode: DES-7210(config)# **ip igmp ssm-map enable.**

38.1.19 ip igmp ssm-map static

Use this command to map the static **ssm-map** source IP address to the group records in the global mode. Use the **no** form of this command to disable the function.

ip igmp ssm-map static *access-list a.b.c.d*

no ip igmp ssm-map static *access-list a.b.c.d*

Parameter description

Parameter	Description
access-list	ACL name in the range 1 to 99, 1300 to 1999 or characters.
a.b.c.d	Unicast address mapped to the group record.

Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	This command is used together with the **ip igmp ssm-map enable** command. After configuration, the port maps the corresponding source IP address to all received messages below **v3**.
Examples	Map the source address 192.168.2.2to all group records permitted by ACL 11 : `DES-7210(config)# ip igmp ssm-map static 11 192.168.2.2.`

38.2 Show Related Commands

38.2.1 show ip igmp groups

Use this command to show the groups directly connected to the device and the group information learnt from IGMP.

Command syntax

show ip igmp groups [*group-address* | *interface-type interface-number*] [**detail**]

Parameter description

Parameter	Description
group-address	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
interface-type	Interface type.
interface-number	Interface number.
detail	Show the detailed information.
N/A	Show the information about all the groups.

Default

N/A

Command mode

User mode or privileged mode.

Usage guidelines

Use this command without any parameters to show group address, interface type, and information about all the multicast groups directly connected to the interface. Information about a specific group is displayed if a group address is added to the command.

Examples

The following example shows information about all the groups:

```
DES-7210# show ip igmp groups
IGMP Connected Group Membership
Group Address     Interface Uptime    Expires    Last Reporter
224.0.1.1         eth2      00:00:09  00:04:17   10.10.0.82
224.0.1.24        eth2      00:00:06  00:04:14   10.10.0.84
224.0.1.40        eth2      00:00:09  00:04:15   10.10.0.91
224.0.1.60        eth2      00:00:05  00:04:15   10.10.0.7
239.255.255.250   eth2      00:00:12  00:04:15   10.10.0.228
239.255.255.254   eth2      00:00:08  00:04:13   10.10.0.84
```

The following example shows detailed information about a specific group:

```
DES-7210# show ip igmp groups 224.1.1.1 detail
Interface        : eth1
Group: 224.1.1.1
Uptime: 00:00:42
Group mode: Include
Last reporter: 192.168.50.111
TIB-A Count: 2
TIB-B Count: 0
Group source list: (R - Remote, M - SSM Mapping)
Source Address Uptime v3 Exp Fwd Flags
192.168.55.55 00:00:42 00:03:38 Yes R
192.168.55.66 00:00:42 00:03:38 Yes R
```

38.2.2 show ip igmp interface

Use this command to show the information of this interface.

Command syntax

Show ip igmp interface [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.
N/A	Show information about all the interfaces.

Default

Command mode

User mode or privileged mode.

Examples

The following example shows the information of all the interfaces:

```
DES-7210# show ip igmp interface
Interface vlan1.1 (Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying device is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds|
```

```
IGMP Snooping is globally enabled|
IGMP Snooping is enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
```

38.2.3 show ip igmp ssm-mapping

Use this command to show the **ssm-map** information of the IGMP configuration.

show ip igmp ssm-mapping *[A.B.C.D)*

Parameter description

Parameter	Description
A.B.C.D	Source address to be mapped

Default configuration

All the ssm-map information of the IGMP is displayed.

Command mode

Global configuration mode.

Usage guidelines

If all the parameters are not used, the related configurations are displayed.

Examples

Show the **ssm-map** configuration information:

```
DES-7210# sh ip igmp ssm-mapping
SSM Mapping: Enabled
Database    : Static mappings configured
```

Show the group information of group 233.3.3.3 to be mapped

```
DES-7210#show ip igmp ssm-mapping 233.3.3.3
Group address: 233.3.3.3
Database    : Static
Source list  : 192.3.3.3
             : 3.3.3.3
```

39 PIM-DM Configuration Commands

39.1 PIM-DM Related Configuration Commands

PIM-DM protocol configuration includes following commands:

- **ip pim dense-mode**
- **ip pim neighbor-filter**
- **ip pim query-interval**
- **ip pim state-refresh disable**
- **ip pim state-refresh origination-interval**

39.1.1 ip pim dense-mode

Use this command to enable **PIM-DM** on the interface. Use the **no** form of this command to disable the function.

ip pim dense-mode

no ip pim dense-mode

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Interface configuration mode.
Examples	DES-7210# **configure terminal** DES-7210(config)# **interface fastethernet** *0/1* DES-7210(config-if)# **ip pim dense-mode**

Before enabling the PIM-DM, enable the multicast forwarding function in the global configuration moe. Otherwise, the multicast data packet cannot be forwarded even the PIM-DM is enabled.

Once the PIM-DM is enabled, the IGMP is enabled automatically on the interface without manual configuration.

Note

During the execution of this command, if the prompt "`Failed to enable PIM-DM on <Interface Name>, resource temporarily unavailable, please try again`" appears, re-execute this command.

During the execution of this command, if the prompt "`PIM-DM Configure failed! VIF limit exceeded in NSM!!!`" appears, it indicates the allowed configured multicast interface number exceeds the upper limit of the multicast interfaces. In this case, if it's still necessary to enable the PIM-DM on the interface, delete the unnecessary PIM-DM, PIM-SM or DVMRP interfaces.

It is not recommended to configure different multicat routing protocols on different interfaces of a device.

39.1.2 ip pim neighbor-filter

Use this command to enable the neighbor filtering on the interface. If the neighbor filtering is set, PIM-DM will not establish the peering relationship with this neighbor or will terminate the established peering relationship with this neighbor once the neighbor is denied by the filtering access list.

The **no** form of this command is used to disable the neighbor filtering function.

ip pim neighbor-filter *access-list*

no ip pim neighbor-filter *access-list*

Parameter description	**Parameter**	**Description**
	access-list	Number or name of the access list.

Default configuration	Disabled.
Command mode	Interface configuration mode.

Examples	DES-7210# **configure terminal** DES-7210(config)# **interface fastethernet** *0/1* DES-7210(config-if)# **ip pim neighbor-filter** *14*

Note

1. When the associated ACL rule is permit, only the neighbor address in ACL can be used as the PIM neighbor of the current interface. When the associated ACL rule is deny, the neighbor address in ACL cannot be used as the PIM neighbor of the current interface.

2. Peering relationship refers to the interaction of protocol packets between the PIM neighbors. If the peering relationship with a PIM device is terminated, the neighbor relationship with this device will not be established, and the PIM protocol packets from this device will not be received.

39.1.3 ip pim query-interval

Use this command to reconfigure the interval of sending the hello message.The **no** form of this command is used to restore hello interval to the default value.

ip pim query-interval *interval-seconds*

no ip pim query-interval

Parameter description	**Parameter**	**Description**
	Interval-seconds	Interval of sending the hello message in the range of 1 to 65535 seconds.

Default configuration	30 seconds.
Command mode	Interface configuration mode.
Usage guidelines	If **hello interval** is set, the **hello holdtime** value will be updated to 3.5 times of **hello interval**.
Examples	DES-7210# **configure terminal** DES-7210(config)# **interface fastethernet** *0/1*

```
DES-7210(config-if)# ip pim query-interval 123
```

39.1.4 ip pim state-refresh disable

Use this command to prohibit the interface from processing and forwarding the PIM-DM state refresh messages. The **no** form of this command is used to enable the PIM-DM state refresh function on the interface.

ip pim state-refresh disable

no ip pim state-refresh disable

Parameter description	N/A.
Default	The state refresh message is processed and forwarded by default.
Command mode	Global configuration mode.
Usage guidelines	When the state refresh function is disabled, the PIM-DM state refresh message is not processed and forwarded. The sent Hello message does not contain the status refresh option. Consequently, the SR Cap field will not be processed when the Hello message is received.

Examples	The following example disables the processing of the PIM-DM state refresh message.
	`DES-7210# configure terminal`
	`DES-7210(config)# ip pim state-refresh disable`

Note

Generally, it is not recommended to disable the status refresh function because disabling this function may converge the PIM-DM multicast forwarding tree again that has been converged, resulting in unnecessary waste of bandwidth and oscillation of multicast routing table.

39.1.5 ip pim state-refresh origination-interval

Use this command to set the interval of sending the PIM-DM state refresh message. The interval is the seconds elapsed between two state refresh messages. The **no** form of this command restores it to the default value.

ip pim state-refresh origination-interval *interval-seconds*

no ip pim state-refresh origination-interval

	Parameter	Description
Parameter description	*Interval-seconds*	Interval of sending the PIM-DM update message in the range of 1 to 100 in seconds.

Default configuration	60 seconds.
Command mode	Interface configuration mode.

Examples

```
DES-7210# configure terminal
DES-7210(config)# interface fastethernet 0/1
DES-7210(config-if)# ip pim state-refresh
origination-interval 65
```

39.2 Show Related Commands

39.2.1 show ip pim dense-mode interface

Use this command to show the information about the PIM-DM interface.

show ip pim dense-mode interface [*interface-type interface-number*] [**detail**]

	Parameter	Description
Parameter description	*interface-type interface-number*	Interface type and interface ID
	detail	Show details of the interface

Default	Privileged/Global configuration/Interface configuration mode
Command mode	User Modeor privileged mode.

Examples

The following example shows the information of the PIM-DM interface:

```
DES-7210# show ip pim dense-mode interface
Address   Interface  VIFIndex  Ver/Mode    Nbr
                                          Mode Count
10.10.10.10 FastEthernet 0/45 3   v2/D         1
50.50.50.50 VLAN4          2      v2/D          1
```

Description of fields in the results:

Field	Description
Address	Primary IP address of the PIM-DM ir
Interface	Name of the PIM-DM interface
VIF Index	VIF ID (ID)
Ver/Mode	PIM version/mode
Nbr Count	Number of neighbors of the PIM-DM interface.

Related commands

Command	Description
show ip pim dense-mode neighbor	Show the information about the neighbors of the PIM-DM interface.

39.2.2 show ip pim dense-mode neighbor

Use this command to show the information about the PIM-DM neighbors.

show ip pim dense-mode neighbor [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and interface ID.

Command mode

Privileged/Global configuration/Interface configuration mode

Examples

The following example shows the information about the PIM-DM neighbors:

```
DES-7210# show ip pim dense-mode neighbor
Neighbor-Address Interface     Uptime/Expires    Ver
10.10.10.1    FastEthernet 0/45 00:19:29/00:01:21  v2
```

```
50.50.50.1    VLAN 4            00:22:09/00:01:39  v2
```

Description of fields in the results:

Field	Description
Neighbor-Address	IP address of the neighbor
Interface	Name of the interface connecting neighbor
Uptime/Expires	Valid time and aging time of the entry
Ver	PIM version

39.2.3 show ip pim dense-mode nexthop

Use this command to show the information about the PIM-DM next hop.

show ip pim dense-mode nexthop

Parameter description	N/A
Command mode	Privileged/Global configuration/Interface configuration mode

Examples

The following example shows the information about the PIM-Dm next hop:

```
DES-7210# show ip pim dense-mode nexthop
Destination  Nexthop   Nexthop   Nexthop   Metric Pref
               Num       Addr      Interface
1.1.1.111      1       50.50.50.1  VLAN 4     0     1
```

Description of fields in the results:

Field	Description
Destination	Multicast source IP address
Nexthop Num	Number of next hop
Nexthop Addr	IP address of next hop
Nexthop interface	Interface connecting to the of next hc
Metric	Route metric
Pref	Route priority

39.2.4 show ip pim dense-mode mroute

Use this command to show the information about the PIM-DM routing table.

show ip pim dense-mode mroute [*A.B.C.D A.B.C.D*] [**summary**]

Parameter description

Parameter	Description
A.B.C.D A.B.C.D	Multicast source IP address and multicast group IP address
summary	Show the brief information of routing entries. ID.

Command mode

Privileged/Global configuration/Interface configuration mode

Examples

The following example shows the information about the PIM-Dm routing table:

```
DES-7210# show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
(1.1.1.111, 229.1.1.1)
  MRT lifetime expires in 205 seconds
  RPF Neighbor: 50.50.50.1, Nexthop:50.50.50.1,VLAN 4
  Upstream IF: VLAN 4
    Upstream State: Pruned, PLT:200
    Assert State: NoInfo
  Downstream IF List:
    FastEthernet 0/45:
      Downstream State: NoInfo
      Assert State: Loser, AT:170
```

40 PIM-SM Configuraiton Commands

40.1 PIM-SM Configuration Commands

PIM-SM protocol configuration includes following commands:

- **clear ip mroute**
- **clear ip mroute statistics**
- **clear ip pim sparse-mode bsr rp-set**
- **ip multicast-routing**
- **ip pim access-register list**
- **ip pim bsr-candidate**
- **ip pim cisco-register-checksum**
- **ip pim dr-priority**
- **ip pim ignore-rp-set-priority**
- **ip pim jp-timer**
- **ip pim mib**
- **ip pim neighbor-filter**
- **ip pim query-interval**
- **ip pim register-rate-limit**
- **ip pim register-rp-reachability**
- **ip pim register-source**
- **ip pim register-suppression**
- **ip pim rp-address**
- **ip pim rp-candidate**
- **ip pim rp-register-kat**
- **ip pim sparse-mode**
- **ip pim spt-threshold**
- **ip pim ssm**

40.1.1 clear ip mroute

clear ip mroute {* | *group_address [source_address]* }

Parameter description

Parameter	Description
*	Delete all the multicast routing entries.
group_address	Delete the multicast routing entries of the specific group.
group_address source_address	Delete the multicast routing entries of the specific group and source IP address.

Default N/A

Command mode Privileged mode

Usage guideline Multicast routing entries can be deleted manually.

Examples

```
DES-7210# clear ip mroute *
DES-7210# clear ip mroute 224.2.2.2
DES-7210# clear ip mroute 224.2.2.2 2.2.2.2
```

40.1.2 clear ip mroute statistics

clear ip mroute statistics {* | *group_address [source_address]* }

Parameter description

Parameter	Description
*	Delete the statistics of all multicast routing entries.
group_address	Delete the statistics of the multicast routing entries of the specific group.
group_address source_address	Delete the statistics of the multicast routing entries of the specific group and source IP address.

Default	N/A
Command mode	Privileged mode
Usage guideline	The statistics of multicast routing entries can be deleted manually.

Examples	`DES-7210# clear ip mroute statistics *`
	`DES-7210# clear ip mroute statistics 224.2.2.2`
	`DES-7210# clear ip mroute statistics 224.2.2.2 2.2.2.2`

40.1.3 clear ip pim sparse-mode bsr rp-set

clear ip pim sparse-mode bsr rp-set *

Parameter description

Parameter	Description
*	Clear all RP-SET.

Default	N/A
Command mode	Privileged mode
Usage guideline	All the RP information learnt dynamically can be cleared manually.
Examples	`DES-7210# clear ip pim sparse-mode bsr rp-set *`

40.1.4 ip multicast-routing

ip multicast-routing

Parameter description	N/A
Default	Disabled

Command mode	Global configuration mode
Usage guideline	This command is mandatory for enabling multicast routing and enabling PIM-SM on an interface. Otherwise, PIM-SM is disabled even though the **ip pim sparse-mode** command is configured.
Examples	`DES-7210(config)# ip multicast-routing`

40.1.5 ip pim accept-register list

ip pim accept-register list *access-lit*

Parameter description

Parameter	Description
access-list	Access control list supporting numerical ACL in the range of 100 to 199 and 2000 to 2699 and name ACL.

Default	There is no restriction on the source IP address pair of register messages on RP.
Command mode	Global configuration mode
Usage guideline	This command is used to restrict the source IP address of register messages on RP.
Examples	`DES-7210 (config)# ip pim accept-register list 100` `DES-7210 (config)# access-list 100 permit ip 192.168.195.0 0.0.0.255 225.1.1.1 0.0.0.255`

Related commands

Command	Description
access-list	

40.1.6 ip pim bsr-candidate

ip pim bsr-candidate *interface-type interface-number* [*hash-mask-length*] [*priority-value*]

Parameter description

Parameter	Description
interface-type interface-number	Interface type and number
hash-mask-length	(Optional) HASK mask length configured for electing the RP in the range 0 to 32, 10 by default.
priority-value	(Optional) Priority configured for the candidate BSR in the range 0 to 255, 64 by default.

Default

N/A

Command mode

Global configuration mode

Usage guideline

A PIM-SM domain must contain a unique BootStrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM domain. This packet contains the address and priority of the BSR.

This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with the address in the received bootstrap message. If the IP address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message.

The current device considers itself to be BSR until it receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IP address).

Examples

```
DES-7210# configure terminal
DES-7210(config)# ip pim bsr-candidate g 0/3
DES-7210(config)# ip pim bsr-candidate g 0/3 30 192
```

40.1.7 ip pim cisco-register-checksum

ip pim cisco-register-chekcsum [group-list *access-list***]**

Parameter description

Parameter	Description
access-list	Access control list supporting numerical ACL in the range of 1 to 99 and 1300 to 1999 and name ACL.
group-list *access-list*	Apply this configuration to all multicast IP addresses by default.

Default

By default, the checksum of register messages calculates the head of PIM message and register message rather than the whole PIM message and is not calculated in Cisco way.

Command mode

Global configuration mode

Usage guideline

This command is used to achieve the compatibility with those devices that the checksum of register messages calculate the whole PIM message including encapsulated multicast data packet rather than the head of the register message.

Examples

```
DES-7210# configure terminal
DES-7210(config)#ip pim cisco-register-checksum
DES-7210(config)#ip pim cisco-register-checksum group-list 99
DES-7210(config)# access-list 99 permit 225.1.1.1 0.0.0.255
```

Related commands

Command	Description
access-list	

40.1.8 ip pim dr-priority

ip pim dr-priority *priority-value*

Parameter description

Parameter	Description
priority-value	The larger the value, the higher the priority is. The range is 0 to 4294967294. The default value is 1.

Default	The DR priority is 1 by default.
Command mode	Interface configuration mode
Usage guideline	To select a DR: ■ If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices has the same priority, the one of the largest IP address is elected to be the DR. ■ If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.
Examples	`DES-7210# configure terminal` `DES-7210(config)# interface` **`g`** *`0/3`* `DES-7210(config-if)# ip pim dr-priority` *`10000`*

40.1.9 ip pim ignore-rp-set-priority

ip pim ignore-rp-set-priority

Parameter description	N/A
Default	By default, the RP priority of the RP-set is taken into account.
Command mode	Global configuration mode
Usage guideline	This command is used to ignore the priority of the RP corresponding to the multicast group.
Examples	`DES-7210#` **`configure terminal`** `DES-7210(config-if)#` **`ip pim ignore-rp-set-priority`**

40.1.10 ip pim jp-timer

ip pim jp-timer *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	Interval to send the join/prune message in the range 1 to 65535 seconds

Default By default, the Join/Prune message is sent at the interval of 60s.

Command mode Global configuration mode

Usage guideline This command is used to set the interval to send the Join/Prune message.

Examples

```
DES-7210# configure terminal
DES-7210(config)# ip pim jp-timer 50
```

40.1.11 ip pim mib

ip pim mib dense-mode

Parameter description N/A

Default By default, the MIB of the sparse mode is used.

Command mode Global configuration mode

Usage guideline This command is used to use the MIB of the dense mode.

Examples

```
DES-7210# configure terminal
DES-7210(config-if)# ip pim mib dense-mode
```

40.1.12 ip pim neighbor-filter

ip pim neighbor-filter *access_list*

Parameter description

Parameter	Description
access_list	Access control list supporting numerical ACL in the range 1 to 99 and name ACL

Default Disabled

Command mode Interface configuration mode

Usage guideline Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.

Examples

```
DES-7210# configure terminal
DES-7210(config)# interface g 0/3
DES-7210(config-if)# ip pim neighbor-filter 14
DES-7210(config-if)# exit
DES-7210(config)# access-list 14 deny 192.168.1.5 0.0.0.255
```

Related commands

Command	Description
access-list	

40.1.13 ip pim query-interval

ip pim query-interface *interval-seconds*

Parameter description

Parameter	Description
interval-seconds	Interval to send the Hello message in the range 1 to 65535 seconds

Default By default, the Hello message is sent at the interval of 30s.

Command mode	Interface configuration mode
Usage guideline	Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 65535.
Examples	DES-7210# **configure terminal** DES-7210(config)# **interface g** *0/3* DES-7210(config)# **ip pim query-interval** *123*

40.1.14 ip pim register-rate-limit

ip pim register-rate-limit *rate*

Parameter description

Parameter	Description
rate	Maximum number of register packets that can be sent per second, in the range of 1 to 65535

Default	By default, there is no rate limitation on register messages.
Command mode	Global configuration mode
Usage guideline	This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.
Examples	DES-7210# **configure terminal** DES-7210(config)# ip pim register-rate-limit *3000*

40.1.15 ip pim register-rp-reachability

ip pim register-rp-reachability

Parameter description	N/A
Default	By default, the RP reachability is not checked before transmission.
Command mode	Global configuration mode
Usage guideline	This command is used to check the RP reachability before transmission. If not, register packets are not transmitted.
Examples	DES-7210# **configure terminal** DES-7210(config)# **ip pim register-rp-reachability**

40.1.16 ip pim register-source

ip pim register-source {*source_ip* | *interface-type interface-number*}

Parameter description

Parameter	Description
source_ip	Source IP address of register packets
interface-type interface-number	Interface whose IP address is used as the source IP address of register packets

Default	By default, the source IP address of register packets is the IP address of the DR interface connecting the multicast source.
Command mode	Global configuration mode
Usage guideline	This command is used to configure the source IP address of register messages. The source IP address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IP address as the destination IP address of the Register-Stop packet.

Examples

```
DES-7210# configure terminal
DES-7210(config)# ip pim register-source 192.168.195.80
DES-7210(config)# ip pim register-source g 0/3
```

40.1.17 ip pim register-suppression

ip pim register-suppression *seconds*

Parameter description

Parameter	Description
suppression	Suppression time in the range of 11 to 21843 seconds

Default

By default, the register packet suppression time is 60 seconds.

Command mode

Global configuration mode

Usage guideline

Executing this command on the DR will change the register packet suppression time configured. if the **ip pim rp-register-kat** command is not configured, executing this command on RP will modify the period of RP keepalive.

Examples

```
DES-7210# configure terminal
DES-7210(config)# ip pim register-suppression 100
```

40.1.18 ip pim rp-address

ip pim rp-address *rp-address [access_list]*

Parameter description

Parameter	Description
rp-address	IP address of RP
access_list	Access control list supporting numerical ACL in the range 1 to 99 and 1300 to 1999 and name ACL. All multicast groups are supported by default.

Default

No IP address is configured for the static RP by default.

Command mode	Global configuration mode
Usage guideline	This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that: ■ If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes precedence. ■ You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once. ■ If there are more than one static RP in a multicast group, the one of the highest IP address is used. ■ Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted. ■ After configuration is performed, the static RP's source IP address is inserted to the group range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IP address. When you select a RP from a static RP group, the first entry, namely the one wit the largest IP address, will be selected first. ■ Deleting a static IP address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP address.
Examples	DES-7210# **configure terminal** DES-7210(config)# **ip pim rp-address** *210.34.0.55* DES-7210(config)# **ip pim rp-address** *210.34.0.55 4* DES-7210(config)# **access-list** *4* **permit** *255.1.1.1 0.0.0.255*

Related commands

Command	Description
access-list	

40.1.19 ip pim rp-candidate

ip pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *access_list*]

Parameter description

Parameter	Description
interface-type interface-number	Interface
priority-value	(Optional) Priority in the range 0 to 255, 192 by default
interval-seconds	(Optional) Interval in the range 0 to 16383 seconds, 60s by default
group_list *access_list*	(Optional) Numberical ACL in the rnage 1 to 99 or name ACL. By default, all multicast groups are permitted.

Default

N/A

Command mode

Global configuration mode

Usage guideline

In the PIM-SM protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain.

To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.

Examples

```
DES-7210# configure terminal
DES-7210(config)# ip pim rp-candidate g 0/3
DES-7210(config)# ip pim rp-candidate g 0/3 priority 200 group-list
3 interval 70
DES-7210(config)# access-list 3 permit 255.1.1.1 0.0.0.255
```

Related commands

Command	Description
access-list	

40.1.20 ip pim rp-register-kat

ip pim rp-register-kat *seconds*

Parameter description	**Parameter**	**Description**
	seconds	KAT timer time in the range 1 to 65525 seconds

Default	210s
Command mode	Global configuration mode
Usage guideline	This command is used to configure the KAT interval of RP.
Examples	DES-7210# **configure terminal** DES-7210(config)# **ip pim rp-register-kat** *250*

40.1.21 ip pim sparse-mode

ip pim sparse-mode

Parameter description	N/A
Default	Disabled
Command mode	Interface configuration mode
Usage guideline	This command is used to enable PIM-SM on the interface.
Examples	DES-7210# **configure terminal** DES-7210(config)# **interface g** *0/3* DES-7210(config-if)# **ip pim sparse-mode**

Note

You need to enable multicast routing forwarding in the global configuration mode before enabling PIM-SM. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM.

During the execution of this command, if the prompt "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.

During the execution of this command, if the prompt "PIM-SM Configure failed! VIF limit exceeded in NSM!!!" appears, it indicates the allowed configured interface number exceeds the upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SM on the interface, delete the unnecessary PIM-SM, PIM-DM or DVMRP interfaces.

40.1.22 ip pim spt-threshold

ip pim spt-threshold [**group-list** *access_list*]

Parameter description

Parameter	Description
access_list	(Optional) Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL. By default, all multicast groups are permitted for SPT switching.

Default

By default, SPT switching is disabled.

Command mode

Global configuration mode

Usage guideline

This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using **group-list**) or all multicast groups (not using **group-list**) .

Examples

```
DES-7210# configure terminal
DES-7210(config)# ip pim spt-threshold
DES-7210(config)# ip pim spt-threshold group-list 12
DES-7210(config)# access-list 12 permit 225.1.1.1 0.0.0.255
```

Related commands	Command	Description
	access-list	

40.1.23 ip pim ssm

ip pim ssm {**default** | **range** *access_list*}

Parameter description	Parameter	Description
	default	Multicast groups of 232/8
	access_list	Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL.

Default	Disabled.
Command mode	Global configuration mode
Usage guideline	This command is used to enable PIM-SSM (or in some specific multicast groups).

Examples	The following command sets the source-specific multicast of the multicast group range 232/8:
	`DES-7210# configure terminal`
	`DES-7210(config)# ip pim ssm default`
	The following command sets the source-specific multicast with ACL 10.
	`DES-7210(config)# ip pim ssm range 10`
	`DES-7210(config)# access-list 10 permit 232.0.0.1 0.0.0.255`

Related commands	Command	Description
	access-list	

40.2 Show Related Commands

40.2.1 show debugging

show debugging

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command is used to turn on debugging switch.

Examples	`DES-7210 # show debugging`
	`PIM-SM Debugging status:`
	`PIM packet debugging is on.`

40.2.2 show ip pim sparse-mode bsr-router

show ip pim sparse-mode bsr-router

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command is used to show BSR information.

Examples

```
DES-7210# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 192.168.127.1
Uptime:     01d23h14m, BSR Priority: 64, Hash mask length: 10
Next bootstrap message in 00:00:42
Role: Candidate BSR   Priority: 64, Hash mask length: 10
State: Elected BSR
Candidate RP: 30.30.100.200(GigabitEthernet 0/3)
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:32
```

40.2.3 show ip pim sparse-mode interface

show ip pim sparse-mode interface [*interface-type interface-number* [**detail**]]

Parameter description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all commands by default.
detail	(Optional) Show the details of an interface.

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline

This command shows the PIM-SM information on the interface.

Examples

```
DES-7210 #show ip pim sparse-mode interface detail
GigabitEthernet 0/3 (vif 2):
  Address 30.30.100.200, DR 30.30.100.200
  Hello period 30 seconds, Next Hello in 13 seconds
  Triggered Hello period 5 seconds
  Neighbors:
   30.30.100.1
```

40.2.4 show ip pim sparse-mode local-members

show ip pim sparse-mode local-member [*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all commands by default.

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline

This command shows the local IGMP information on the PIM-SM-enabled interface.

Examples

```
DES-7210 (config-if)#show ip pim sparse-mode local-members
PIM Local membership information
GigabitEthernet 0/3:
  (*, 225.1.1.1) : Include
Loopback 1:
```

40.2.5 show ip pim sparse-mode mroute

show ip pim sparse-mode mroute *[group_address|source_address]*

Parameter description

Parameter	Description
group_address	Group IP address in the form of A.B.C.D.
source_address	Source IP address in the form of A.B.C.D

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline

This command is used to show route information. Only one group IP address, one source IP address or one group IP address-source IP address pair can be configured at a time. You can also specify no group IP address or source IP address.

40.2.6 show ip pim sparse-mode neighbor

show ip pim sparse-mode neighbor

Parameter description	**Parameter**	**Description**
	detail	(Optional) Show the details of an interface.

Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command shows the information on neighbors .
Examples	DES-7210# **show ip pim sparse-mode neighbor detail** Nbr 5.5.5.3 (VLAN 1) Expire in 81 seconds

40.2.7 show ip pim sparse-mode nexthop

show ip pim sparse-mode nexthop

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command shows the information on the next hop, including interface number, IP address and metric.

40.2.8 show ip pim sparse-mode rp mapping

show ip pim sparse-mode rp mapping

Parameter description	N/A
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode
Usage guideline	This command shows the information on all RPs and the multicast groups they serve.

Examples

```
DES-7210# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 30.30.200.1
Info source: 30.30.200.1, via bootstrap, priority 192
Uptime: 00:00:51, expires: 00:01:39
RP: 30.30.100.1
Info source: 30.30.200.1, via bootstrap, priority 192
Uptime: 00:19:14, expires: 00:01:38
Group(s): 224.0.0.0/4, Static
RP: 100.100.100.100
Uptime: 00:45:35
```

40.2.9 show ip pim sparse-mode rp-hash

show ip pim sparse-mode rp-hash *group-address*

Parameter description

Parameter	Description
group-address	Group address to be resolved

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage guideline This command shows the information on the RP of the specific group IP address.

Examples

```
DES-7210# show ip pim sparse-mode rp-hash 255.1.1.1
RP: 30.30.100.1
Info source: 30.30.100.1, via bootstrap
```

41 Multicast Routing Configuration Commands

41.1 Configuration Related Commands:

- **clear ip mroute**
- **clear ip mroute statistics**
- **ip mroute**
- **ip multicast route-limit**
- **ip multicast ttl-threshold**
- **ip multicast-routing**
- **ip multicast boundary**
- **ip multicast static**

41.1.1 clear ip mroute

Use this command to remove the forwarding information of the IP multicast routes.

clear ip mroute {***** | *group-address* [*source -address*]}

Parameter description	**Parameter**	**Description**
	*	Remove all the forwarding information in the IP multicast route table.
	group-address	Group IP address of IP multicast routes.
	source-address	Source IP address of multicast routess.

Command mode	Privileged mode.

Examples

Following example shows how to remove the entry whose group IP address is 230.0.0.1 from the multicast routing table:

```
DES-7210# clear ip mroute 230.0.0.1
```

Related commands

Command	Description
show ip mroute	Show the forwarding information of multicast routes.

41.1.2 clear ip mroute statistics

Use this command to remove the statistics of IP multicast routes.

clear ip mroute statistics {***** | *group-address* [*source -address*]}

Parameter description

Parameter	Description
*	Remove all the forwarding entries in the multicast route table.
group-address	Group IP address of IP multicast routes
source-address	Source IP address of multicast route.

Command mode

Privileged mode.

Usage guideline

This command allows you to clear the statistics information of IP multicast routes.

Examples

Following example shows how to clear the statistics of entry with the group IP address 230.0.0.1 from the multicast routing table.

```
DES-7210# clear ip mroute statistics 230.0.0.1
```

Related commands

Command	Description
show ip mroute	Show the multicast route forwarding information.
clear ip mroute	Clear the multicast route forwarding information.

41.1.3 ip mroute

Use this command to configure static multicast routes. Use the **no** form of this command to delete the configured routes.

ip mroute *source-address mask* [*protocol as-number*] {*rpf-addrress* | *interface-type interface-number*} [*distance*]

no ip mroute *source-address mask* [*protocol as-number*] {*rpf-addrress* | *interface-type interface-number*} [*distance*]

Parameter description

Parameter	Description
source-address	Source IP address of the multicast route
mask	Mask of the source IP address
protocol	(Optional) The unicast routing protocol being used.
rpf-address	Incoming interface of the multicast route
interface-type interface-number	Interface type and interface ID.
distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Default

distance: 0.

Command mode

Global configuration mode.

Usage guideline

This command is used to configure the route for the purpose of RFF check. Note that the configured route is prior to the route learned in the unicast form.

Examples

The following example allows the multicast routes of all the sources in a network to pass 172.30.10.13:

```
DES-7210(config)# ip mroute 172.16.0.0 255.255.0.0
```

	172.30.10.13

41.1.4 ip multicast route-limit

Use this command to limit the number of the entries that can be added to the multicast routing table.

ip multicast route-limit *limit* [*threshold*]

no ip multicast route-limit *limit* [*threshold*]

Parameter description	**Parameter**	**Description**
	limit	The number of the entries that can be added to the multicast routing table is 1 to 2147483647. The default value is 1024.
	threshold	(Optional) Number of multicast routes at which alarms will be triggered. The default value is 2147483647.

Default	The default value of *limit* is 1024. The default value of *threshold* is 2147483647.
Command mode	Global configuration mode.
Usage guideline	This command is used to restrict the number of route adding to the IPv6 multicast table. Note that the hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.
Examples	The following example sets the route limit to 500. `DES-7210(config)# ip multicast route-limit 500`

41.1.5 ip multicast ttl-threshold

Use this command to configure TTL (time-to-live) threshold on the interface. Use the **no** form of the command to restore it to the default value.

ip multicast ttl-threshold *ttl-value*

ip multicast ttl-threshold

Parameter description

Parameter	Description
ttl-value	TTL threshold on the interface, within the range of 0 to 255.

Default

The default *ttl-value* is 1.

Command mode

Interface configuration mode.

Usage guideline

Use **show running-config** to display configuration. A device with multicast enabled can maintain one TTL threshold for every interface. If the TTL of the multicast packet received is greater than the threshold of the interface, the packets will be forwarded. Otherwise, the packet is discarded. Note that the TTL threshold is effective only to the multicast frames. In addition, you must configure it on the L3 interface. When TTL threshold is 0, the data flow will not go through the correspondent interface.

Examples

The following example sets the TTL threshold on the interface to 5.

```
DES-7210(config-if)# ip multicast ttl-threshold 5
```

41.1.6 ip multicast-routing

Use this command to enable multicast routing forwarding. The **no** form of this command disables multicast routing forwarding.

ip multicast-routing

no ip multicast-routing

Default

Disabled.

Command mode

Global configuration mode.

Usage guideline	This command allows you to enable IPv4 multicast routing forwarding. The multicast protocol will not be enabled with IPv4 multicast routing forwarding disabled. **Note:** For DES-7200 series, the IPv4 multicast routing forwarding and SVGL, IVGL-SVGL modes of IGMP SNOOPING are exclusive. You shall ensure that the SVGL, IVGL-SVGL modes of IGMP SNOOPING are disabled before enabling the multicast routing forwarding, or it prompts: `ip multicast-routing conflicts with SVGL mode of IGMP SNOOPING!` The IPv4 multicast routing forwarding can be co-used with the IGMP SNOOPING IVGL mode, but the source IP check function cannot be enabled.
Examples	This command enables multicast routing forwarding. `DES-7210(config)# ip multicast-routing`

Note It is not recommended to configure different v4 multicast routing protocols on different interfaces of a device.

41.1.7 ip multicast-rpf

Use this command to configure the RPF checking mode of the multicast route.

ip multicast-rpf *rpf-mode*

no ip multicast-rpf

Parameter description

Parameter	Description
rpf-mode	Routed-port: Check the routed port by the upstream interface; SVI: Check the SVI by the upstream interface.

Default	The default mode is SVI.
Command mode	Global configuration mode.

41.1.8 ip multicast boundary

Use this command to configure the boundary of an IP multicast group. The **no** form of this command removes the configured boundary.

ip multicast boundary *access-list*

no ip multicast boundary *access-list*

Parameter description

Parameter	Description
access-list	Access list associated with the multicast boundary.

Default

The boundary of a specified IP multicast group is defined by default.

Command mode

Interface configuration mode

Usage guideline

Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IP address.

Note:

This command filters IGMP and PIMSM packets of the specified IP address range. Multicast packets will not be received and sent through the interface of the boundary.

Examples

The following example configures svi1 as the boundary of all IP multicast groups.

```
DES-7210(config)# ip access-list mul-boun
DES-7210(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255
DES-7210(config-std-nacl)#exit
DES-7210(config)# interface vlan 1
DES-7210(config-if)# ip multicast boundary mul-boun
```

41.1.9 ip multicast static

Use this command to enable flow control for multicast packets on the Layer 2 interface. The **no** form of this command removes the setting.

ip multicast static *source-address group-address interface-type interface-number*

no ip multicast static *source-address group-address interface-type interface-number*

Parameter description

Parameter	Description
source-address	Source IP address
group-address	IP address of the multicast group
interface-type interface number	Layer 2 interface on which multicast packets are allowed to forward

Default

Disabled

Command mode

Global configuration mode

Usage guideline

You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces.

This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-DM or PIM-SM) may be affected because some features of the multicast protocol are driven by multicast flows.

Examples

The following example configures forwarding multicast flows (192.168.43.4 and 255.1.1.5) through GigabitEthernet 2/6 and FastEthernet 3/2.

```
DES-7210(config)# ip multicast static 192.168.43.4 225.1.1.5 G2/6
DES-7210(config)# ip multicast static 192.168.43.4 225.1.1.5 F3/2
```

41.2 Show Related Commands

41.2.1 show ip mroute

Use this command to show the multicast forwarding table.

show ip mroute [*group-address*] [*source-address*] [**dense**] [**sparse**] [**summary**] [**count**]

Parameter description

Parameter	Description
group-address	Multicat group IP address
source-address	Multicast source IP address
dense	Show PIM-DM multicast routing table.
sparse	Show PIM-SM multicast routing table.
summary	Show the summary of the multicast routing table.
count	Show the count of the multicast routing table.

Command mode

Privileged mode.

Examples

The following example shows the information of the multicast routing table:

```
DES-7210# show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires
00:02:59
Owner PIM-SM, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example shows the information of a specific entry:

```
DES-7210# show ip mroute 10.10.1.52 224.0.1.3
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires
```

```
00:01:28
Owner PIM-SM, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example shows the count of the routing table:

```
DES-7210# show ip mroute count
IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10
Forwarding Counts: Pkt count/Byte count, Other Counts:
Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat
sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following example shows the summary of the routing table:

```
DES-7210# show ip mroute summary
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM,
Flags: T
```

Field	Description
Flags	I-Immediate statistic T-Timed statistic F-Already set to the forwarding tabl
Timers:Uptime/Stat Expiry	Time when the entry is created. Time when it is aged.
Interface State	Interface state.

Owner	Owner of the entry, which may be a multicast routing protocol
Incoming interface	Expected packet incoming interface. If the actual incoming interface does not match it, the packets will be discarded.
Outgoing interface list	Outgoing interface list; the packets will be forwarded on the interfaces in the list.
Forwarding Counts: Pkt count/Byte count,	Forwarding count: packet count/byte count forwarded by the entry
Other Counts: Wrong If pkts	Count of the packets received from the wrong incoming interface.

Related commands

Command	Description
ip multicast-routing	Enabling the multicast routing forwarding.
ip pim dense-mode	Enable the PIM-DM on the interface.
ip pim sparse-mode	Enable the PIM-SM on the interface.

41.2.2 show ip rpf

Use this command to show the RPF information of the specified source IP address.

show ip rpf {*source-address*}

Parameter description

Parameter	Description
source-address	Specified source IP address

Command mode

Privileged mode.

Examples

The following example shows the information of the RPF to 192.168.1.54:

```
DES-7210# show ip rpf 192.168.1.54
RPF information for 192.168.1.54
RPF interface: VLAN 1
```

```
RPF neighbor: 0.0.0.0
RPF route: 192.168.1.0/24
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0 RPF information for 192.168.1.54
RPF interface: VLAN 1
RPF neighbor: 0.0.0.0
RPF route: 192.168.1.0/24
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0
```

41.2.3 show ip mvif

Use this command to show the basic information of the multicast interface.

show ip mvif { *interface-type interface-number* }

Parameter description

Parameter	Description
interface-type interface-number	Interface Type and number

Command mode

Privileged mode.

Examples

The following example shows the basic information of the multicast interface of **svil**.

```
DES-7210#show ip mvif vlan 1
Interface    Vif   Owner    TTL  Local     Remote       Uptime
             Idx   Module    Address       Address
VLAN 1       1    PIM-DM     2   192.168.1.1   0.0.0.0    00:13:16
```

41.3 Debugging Related Commands

41.3.1 debug nsm mcast all

Use this command to turn on all multicast debugging switches. The **no** form of this command turns off all the debugging switches.

debug nsm mcast all

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	Turning on all multicast debugging switches to check related running process.
Examples	The following example turns on all the multicast debugging switches. `DES-7210# debug nsm mcast all`

41.3.2 debug nsm mcast fib-msg

Use this command to turn on the fib-msg debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast fib-ms

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the fib-msg debugging switch. `DES-7210# debug nsm mcast fib-msg`

41.3.3 debug nsm mcast vrf

Use this command to turn on the VRF debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast vrf

Default	Disabled

Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the VRF debugging switches. `DES-7210# debug nsm mcast vrf`

41.3.4 debug nsm mcast register

Use this command to turn on the register debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast register

Default	Disabled
Command mode	Privileged EXEC configuration mode
Usage guideline	N/A
Examples	The following example turns on the register debugging switches. `DES-7210# debug nsm mcast register`

41.3.5 debug nsm mcast stats

Use this command to turn on the interface statistics debugging switch. The **no** form of this command turns off the debugging switch.

debug nsm mcast stats

Default	Disabled
Command mode	Privileged EXEC configuration mode

Usage guideline	N/A
Examples	The following example turns on the interface statistics debugging switches. `DES-7210# debug nsm mcast stats`

42 MPLS Configuration Commands

42.1 Basic MPLS Commands

42.1.1 advertise-labels for

Use this command to set the advertise-labels for specified routings.

advertised-labels for {**bgp-routes** | **host-routes**}

no advertised-labels for {**bgp-routes** | **host-routes**}

Parameter description

Parameter	Description
bgp-routes	Distribute labels to the valid bgp routes .
host-routes	Only distribute labels to the host routes with 32-bit mask length.

Default configuration

By default, it distributes labels to the IGP routes, not the BGP routes.

Command mode

config-mpls-router mode

Usage guidelines	Use the **advertise-labels for bgp-routes** command to distribute the labels to the BGP routes, making the LDP session disconnect and rebuild. In the network, since BGP carries with many routes and maintains the routes in other autonomous areas which is unecessary to the self-autonomous area, if LDP distributes the labels to the BGP routes, a large amount of the label resources will be used. To this end, LDP does not distribute the labels to the BGP routes by default. However, this command can be used if the user wants to distribute the labels to the BGP routes according to the an actual requirement and advertise to the LDP neighbor. Use the **advertise-labels for host-routes** command to distribute the labels to the route prefix of 35-bit mask(namely the host route), making the LDP session disconnect and rebuild. In some application, it may not be necessary to distribute the labels to all IGP routes and set up LSP. For example, in the MPLS network for transmitting the user service, such as L3VPN, the VPN users in different locations communicate by the MPLS transmission network. In this application, it is not necessary to distribute the labels and set up the LSP in every network segment of the MPLS transmission network, but set up the LSP between the PEs. You can execute the command advertise-labels for host-routes on the PE and P device in the MPLS transmission network to enable the LDP to distribute the labels to the 32-bit host routes and then save the label resources.

Examples	`DES-7210(config)# mpls router ldp` `DES-7210(config-mpls-router)# advertise-labels for bgp-routes`

42.1.2 discovery targeted-hello

Use this command to set the holdtime or interval for the extended peer hello message. Use the **no** form of this command to restore the default value.

discovery targeted-hello {**holdtime|interval**} *seconds*

no discovery targeted-hello {**holdtime|interval**}

Parameter description

Parameter	Description
holdtime	The holdtime of the hello message for the extended mechanism.

	interval	The interval of the hello message for the extended mechanism.
	seconds	Range within 1-65535

Default configuration

By default, the holdtime of the hello message for the extended mechanism is 45s, and the interval of the hello message is 5s, which is 1/9 of the holdtime.

Command mode

config-mpls-router mode

Usage guidelines

For the actual configuration, it is necessary to ensure the holdtime of the target hello is larger than the interval value. Otherwise, LDP can not work normally according to the requirement. Note that this command is valid for the targeted hello used by the extended discovery mechanism only.

Examples

```
DES-7210(config)# mpls route ldp
DES-7210(config-mpls-router)# discovery target-hello holdtime 90
```

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute

42.1.3 label-merge

Use this command to enable global label merge. Use the **no** form of this command to disable this function.

[**no**] **label-merge**

Default configuration	Enabled.
Command mode	**config-mpls-router** mode.
Usage guidelines	In the DU advertise control mode, label merge cannot be disabled. This command configuration resets the LDP session.
Examples	`DES-7210(config)# mpls route ldp` `DES-7210(config-mpls-router)# label-merge`

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute
mpls ldp distribution-mode	Configure the label distribution mode used for each interface.

42.1.4 label-retention-mode

Use this command to set the label retention mode. Use the **no** form of this command to restore the default value.

label-retention-mode {liberal | conservative}

[no] label-retention-mode

Parameter description

Parameter	Description
liberal	Use the liberal label retention mode
conservative	Use the conservative label retention mode

Default configuration	Use the liberal label retention mode
Command mode	**config-mpls-router** mode
Usage guidelines	Use this command to reset and rebuild the LDP session.
Examples	`DES-7210(config)# mpls route ldp` `DES-7210(config-mpls-router)# label-retention-mode liberal`

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute

42.1.5 label-switching

When the MPLS multi-service card is used to forward the MPLS service, use this command to enable the interface to process the MPLS label message.

[**no**] **label-switching**

Default configuration	For the equipment which uses the MPLS multi-service card to forward the MPLS service, its interface can not process the MPLS label message by default.
Command mode	Interface configuration mode.

Usage guidelines

This command is valid only for the equipment which uses the MPLS multi-service card(7200-ASE3) to forward the MPLS service.

Examples

```
DES-7210(config)# interface Gi4/1
DES-7210(config-if)# label-switching
```

Related commands

Command	Description
show mpls label-pool	Show the usage of the label pool in each label space

42.1.6 ldp router-id

Use this command to set the LSR ID of the LDP. Use the **no** form of this command to restore the default value.

[**no**] **ldp router-id** *A.B.C.D*

Parameter description

Parameter	Description
A.B.C.D	The configured IP address

Default configuration

Use Router ID as the LDP LSR ID.

Command mode

config-mpls-router mode

Usage guidelines

The value of **ldp router-id** should ensure the global unique. For the LDP uses **ldp router-id** as **transport-address** by default, it is necessary to ensure the **ldp router-id** is route reachable for other LSRs.

Examples

```
DES-7210(config-mpls-router)# ldp router-id 10.10.10.30
```

Related commands

Command	Description
show mpls ldp parameter	Show all LDP global configuration attributes

42.1.7 loop-detection

Use this command to enable loop detection. Use the **no** form of this command to disable loop detection.

[no]loop-detection

Default configuration

Disabled.

Command mode

config-mpls-router mode

Usage guidelines

Use this command to reset and rebuild the LDP session.

Examples

```
DES-7210(config)# mpls router ldp
DES-7210(config-mpls-router)# loop-detection
```

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute
mpls ldp max-path-vector	Configure the maximum path vector allowed for LDP loop detection

	mpls ldp max-hop-count	Configure the maximum hop count allowed for LDP loop detection

42.1.8 lsp-control-mode

Use this command to set the LDP control mode globally. Use the **no** form of this command to restore the default value.

lsp-control-mode [**independent** | **ordered**]

no lsp-control-mode

Parameter description

Parameter	Description
independent	Use the independent control mode
ordered	Use the ordered control mode

Default configuration

Independent control mode

Command mode

config-mpls-router mode

Usage guidelines

Use this command to reset and rebuild the LDP session.

Examples

```
DES-7210(config)# mpls router ldp
DES-7210(config-mpls-router)# lsp-control-mode ordered
```

Related

Command	Description

commands	**show mpls ldp parameters**	Show the LDP global configuration attribute

42.1.9 mpls ip (Global configuration mode)

Use this command to enable the MPLS forward in the global configuration mode. Use the **no** form of this command to disable MPLS forward.

[no] mpls ip

Default configuration	The MPLS forward is not enabled.
Command mode	Global configuration mode.
Usage guidelines	To implement the mpls forward, it is necessary to enable the MPLS globally firstly. This command is invalid for the mpls forward on the switch. After the mpls forward is disabled by the process forward, the switch can not send and receive the MPLS messages.
Examples	`DES-7210(config)# mpls ip`

Related commands	**Command**	**Description**
	mpls ip	Enable the MPLS in the interface configuration mode.

42.1.10 mpls ip (Interface configuration mode)

Use this command to enable the MPLS forward and the LDP functions in the interface configuration mode. Use the no form of this command to disable the LDP function to terminate the MPLS forward.

[**no**] **mpls ip**

Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	For the interface which doesn't use the MPLS multi-service card to forward the MPLS service, the MPLS forward function is disabled by default. Therefore, you must use this command to enable the MPLS forward function, and the LDP function on the interface is enabled automatically at the same time. If the LDP function is not enabled on this interface, it can not use the LDP to set up the LSP. It only allows enable the MPLS function on the L3 interface.
Examples	`DES-7210(config)# interface Gi4/1` `DES-7210(config-if)# mpls ip`

Related commands

Command	Description
mpls ldp hello-interval	Configure the interval for sending hello messages
mpls ldp hello-holdtime	Configure the hello packet holdtime

42.1.11 mpls ip fragment

Use this command to set the processing if it exceeds the MPLS MTU after the IP message is encapsulated with the MPLS label.

[no] mpls ip fragment

Default configuration	After the entered IP packet is encapsulated with the MPLS label, if its size exceeds the defined size of the MPLS MTU, it will carry out the fragment to the original IP packet before the MPLS label is encapsulated to send.

Command mode	Global configuration mode.
Usage guidelines	This command is valid only for the process forward. Use the **no mpls ip fragment** command to disable the fragment function for process forward. Namely, it will be discarded directly if its size exceeds the defined size of the MPLS MTU after the entered IP packet is encapsulated with the MPLS label.
Examples	`DES-7210(config)# no mpls ip fragment`

Related commands

Command	Description
mpls ip	Enable MPLS globally..

42.1.12 mpls ip icmp forward

For the ICMP error message generated by multiples layers (larger than or equal to 2) of labels, it will be forwarded until the PE returns to the source terminal.

mpls ip icmp forward

no mpls ip icmp forward

Default configuration	The multi-layer lable will not generate the ICMP error message by default.
Command mode	Global configuration mode.

Usage guidelines	For the IP packet encapsulated by multiples layers (larger than or equal to 2) of labels, the generated ICMP error message will forward until the PE returns to the source terminal. By default, the IP packet of the multiples layers (greater than or equal to 2) of labels will not generate the ICMP error message. This command is valid only for the process forward.

Examples	`DES-7210(config)# mpls ip icmp forward`

Related commands

Command	Description
mpls ip	Enable MPLS globally.

42.1.13 mpls ip ttl expiration

Use this command to set the generated ICMP timeout error message to be forwarded along the local IP route if the TTL of the label message is timeout when it is forwarded within MPLS network.

mpls ip ttl expiration

no mpls ip ttl expiration

Default configuration	By default, it will return the ICMP message according to the local IP route for the MPLS TTL timeout message of the L1 label, and it will be discarded directly for the multiple layers of labels. This command is valid only for the process forward.

Command mode	Global configuration mode.

Usage guidelines	It will use the **no mpls ip ttl expiration** command to discard the message timeout directly when setting the MPLS TTL.

Examples	`DES-7210(config)# no mpls ip ttl expiration`

Related commands

Command	Description
mpls ip	Enable MPLS globally.

42.1.14 mpls ip ttl propagate

Use this command to enable or disable the IP TTL copy function of the MPLS.

mpls ip ttl propagate {**public** | **vpn**}

no mpls ip ttl propagate

Parameter description

Parameter	Description
public	Specify whether to enable TTL copy function or not for the sending messages.
vpn	Specify whether to enable TTL copy function or not for the forwarding messages.

Default configuration	By default, it enables TTL copy function for both the sending and forwarding messages.
Command mode	Global configuration mode

Usage guidelines

The following are two modes of MPLS TTL:

- TTL copy mode: it is the default working mode. In this mode, the pushed label TTL is copied from the TTL of the existed head of the IP packet or the MPLS packet when Pushing the label. The TTL of the internal IP packet or the MPLS packet is copied from the TTL of the external label when Popping the label.
- TTL non-copy mode: in this mode, set the value of pushed label TTL to 255 when Pushing the label and keep the value of the TTL of the internal IP packet or the MPLS packet when Popping the label.

Examples

The following example disables the TTL copy function of the forwarding message:

```
DES-7210(config)# mpls ip ttl propagate public
```

Related commands

Command	Description
mpls ip	Enable MPLS globally.

42.1.15 mpls ldp distribution-mode

Use this command to set the label distribution mode used by LDP on each interface. Use the **no** form of this command to restore the default value.

mpls ldp distribution-mode {**dod | du**}

no mpls ldp distribution-mode

Parameter description

Parameter	Description
dod	Use the downstream on-demand distribution mode
du	Use the downstream active distribution mode

Default configuration	Use the downstream active distribution mode.
Command mode	Interface configuration mode.
Usage guidelines	If the interconnected LDP sessions use different distribution modes, the du mode will be used forcibly for both of them. Use this command to reset and rebuild the LDP session.
Examples	`DES-7210(config)# interface vlan 10` `DES-7210(config-if)# mpls ldp distribution-mode dod`

Related commands

Command	Description
loop detection-mode	Configure loop detection

42.1.16 mpls ldp hello-holdtime

Use this command to configure the holdtime in seconds for LDP hello packets on each interface. Use the **no** form of this command to restore the default value.

[**no**] **mpls ldp hello-hellotime** <*1-65535*>

Parameter description

Parameter	Description
<*1-65535*>	Holdtime of hello messages, in seconds. Holdtime 65535 stands for the hello messages will never timeout.

Default configuration	15 seconds

Command mode	Interface configuration mode.
Usage guidelines	This command is valid only for the LDP Link Hello for the basic discovery mechanism and possible lead to changes of interval of sending Hello messages. Use **discovery targeted-hello** command to set the hello holdtime for the exteded discovery mechanism.
Examples	`DES-7210(config)# interface vlan 10` `DES-7210(config-if)# mpls ldp hello-holdtime 30`

Related commands

Command	Description
mpls ldp hello-interval	Configure the interval for sending hello messages
discovery targeted-hello	Configure the interval and timeout time of sending hello messages for the extended discovery mechanism.

42.1.17 mpls ldp hello-interval

Use this command to configure the holdtime in seconds for LDP hello packets on each interface. Use the **no** form of this command to restore the default value.

mpls ldp hello-interval <*1-65535*>

no mpls ldp hello-interval

Parameter description

Parameter	Description
<*1-65535*>	Send the interval for hello messages, in second.

Default configuration	5 seconds
Command mode	Interface configuration mode.
Usage guidelines	For the actual configuration, it should ensure this value is less than the value of hello-holdtime. Otherwise, the LDP can not work normally according to the requirement. This command is valid only for the LDP Link Hello for the basic discovery mechanism. Use **discovery targeted-hello** command to set the hello holdtime for the extended discovery mechanism.
Examples	`DES-7210(config)# interface vlan 10` `DES-7210(config-if)# mpls ldp hello-interval 10`

Related commands

Command	Description
mpls ldp hello-holdtime	Configure the hello packet holdtime
discovery targeted-hello	Configure the interval and timeout time of sending hello messages for the extended discovery mechanism.

42.1.18 mpls ldp keepalive-holdtime

Use this command to configure the holdtime for keepalive packets on each interface. Use the **no** form of this command to restore the default value.

mpls ldp keepalive-holdtime <*15-65535*>

no mpls ldp keepalive-holdtime

Parameter

Parameter	Description

description	*<15-65535>*	Holdtime of keepalive messages, in second.

Default configuration	45 seconds
Command mode	Interface configuration mode.
Usage guidelines	This command is valid for the LDP session to be built, not for the built LDP session. This command execution has no influence on the LDP session set up by the extended discovery mechanism. Use the targeted-session holdtime command to modify the Keepalive Holdtime of the LDP session set up by the extended discovery mechanism.
Examples	`DES-7210(config)# interface vlan 10` `DES-7210(config-if)# mpls ldp keepalive-holdtime 90`

Related commands

Command	Description
targeted-session holdtime	Set the holdtime of keepalive messages for the extended mechanism.

42.1.19 mpls ldp max-hop-count

Use this command to configure the maximum hop count allowed for loop detection on each interface. Use the **no** form of this command to restore the default value.

mpls ldp max-hop-count *<1-255>*

no mpls ldp max-hop-count

Parameter

Parameter	Description

description	*<1-255>*	Maximum hop count allowed for loop detection.

Default configuration

The default value is 254.

Command mode

Interface configuration mode.

Usage guidelines

The hop count value is valid with the loop detection configured. If the hop count value in the label mapping message or the label request message of LDP is greater than the configured value, it is deemed that a loop occurs. This command is invalid for the label mapping message and label request message received previously, but valid for the ones received later.

Examples

```
DES-7210(config)# interface vlan 10
DES-7210(config-if)# mpls ldp max-hop-count 30
```

Related commands

Command	Description
loop-detection-node	Configure LDP loop detection

42.1.20 mpls ldp max-label-requests

Use this command to configure the maximum label requests allowed on each interface. Use the **no** form of this command to restore the default value.

mpls ldp max-label-requests *<0-255>*

no mpls ldp max-label-requests

Parameter

Parameter	Description

description	*<0-255>*	Maximum request times

Default configuration

The default value is 0, meaning that the label requests will not be retransmitted.

Command mode

Interface configuration mode.

Usage guidelines

This command is invalid for the label request times in the built LDP session on the interface, and valid for newly-built LDP session. The value 0 means that the label requests will not be retransmitted.

Examples

```
DES-7210(config)# interface vlan 10
DES-7210(config-if)# mpls ldp max-label-requests 5
```

Related commands

Command	Description
mpls-ldp-distribution-mode	Configure the label distribution mode

42.1.21 mpls ldp max-path-vector

Use this command to configure the maximum path vector value allowed for loop detection on each interface. Use the **no** form of this command to restore the default value.

mpls ldp max-path-vector *<0-254>*

no mpls ldp max-path-vector

Parameter description

Parameter	Description
<0-254>	Maximum path vector value

Default configuration	The default value is 254.
Command mode	Interface configuration mode.
Usage guidelines	The path vector value is valid with the loop detection of the LDP instance enabled. If the LDR ID number, that is in the path vector list of the label mapping message or the label request message of LDP, is greater than the configured value, it is deemed that a loop occurs. This command is invalid for the built LDP session, but influences the LDP session to be built.
Examples	`DES-7210(config)# interface vlan 10` `DES-7210(config-if)# mpls ldp max-path-vector 10`

Related commands

Command	Description
loop-detection	Set LDP loop detection.

42.1.22 mpls ldp max-pdu

Use this command to configure the maximum PDU value. Use the **no** form of this command to restore the default value.

mpls ldp max-pdu *<256-4096>*

no mpls ldp max-pdu

Parameter description

Parameter	Description
<256-4096>	The maximum PDU length value when exchanging the LDP messages, in bytes.

Default configuration	The default value is 4096.
Command mode	Interface configuration mode.
Usage guidelines	Using this commang cannot influence the LDP session built or to be built on the interface.
Examples	`DES-7210(config)# interface vlan 10` `DES-7210(config-if)# mpls ldp max-pdu 256`

42.1.23 transport-address

Use this command to set the global transport address. Use the **no** form of this command to restore the default value.

[no] transport-address [**interface** | *ipaddr* | *interface_name*]

Parameter description

Parameter	Description
interface	Use the IP address of the corresponding interface as the transmission address for the session on each interface.
ipaddr	All sessions use this specified IP address as the transmission address uniformly.
interface _name	All sessions use this master IP address of the specified interface as the transmission address uniformly.

Default configuration	Use the LSR ID of LDP as the transport-address.

Command mode	**config-mpls-router** mode.

Examples

```
DES-7210(config-mpls-router)# transport-address 192.168.0.1
```

Related commands

Command	Description
show mpls ldp parameters	Show all LDP parameters globally.

42.1.24 mpls mtu

Use this command to configure the MTU value when the MPLS messages are forwarded.

mpls mtu <*64-6535*>

no mpls mtu

Parameter description

Parameter	Description
<*64-65535*>	The mtu value supported by the interface, in byte.

Usage guidelines	The path vector value is valid with the loop detection of the LDP instance enabled. If the LDR ID number, that is in the path vector list of the label mapping message or the label request message of LDP, is greater than the configured value, it is deemed that a loop occurs. This command is invalid for the built LDP session, but influences the LDP session to be built.
Default configuration	The MPLS MTU value equals to the interface MTU and the length of 2 labels.

Command mode	Interface configuration mode.
Usage guidelines	To configure the MPLS MTU on the interface, by default, the transmittable MTU of the MPLS label message is the interface MTU plus 8 bytes. The MPLS MTU determines whether to fragment the MPLS message during the message sending. The length of the MPLS MTU includes the total length of the MPLS encapsulating and encapsulated(IP) layer. The MPLS MTU on the interface must not exceed the actual transmitted units. This command is valid for the process forward only. The switch hardware forwards the messages according to the configured MTU on the interface and discards the messages that exceed the confgured MTU. Use the **mtu** command in the interface configuration mode to adjust the MTU on the interface.
Examples	`DES-7210(config)# interface Gi4/1` `DES-7210(config-if)# mpls mtu 1510`

Related commands

Command	Description
mpls ip	Enable the MPLS globally.

42.1.25 mpls router ldp

Use this command to enable LDP, use the **no** form of this command to disable LDP.

[no] mpls router ldp

Default configuration	Disabled
Command mode	Global configuration mode.

Examples	DES-7210(config)# **mpls router ldp** DES-7210(config-mpls-router)#

42.1.26 mpls static ftn

Use this command to allow you to add one FTN entry to the global FTN table. Use the **no** form of this command to delete the specified FTN entry from the FTN table.

mpls static ftn *A.B.C.D*/*Mask* **out-label** *label* **nexthop** *interface-name nexthop-ip*

no mpls static ftn *A.B.C.D/Mask*

Parameter description

Parameter	Description
A.B.C.D/*Mask*	Corresponding **FEC**, namely the destination address.
out-label *label*	Corresponding out-label of this **FEC**.
nexthop *interface-name* *nexthop-ip*	The next hop of this **FEC**, including the egress and the ip address of the next hop.

Command mode

Global configuration mode.

Usage guidelines

This command allows you to add an FTN entry to the FTN table. After the router with MPLS enabled receives an IP packet, it looks up for the next hop in the FTN table according to the destination address of the IP packet according to maximum match. If the next hop is found, it performs label forwarding to the IP packet.For the FTN whose destination and mask is 0, it is valid only when this default route exists in the IP route forwarding table.

Examples

DES-7210(config)# **mpls static ftn** *192.168.0.0/16* **out-label** *100* **nexthop** *gi4/1 10.10.10.1*

Related commands	Command	Description
	show mpls forwarding-table	Show the overview information of the global FTN table

42.1.27 mpls static l3vpn-ftn

Use this command to add the FTN of one L3 VPN. Use the **no** form of this command to delete this FTN.

mpls static l3vpn-ftn *vrf-name A.B.C.D/Mask* **out-label** *label* **remote-pe** *ip-addr*

mpls static l3vpn-ftn *vrf-name A.B.C.D/Mask* **local-forward nexthop interface** *nexthop-ip*

no mpls static l3vpn-ftn *vrf A.B.C.D/Mask*

Parameter description	Parameter	Description
	vrf-name	Specify the name of the VRF whose FTN table to which the FTN entry is to be added
	A.B.C.D/Mask	***Fec, namely the destination network.***
	out-label *label*	It indicates that the corresponding private network FTN should reach to other PE forwarding through the LSP tunnel. At the same time, it will be specified with the private network label used for the forward.
	remote-pe *ip-addr*	The address of the egress PE.
	local-forward nexthop *interface-name nexthop-ip*	It indicates that the corresponding private network FTN will be forwarded to the next hop by this PE directly. At the same time, it will specify the egress of the next hop and the IP address.

Command mode	Global configuration mode.

Usage guidelines	This command allows you to add an FTN entry to the FTN table specified by the vrf-name. After the router with MPLS enabled receives an IP packet, it looks up for the next hop in the FTN table according to the destination address of the IP packet according to maximum match. If the next hop is found, it performs label forwarding to the IP packet. For the FTN whose destination and mask is 0, it is valid only when this route exists in the IP route forwarding table.
Examples	DES-7210 (config)# **mpls static l3vpn-ftn** *192.168.0.0/16* **out-label** *100* **remote-pe** *10.10.10.1*

Related commands

Command	Description
show mpls forwarding-table	Show the overview information of the global FTN table

42.1.28 mpls static l2vc-ftn

Use this command to configure one static VC FTN item. Use the **no** form of this command to to delete the configured FTN item.

mpls static l2vc-ftn *vc-id vc-peer-ip* **out-label** *label*

no mpls static l2vc-ftn *vc_id vc_peer_ip*

Parameter description

Parameter	Description
vc-id	The id of the VC instance.
vc-peer-ip	The IP address at another PE of Vc.
out-label *label*	Used for the private network egress label when this VC FTN is forwarded.

Command mode	Global configuration mode.

Usage guidelines	This command is used to create one ftn item for the vc instance. After the frame is received from the AC binding with this VC, it will be stamped with the private network label for the data frame according to the content of this ftn item, and find the LSP that reaches the peer PE according to the vc peer ip, and then forward the frame.

Examples

```
DES-7210(config)# mpls static l2vc-ftn 1 10.10.10.1 out-label 21
```

Related commands

Command	Description
show mpls l2vc ftn-table	Show the ftn table item of all VC instances.
show mpls forwarding-table	Show the forwarding table item of the MPLS.

42.1.29 mpls static ilm in-label

Use this command to add one ILM table item to the ILM table. Use the **no** form of this command to delete the configured ILM item.

mpls static ilm in-label *in-label* **forward-action swap-label** *label* **nexthop** *interface-name nexthop-ip* **fec** A.B.C.D/Mask

mpls static ilm in-label *in-lab*el **forward-action pop-l3vpn-nexthop** *vrf-name* **nexthop** *interface-name nexthop-ip* **fec** *A.B.C.D/Mask*

mpls static ilm in-label *in-label* **forward-action pop-l2vc-destport** *interface-name* **fec** *vc-id*

no mpls static ilm in-label *in-label*

Parameter description

Parameter	Description
In-label	The ingress label value of this ILM table item.
forward-action	Specify the forward behavior of this ILM table item. **swap-label:** apply to the ILM table item of the public network, to indicate the label switching and forward. **pop-l3vpn-nexthop:** apply to the ILM table

	item of the L3 VPN, to indicate the pop-up label, and forward it to the next hop of the specified VRF. **pop-l2vc-destport:** apply to the ILM table item of the L2 VPN, to indicate the pop-up label, and forward the message from the specified interface.
label	For the **swap-label** forward behavior, it will specify the egress label value of the switched label value.
vrf-name	For the **pop-l3vpn-nexthop** forward behavior, it will specify the VPN of the specified ILM, namely VRF.
Interface-name	For the **pop-l2vc-destport** forward behavior, it will specify the forwarded egress.
nexthop *interface-name nexthop-ip*	Specify the next hop, including the egress and the IP address of the next hop.
fec	Indicate this ILM is created for which FEC.
A.B.C.D/Mask	Correspond to the fec format of the global or **l3 vpn** application, to indicate one destination network.
vc-id	Correspond to the fec format of the **l2vpn** application, to indicate the VC instance.

Command mode	Global configuration mode.
Usage guidelines	This command allows you to add an ILM entry to the ILM table. After the router with MPLS enabled receives an IP packet with label, it looks up for the next hop in the ILM table according to the label of the IP packet according to maximum match. If the next hop is found, it swaps, pops up the label of the IP packet or performs VPN forwarding after pop-up.

Examples

```
DES-7210 (config)# mpls static ilm in-label 20 forward-action
swap-label 30 nexthop gi4/2 10.10.10.1 fec 172.16.0.0/26
```

Related commands

Command	Description
show mpls forwarding-table	Show the information of the MPLS forwarding table.

42.1.30 neighbor

Use this command to create a ldp extended peer. Use the **no** form of this command to delete the ldp extended peer.

[no] neighbor *A.B.C.D*

Parameter description

Parameter	Description
A.B.C.D	The Router ID of the peer LSR.

Default configuration

There is no LDP extended peer by default.

Command mode

config-mpls-router mode.

Usage guidelines

To set up a extended LDP session, the both ends of the LSR of the session to be built must be configured. It fails to set up the extended LDP session if the extended peer is configured at only one end.

Examples

```
DES-7210(config)# mpls router ldp
DES-7210(config-mpls-router)# neighbor 10.10.10.1
```

Related commands

Command	Description
show mpls ldp discovery	Show the information of neighbor discovered by the LDP.
show mpls ldp neighbor	Show the LDP session state.

42.1.31 propagate-release

Use this command to enable label release. Use the **no** form of this command to disable this function with no label release messages transmitted.

[**no**] **propagate-release**

Default configuration

Disabled

Command mode

config-mpls-router mode.

Usage guidelines

This command execution does not influence the label release messages previously received from the LDP instance, only the ones received later.

Examples

```
DES-7210(config)# mpls router ldp
DES-7210(config-mpls-router)# propagate-release
```

Related commands

Command	Description
show mpls ldp parameters	Show the LDP global configuration attribute

42.1.32 show mpls forwarding-table

Use this command to show the MPLS forwarding table.

show mpls forwarding-table [[[*A.B.C.D MASK*] [**label** *label*] [**interface** *interface-name*] [**next-hop** *A.B.C.D*] [[**ftn** [**ip** | **vc** | **detail**]]|[[ ]] | [[**ilm**] [ ] [**ip | vc** | **detail**]]]|[ ]]] | [**detail**]|[ ] | [**vrf** *vrf-name*]|] | [**summary**]

Parameter description

Parameter	Description
A.B.C.D/mask	Show ILM and FTN entry of the specified FEC.
label *label*	Show ILM entry of the specified label.
interface *interface-name*	Show the MPLS forward entry(ILM and FTN) of the specified egress port.
next-hop *A.B.C.D*	Show the MPLS forward entry(ILM and FTN) of the specified next-hop address.
ftn	Show to forward the mapping table item of the forwarding equivalence class
ilm	Show the mapping table item of the egress label.
vc	Show the MPLS forwarding table item added by the vc.
ip	Show the MPLS forwarding table item generated by the ip route.
detail	Show the detailed information of the mpls forwarding table item.
vrf	Show the MPLS forwarding table item related to some VRF.
summary	Show the statistics information of the MPLS process forwarding

Command mode	User mode, privileged user mode
Usage guidelines	This command shows the MPLS forwarding path, including the FTN table and ILM table.

Examples

```
DES-7210# Show mpls forwarding-table
Local  Outgoing   Prefix  Outgoing      Next Hop
tag    tag or VC    or Tunnel Id       interface
--IP forward   120.1.1.0/24  GigabitEthernet 3/19  0.0.0.0
--IP forward 167.168.195.0/24 GigabitEthernet 3/19 120.1.1.10
```

Local tag: The label distributed by this forwarding equivalence class equipment to other equipments. It will not show for the void label.

Outgoing tag or VC: This forwarding equivalence class sends the message encapsulation label locally. At present, the existing operation includes:

PUSH: It is necessary to add the label when the message is sent by this equipment.

POP: It is necessary to pop up the label when the message is sent by this equipment.

SWAP: It is necessary to switch the label when the message is sent by this equipment.

POP IP: It is necessary to pop up the label when the message is sent by this equipment, and carry out the IP forwarding.

POP L2PORT: It is necessary to pop up the label when the message is sent by this equipment, and carry out the forwarding by the L2 port (VPLS).

POP VC: It is necessary to pop up the label when the message is sent by this equipment, and carry out the forwarding by the specified interface (VPWS).

IP forward: The IP message is forced to continue the IP forwarding after it carries out the MPLS process by this equipment.

DROP: The message is discarded directly by this equipment.

Prefix or Tunnel Id: The forwarding equivalence class, IP address and mask. For the tunnel, it is the endpoint address of the tunnel.

Outgoing interface: The outgoing interface of the message forwarding.

Next Hop: The next hop of the message forwarding, the next hop is 0, to indicate the local direct interconnection network.

```
DES-7210# sh mpls forwarding-table summary
MPLS forwarding is ON
Enable count:1
```

```
ILM entrys:14
ILM changes:14
ILM failed changes :0
IP FTN entrys:0
IP FTN changes:4
IP FTN faild changes:0
L2 FTN entrys:0
L2 FTN changes:0
L2 FTN faild changes:0
In label packets:0
Out label packets:0
Send label packets:0
In ip packets:0
Out ip packets:0
Out ip statck packets:0
Forwarding packets:0
Fragment packets:0
Fragment error packets:0
Label error packets:0
Label failed packets:0
Ttl over packets:0
Buffer failed packets:0
Ip don't fragment packets:0
Other failed packets:0
```

42.1.33 show mpls label-pool

Use this command to show the usage of the label pool in various label spaces. You can show the data of all the label spaces, or that of a specific label space by specifying a label space number.

show mpls label-pool [*label-space*]

Parameter description

Parameter	Description
label-space	Specify the label-space whose label pool is to be shown.

Command mode

Privileged user mode.

Usage guidelines	This command allows you to show the usage of the label pool of all label spaces or a specific label space, including label pool size, maximum/minimum label value, and allocation of each label pool.

Examples

```
DES-7210# show mpls label-pool
label space: 0
label pool bucket size 512
min label 16, max label 1048575
label block used 2, free 2046
CLI:    0,    1    (Include label [16,1023], reserved)
LDP:    3,    4
```

Related commands

Command	Description
label-switching	Enable label switching

42.1.34 show mpls ldp bindings

Use this command to show the LDP label database information.

show mpls ldp bindings

Command mode	Privileged user mode.
Usage guidelines	This command shows the FEC and label binding information. This command allows you to view the working status of the LDP, whether the LDP has normally bound the FEC, as well as the specific label value of a specific FEC binding, whether a local binding or remote binding.

Examples

```
DES-7210# show mpls ldp bindings
169.254.0.0/16  remote binding:  no outlabel lsr: 192.168.0.2:0
192.168.0.1/32  remote binding:  label: gen 640 lsr: 192.168.0.2:0
ingress
```

```
192.168.0.2/32  remote binding:  label: gen impl-null
lsr: 192.168.0.2:0 ingress
192.168.3.0/24  remote binding:  label: gen impl-null
lsr: 192.168.0.3:0 ingress
192.168.4.0/24  remote binding:  no outlabel lsr: 192.168.0.3:0
192.168.0.100/32  local binding:   label: gen impl-null
192.168.4.0/24  local binding:   label: gen impl-null
```

Related commands

Command	Description
show mpls ldp neighbor	Show the LDP session status.

42.1.35 show mpls ldp discovery

Use this command to show the neighbor of LDP discovery.

show mpls ldp discovery

Command mode

Privileged user mode

Usage guidelines

This command allows you to show the interfaces on which the LDP neighbor has been discovered, the LDP neighbors discovered, the hello packet source address of the LDP neighbor, and hello keepalive interval.

Examples

```
DES-7210# show mpls ldp discovery
Local LDP Identifier:
   8.8.8.8:0
   Discovery Sources:
   Interfaces:
      GigabitEthernet 2/1 (ldp): xmit/recv
         LDP Ident: 10.30.10.10:0
      GigabitEthernet 2/2 (ldp): xmit
   Targeted Hellos:
      8.8.8.8 -> 10.5.0.1 (ldp): active, xmit
      8.8.8.8 -> 10.30.10.10 (ldp): active/passive, xmit
```

```
2.2.2.2 -> 10.30.10.10 (ldp): passive, xmit/recv
   LDP Ident: 10.30.10.10:0
```

Local LDP Identifier: The LDP identifier for the local router.

Interfaces: The interface information lists discovered by the active LDP.

Xmit: The Hello messages sent on the interface.

recv: The Hello messages received on the interface. **Targeted Hellos:** The sending path lists for all targeted hello messages.

active: The local LSR sends targeted Hello messages actively.

passive: The neighbor LSR sends targeted Hello messages actively and the local LSR responses.

Related commands

Command	Description
show mpls ldp interface	Show the LDP-enabled interface information.

42.1.36 show mpls ldp neighbor

Use this command to show the LDP neighbor information.

show mpls ldp neighbor

Command mode

Privileged user mode.

Usage guidelines

Show all LDP neighbors including the TCP connection port between the local LDP and peer LDP, LDP status, received/sent message count, ect.

Examples

```
DES-7210# show mpls ldp neighbor
Peer LDP Ident: 10.20.10.10:0; Local LDP Ident: 8.8.8.8:0
      TCP connection: 10.20.10.10.62488 - 8.8.8.8.646
      State: OPERATIONAL; Msgs sent/recv: 42/45; UNSOLICITED
      Up time: 00:33:49
      LDP discovery sources:
        Link Peer on GigabitEthernet 2/1, Src IP addr: 192.168.201.220
```

```
  Targeted Hello 8.8.8.8 -> 10.20.10.10
Addresses bound to peer LDP Ident:
  10.20.10.10   192.168.201.220 192.168.198.1   10.5.0.1
```

Peer LDP Ident: The LDP identifier for the LDP session peer.

Local LDP Identifier: The LDP identifier for the local router.

TCP connection： The TCP connection supported this LDP session.

State: The LDP session state.

Msgs sent/recv: The statistics for the amount of LDP messages which are sent to and received from the session peer.

UNSOLICITED&ONDEMAND: The label distribution mode.

Related commands

Command	Description
show mpls ldp discovery	Show the neighbor information discovered by LDP.

42.1.37 show mpls ldp parameters

Use this command to show the LDP global configuration parameters.

show mpls ldp parameter

Command mode

Privileged user mode.

Usage guidelines

It can show various attribute information of the LDP, including the LSR ID, transport-address, loop detection mechanism, label distribution and control mode, label retention mode, interval and holdtime of the hello message for the extended mechanism as well as the interval and holdtime of the keepalive message.

Examples

```
DES-7210# show mpls ldp parameters
  Protocol version: 1
    Ldp Router ID: 8.8.8.8
```

```
Control Mode: INDEPENDENT
Propogate Release: FALSE
Label Merge: TRUE
Label Retention Mode: LIBERAL
Loop Detection Mode: off
Targeted Session Keepalive HoldTime/Interval: 180/60 sec
Targeted Hello HoldTime/Interval: 90/10 sec
```

Related commands

Command	Description
ldp router-id	Configure the ldp router-id.
lsp-control-mode	Configure the LDP control mode
ldp-label-retention -mode	Configure the label retention mode
propagate-release	Configure the label propagate release
label-merge	Configure the label-merge
loop-detection-mode	Configure loop detection

42.1.38 show mpls ldp session

Use this command to show LDP session information.

show mpls ldp session

Command mode

Privileged user mode

Usage guidelines

This command allows you to show the information of the LDP sessions being or already established, including session status, peer IP address, TCP port number, keepalive interval and keepalive time, session PDU, label distribution mode, loop detection mode and peer interface address.

Examples

```
DES-7210# show mpls ldp session
Session-5-UP:LDP Identifier 192.168.0.2:0 State OPERATIONAL
session not backup msg data
session hold msg count: 0 ,write thread (nil),historymax 1
Remote dest 192.168.4.1:646 , Our is ACTIVE
Keepalive recv timer is on , Hold time is 30 sec
Keepalive send timer is on , Interval is 10 sec
Max PDU is 4096
Path vector limit is 0
Distribution mode is UNSOLICITED
Loop detection mode is NONE
Backoff timer is off
Session attach socket FD[2572], read thread is 0xc6019c0, write thread
is (nil)
LDP Peer Address:
192.168.4.1
192.168.0.2
192.168.3.2
```

42.1.39 show mpls summary

Use this command to show the MPLS global configurations.

show mpls summary

Command mode

Privileged user mode.

Usage guidelines

This command allows you to view the basic information of the MPLS, including maximum/minimum available labels, information of each label space, label space used by each interface, and total number of interfaces with MPLS enabled.

Examples

```
DES-7210# show mpls summary
Per label-space information:
Label-space 0 is using minimum label: 16 and maximum label: 1048575
Label-switching Interface:
Interface              Label space
GigabitEthernet 4/1      0
```

```
GigabitEthernet 4/2      0

Total number of mpls interface is 2
```

Related commands

Command	Description
label-switching	Enable label switching

42.1.40 target-session holdtime

Use this command to set the keepalive holdtime for the extended mechanism. Use the **no** form of this command to restore the default value.

target-session holdtime *seconds*

Parameter description

Parameter	Description
seconds	Set the holdtime, with the value range **<15-65535>.**

Default configuration

By default, the holdtime of the LDP session built in the extended discovery mechanism is 180s. The sending interval of the keepalive message is 60s, which is 1/3 of the session holdtime.

Command mode

config-mpls-router mode.

Usage guidelines

Note that this command is valid for the LDP session only built in the extended discovery mechanism, not for the LDP session already set up.

Examples

```
DES-7210(config)#mpls router ldp

DES-7210(config-mpls-router)# target-session holdtime 90
```

Related commands	Command	Description
	show mpls ldp parameters	Show the LDP global configuration parameters

42.2 BGP/MPLS L3 VPN Commands

42.2.1 address-family ipv4 vrf

Use this command to enter to or exit from the VRF address family mode, and set the interaction of a vrf route.

[no] address-family ipv4 vrf *vrf-name*

Parameter description	Parameter	Description
	vrf-name	VRF name.

Default configuration	By default, no VRF address family is defined.

Command mode	Router mode.

Usage guidelines	This command allows you to enable (or disable) the route information exchange between the PE and CE. Use command **exit-address-family** to return to the BGP configuration mode.

Examples	DES-7210(config)# **router bgp** *100* DES-7210(config-router)# **address-family ipv4 vrf** *vrf1*

Related	Command	Description

commands	**neighbor activate**	Activate an address family
	exit-address-family	Exit from this mode.

42.2.2 address-family vpnv4

Use this command to enter to or exit from the vpn address family mode and enables VPN information interaction between the PEs.

[no] address-family vpnv4 [unicast]

Parameter description	**Parameter**	**Description**
	unicast	Specify the unicast address prefix

Default configuration	By default, no vpn address family is defined.
Command mode	Router mode
Usage guidelines	Use this command to enable the VPN routing information interaction between PEs and enter the **address-family VPN** mode. Use command **exit-address-family** to exit from the address-family VPN configuration mode.

Examples

```
DES-7210(config)# router bgp 100
DES-7210 (config-router)# address-family vpnv4
```

Related commands	**Command**	**Description**
	neighbor activate	Activate an address family

	exit-address-family	Exit from this mode.

42.2.3 clear ip bgp vrf

Use this command to reset the sessions of all members in VRF.

clear ip bgp vrf *vrf-name* [*| *address*] [[**soft**][**in|out**]]

	Parameter	Description
Parameter description	*vrf-name*	VRF name.
	*	Reset all BGP sessions in VRF.
	address	Reset the BGP sessions of the specified peer in VRF.
	ipv4 unicast	IPv4 unicast session.
	in	Reset the actively-connected session bulit by the peer.
	out	Reset the actively-connected session bulit by the local BGP speaker.
	soft	Reset the route information sent to or received from the specified peer by command.
	soft in	Reset the received route information by command.
	soft out	Reset the distributed route information by command.

Default configuration	N/A.
Command mode	Privileged EXEC mode

Usage guidelines	Use this command to reset the BGP sessions of all members in VRF.

Examples	DES-7210(config)# **clear ip bgp vrf my-vrf in**

42.2.4 exit address-family

Use this command to exit the VRF address family configuration or vpn address family configuration mode.

exit address-family

Command mode	Specific address family configuration mode

Examples	DES-7210(config)# **router bgp** *100* DES-7210(config-router)# **address-family vpnv4 unicast** DES-7210(config-router-af)# **exit address-family**

42.2.5 ip route static inter-vrf

Use this command to enable or disable the static inter-vrf route.

[no] ip route static inter-vrf

Default configuration	Enable the static inter-vrf route by default.

Command mode	Global configuration mode

Usage guidelines	If users configure the **no ip route static inter-vrf**, the inter-vrf route of static configuration will not be valid. If the active static inter-vrf route is existed, when you configure it again, it will print similar information as follow, to prompt to delete the static inter-vrf route. *Aug 7 10:58:34: %NSM-6-ROUTESACROSSVRF: **Un-installing route** [*x.x.x.x/8*] **from global routing table with outgoing interface** *x/x.*
Examples	`DES-7210(config)# no ip route static inter-vrf`

42.2.6 ip route vrf

Use this command to create a static routing table entry for the VFR. Use the **no** form of this command to delete the entry.

[**no**] **ip route vrf** *vrf-name ip-addr mask interface next-hop-address* [**global**]

Parameter description

Parameter	Description
vrf-name	VRF name.
ip-addr	Prefix of the destination address of the route
Mask	Mask of the prefix of the destination address
interface	Egress of the destination address.
next-hop	Next hop of the destination address
global	Indicate the next hop is of the global VRF.

Default configuration	There is no static route by default.

Command mode	Global configuration mode
Usage guidelines	The outgoing interface can be specified to bind to the interface of other vrf, to configure the static inter-VRF route. If the global parameter is configured, it is considered as the route of the global VRF. However, if the interface and global parameter are configured at the same time, and the interface is not within the global vrf, it will take the vrf where the interface locates as the standard. Note: Configure the global to cross the global inter-vrf. It is not limited by the no ip route static inter-vrf.
Examples	`DES-7210(config)# ip route vrf vrf1 10.10.10.0 255.255.255.0 gi3/1 192.168.18.1`

42.2.7 ip vrf

Use this command to create a VRF. Use the **no** form of this command to delete a VRF.

[**no**] **ip vrf** *vrf-name*

Parameter description

Parameter	Description
vrf-name	VRF name.

Default configuration	By default, no vrf is defined.
Command mode	Global configuration mode
Examples	`DES-7210(config)# ip vrf vrf1`

Related commands	**Command**	**Description**
	ip vrf forwarding	Bind the VRF with an interface
	show ip vrf	Show VRF configurations.
	rd	Configure the RD for the VRF
	route-target	Configure the RT attribute for the VRF.

42.2.8 ip vrf forwarding

Use this command to bind the VRF with an interface. Use the **no** form of this command to remove the binding.

[**no**] **ip vrf forwarding** *vrf-name*

Parameter description	**Parameter**	**Description**
	vrf-name	VRF name.

Default configuration	By default, the VRF is not binding with any interface.

Command mode	Interface configuration mode

Examples

```
DES-7210(config)# int eth1
DES-7210(config-if)# ip vrf forwarding vrf1
```

Related	**Command**	**Description**

commands	**ip vrf**	Create a VRF instance
	show ip vrf	Show the VRF configurations

42.2.9 maximum routes

Use this command to limit the maximum routes within the vrf. Use the **no** form of this command to cancel this limit.

maximum routes *limit* {**warn-threshold | warning-only**}

no maximum routes

	Parameter	Description
Parameter description	*limit*	Limit the routes. The routes which exceed the limits will not be written into the core route table, ranging from 1 to 4294967295.
	warn-threshold	Print the warning threshold, It will print the warning after the percent is reached, ranging from 1 to 100.
	warning-only	After the configured limit is reached, it only prints the warning. But it is still allowed to add to the core route table.

Default configuration	There is no limit for the configuration by default.
Command mode	VRF configuration mode
Usage guidelines	This command is used to limit the allowed routes within the VRF. If it only hopes to get the warning, use the warning-only parameter.

Examples

```
DES-7210(config)# ip vrf vrf1
DES-7210(config-vrf)# rd 200:1
DES-7210(config-vrf)# maximum routes 1000 warning-only
```

42.2.10 neighbor activate

Use this command to activates the neighboring or peer group under current address mode. Use the **no** form of this command to restore the default value.

neighbor {*peer-address* | *peer-group-name*} **activate**

no neighbor {*peer-address* | *peer-group-name*} **activate**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer. This address can be the IPv4 or IPv6 address.
peer-group-name	Specify the name of the peer group. The peer group name doesn't exceed 32 characters.

Default configuration

It is enabled under the address family IPv4.

Command mode

The BGP configuration mode, the IPv4 address family configuration mode of BGP, the IPv6 address family configuration mode of BGP, the IPv4 VRF configuration mode of BGP and the VPNv4 address family configuration mode of BGP.

Usage guidelines

For the address family of ipv4, this function is enabled by default. For other address family type, you need to configure this command for route information exchange.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.0.0.1 remote-as 100
```

```
DES-7210(config-router)# address-family vpnv4
DES-7210(config-router-af)# neighbor 10.0.0.1 activate
```

Related commands

Command	Description
router bgp	Open the BGP protocol.
neighbor remote-as	Configure the peer of BGP

42.2.11 neighbor allowas-in

When you configure the PE, you can use this command to allow the PE to receive the messages with AS numbers duplicated with this PE. Use the **no** form of this command to restore the default value.

neighbor {*peer-address* | *peer-group-name*} **allowas-in** *number*

no neighbor {[*peer-address* | *peer-group-name*} **allowas-in**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.
number	The repeated times of the allowed AS number. The default value is 3. The range is within [1, 10].

Default configuration

By default, the allowas-in function is not enabled

Command mode

BGP VPN address-family configuration mode, IPv4VRF address family configuration mode of BGP

Usage guidelines	The typical application is in the spoke-hub model. Configure this command on the PE so that the PE can receive and send the advertised address prefix. Configure two VRFs on the PE. Set one of them to receive the route information of all PEs, and notify it to the CE; the other vrf receives the route information advertised by the CE and advertises them to all the PEs. You can make settings at both the IBGP peer and EBGP peer.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.0.0.1 remote-as 100
DES-7210(config-router)# address-family ipv4 vrf vpn1
DES-7210(config-router-af)# neighbor 10.0.0.1 allowas-in
```

Related commands

Command	Description
router bgp	Open the BGP protocol.
neighbor remote-as	Configure the peer of the BGP.

42.2.12 neighbor as-override

Use this command to configure the PE to cover the AS number of a site. Use the **no** form of this command to restore the default value.

neighbor {*peer-address* | *peer-group-name*} **as-override**

no neighbor {*peer-address* | *peer-group-name*} **as-override**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.

Default configuration	By default, the as-override function is not enabled.
Command mode	IPv4VRF address family configuration mode of BGP
Usage guidelines	Normally, the BGP protocol will not receive the route information with the same AS number as the AS. You can use this command to cover the AS number so that the BGP protocol can receive the route information from the same AS number. In the VPN, the most typical application lies in that the two CE ends have the same AS number. Normally, these two CEs cannot receive the other from the other party. After the above command is configured on the PE, you can let the PE cover the AS number of the CE so that the CE from the other end can receive the route information. Only set this function for the EBGP peer.

Examples	`DES-7210(config)# router bgp 60`
	`DES-7210(config-router)# neighbor 10.0.0.1 remote-as 100`
	`DES-7210(config-router)# address-family ipv4 vrf vpn`
	`DES-7210(config-router-af)# neighbor 10.0.0.1 as-override`

Related commands

Command	Description
router bgp	Enable BGP protocol
neighbor remote-as	Configure the peer of BGP

42.2.13 neighbor description

Use this command to set the descriptive language for specified peer (group). Use the **no** form of this command to cancel this configuration.

neighbor {*peer-address* | *peer-group-name*} **description text**

no neighbor {*peer-address* | *peer-group-name*} **description**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.
text	Use to describe the text of this peer (group). Range: up to 80 characters.

Default configuration

Disabled.

Command mode

BGP configuration mode, IPv4VRF address family configuration mode of BGP

Usage guidelines

This command is used to add the descriptive character for the peer (group).It can help us remember the characteristics and features of this peer (group) better.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.1.1.1 remote-as 80
DES-7210(config-router)# neighbor 10.1.1.1 description xyz.com
```

Related commands

Command	Description
router bgp	Enable BGP protocol
neighbor remote-as	Configure the peer (group) of BGP.

42.2.14 neighbor remote-as

Use this command to configure the peer (group) of BGP. Use the **no** form of this command to delete the configured peer (group).

neighbor {*peer-address* | *peer-group-name*} **remote-as** *as-number*

no neighbor {*peer-address* | *peer-group-name*} **remote-as** *as-number*

Parameter description

Parameter	Description
peer-address	Specify the address of the peer, which may be the IPv4 or IPv6 address.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.
as-number	AS number of the BGP peer (group). The range is from 1 to 65535.

Default configuration

No BGP peer is configured.

Command mode

BGP configuration mode, IPv4 address family configuration mode of BGP, IPv6 address family configuration mode of BGP and IPv4 VRF configuration mode of BGP

Usage guidelines

If you specify the BGP peer group, all members of the peer group will inherit the setting of this command.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# neighbor 10.0.0.1 remote-as 80
```

Related commands

Command	Description
router bgp	Enable BGP protocol

42.2.15 neighbor shutdown

Use this command to disable the BGP connection established for specified BGP peer. Use the **no** form of this command to restart the BGP peer (group).

neighbor {*peer-address* | *peer-group-name*} **shutdown**

no neighbor {*peer-address* | *peer-group-nam*e} **shutdown**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer, which can be the IPv4 or IPv6 address.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.

Default configuration

Disabled.

Command mode

BGP configuration mode, IPv4 address family configuration mode of BGP, IPv6 address family configuration mode of BGP and IPv4 VRF configuration mode of BGP

Usage guidelines

This command is used to disable the valid connection established for specified peer (group), and delete all associated route information.However, this command still remains the configuration information of this specified peer (group).

If you specify the BGP peer group, all members of the peer group will inherit the setting of this command. However, if you set this command for some member of the peer, it will cover the peer group-based setting.

Examples

```
DES-7210(config)# router bgp 60
DES-7210(config-router)# neighbor 10.0.0.1 shutdown
```

Related commands

Command	Description
router bgp	Enable BGP protocol
neighbor remote-as	Configure the peer of BGP
show ip bgp summary	Show the connection status of BGP

42.2.16 neighbor soo

Use this command to configure the neighbor source site attribute value. Use the **no** form of this command to cancel the neighbor source site attribute value.

neighbor [*peer-address* | *peer-group-name*] **soo soo-value**

no neighbor [*peer-address* | *peer-group-nam*e] **soo**

Parameter description

Parameter	Description
peer-address	Specify the address of the peer.
peer-group-name	Specify the name of the peer group. The name of the peer group doesn't exceed 32 characters.
soo-value	Value of soo. soo-value can have two different kinds of parameters: (1)soo-value＝ as-num:nn an-num is the puclic autonomous area system number, and nn is specified by the user (2)soo-value ＝ ip-addr:nn The ip-addr address must be a global IP address, and nn is specified by the user

Default configuration	By default, the soo function is not enabled.
Command mode	BGP IPv4 address family configuration mode
Usage guidelines	In the CE model, this command prevents the route information from the CE to the PE to return to the CE end.

Examples

```
DES-7210(config)# router bgp 65000
DES-7210(config-router)# address-family ipv4 vrf vpn1
DES-7210(config-router-af)# neighbor 10.0.0.1 remote-as  100
DES-7210(config-router-af)# neighbor 10.0.0.1 soo 100:100
```

Related commands

Command	Description
router bgp	Enable BGP protocol

42.2.17 rd

Use this command to define the RD value of the VRF

rd *rd-value*

Parameter description

Parameter	Description
rd_value	The RD value.

Default configuration	By default, no RD value is configured. The default RD value is 0:0.

Command mode	VRF configuration mode.
Usage guidelines	If you have defined a VRF and configured the RD value for it, you cannot modify the RD value. If it is absolutely necessary to modify the RD value, the only way is to first delete the VRF and then configure the RD value for it. One VRF can have only one RD value, and you cannot define multiple RD values for it.
Examples	`DES-7210(config)# ip vrf vrf1` `DES-7210 (config-vrf)# rd 100:1`

Related commands

Command	Description
ip vrf	Create a VRF instance
show ip vrf	Show the VRF configuration

42.2.18 redistribute

The route redistributed command can be used to carry out the redistribution between the route information of other route protocol and BGP, and the no form of this command can be used to delete this function and its parameter configuration.

redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

no redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

Parameter description

Parameter	Description
protocol-type	Type of source protocol for the redistributed route. There are connected, static and rip protocol at present.
route-map *map-tag*	The name of the associate **route-map**. No associate with **route-map** by default.

	metric *metric-value*	The default metric value of the configured redistribution route. This value is not set by default.

Default configuration

It is disabled by default.

Command mode

BGP configuration mode, IPv4 address family configuration mode of BGP, IPv6 address family configuration mode of BGP and IPv4 VRF configuration mode of BGP

Usage guidelines

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time. The switches can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

Description: When the no command is configured, if the parameters are configured and there are corresponding parameter configurations, it will cancel the configuration of corresponding parameters.If there is no parameter, this configuration of redistribute will be canceled.

Caution: for the metric value of the route, it will apply the route-map to process according to original value. If it is processed in the route-map, it will use the value after the route-map process. If this value is not set in the route-map, but the metric option is configured, it will use the metric configuration value. If there is not any value, it will use the redistributed value.

Examples

```
DES-7210(config-router)# redistribute static route-map static-rmap
DES-7210(config-router)# no redistribute static
route-map static-rmap
DES-7210(config-router)# no redistribute static
```

Related commands

Command	Description
show ip protocols	Show the protocol configuration.

42.2.19 redistribute OSPF

The route redistributed command can carry out the redistribution between the route information of the OSPF route protocol and BGP, and the no form of this command can be used to delete this function and its parameter configuration.

redistribute ospf *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [**1**|**2**] **nssa-external** [**1**|**2**]]

no redistribute ospf *process-id* [**route-map** *map-tag*] [**metric**

metric-value] [match {internal|external [1|2]|nssa-external [1|2]}]

Parameter description

Parameter	Description
process-id	Process ID of the redistributed OSPF protocol.
route-map *map-tag*	The name of the associate **route-map.** No associated with **route-map** by default.
metric *metric-value*	Configured default metric value of the redistributed route. This value is not set by default.
match	Used to set the matched subtype of the OSPF route.
internal	Internal subtype of route for OSPF, the default configuration of match item for the redistributed ospf route.
external [**1**|**2**]	External type of route for OSPF, can describe the type 1 or type 2 in detail. If not specified, it includes the type 1 and type 2.
nssa-external [**1**|**2]**	nssa-external type of route for OSPF, can describe the type 1 or type 2 in detail. If not specified, it includes the type 1 and type 2.

Default configuration	Disable the redistributed OSPF route.
Command mode	BGP configuration mode, IPv4 address family configuration mode of BGP, IPv6 address family configuration mode of BGP and IPv4 VRF configuration mode of BGP
Usage guidelines	When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time. The switches can run the protocols at the same time, so it should redistribute the protocols.

Note

When the no command is configured, if the parameters are configured and there are corresponding parameter configurations, it will cancel the configuration of corresponding parameters.If there is no parameter, this configuration of redistribute will be canceled. When all of the route subtypes are deleted, it is the default route type.

Caution

The filtration rule of the OSPF route is to carry out the filtration of the OSPF route type according to the configured match option, and then carry out the filtration of the route-map rule.For the metric value of the route, it will carry out the route-map process according to the redistributed metric value. If it is processed in the route-map, it will use the value after the route-map process. If it is not processed in the route-map, but the metric option is configured, it will use the metric configuration value. If there is no any value, it will use the redistributed value directly.

Examples

```
DES-7210(config-router)# redistribute ospf 2 route-map static-rmap
DES-7210(config-router)# no redistribute ospf 4 match external
route-map ospf-rmap
DES-7210(config-router)# no redistribute ospf 78
```

Related commands

Command	Description
show ip protocols	Show the protocol configuration.

42.2.20 route-target

Use this command to define or cancel the RT attribute of a VRF.

[**no**] **route-target** {**import | export | both**} *rt-value*

Parameter description

Parameter	Description
import	Set the import value for the VRF
export	set the export value for the VRF
both	Set the import and export value for the VRF

Default configuration

By default, no Route-Target is defined.

Command mode

VRF configuration mode

Usage guidelines

In one VRF, you can configure multiple import and expoer route-target attribute values.

Examples

```
DES-7210(config)# ip vrf vrf1
DES-7210(config-vrf)# route-target import 100:1
DES-7210(config-vrf)# route-target export 100:2
DES-7210(config-vrf)# route-target both 100:4
```

Related commands

Command	Description
ip vrf	Create a VRF instance

42.2.21 show ip bgp vpnv4

Use this command to show the VPN route information.

show ip bgp vpnv4 all [*network* | **neighbor** [*address*] | **summary** | **label**]

show ip bgp vpvn4 vrf *vrf-name* [*network* | **summary** | **label**]

show ip bgp vpvn4 rd *rd-value* [*network* | **neighbor** [*address*] | **summary** | **label**]

Parameter description

Parameter	Description
network	Show the prefix of the specified destination network.
neighbor	Show the neighbor information of the specified route
summary	Show the summary information of the route
label	Show the label information of the route.
all	Show the VPN route information of all VRFs.
vrf	Show the VPN route information of the specified VRF.
rd	Show the VPN route information of the specified RD value.

Default configuration

N/A.

Command mode

Privilege mode.

Usage guidelines

This command allows you to show the VPN route information.For the MPLS BGP application environment, the route of bgp vrf is imported by the MP-BGP optimal. Hence, for the vpn route of multiple MP-BGPs, it will only show the optimal one in the show ip bgp vpnv4 vrf. The detailed MP-BGP route information should be viewed in show ip bgp vpnv4 all.

Examples

```
DES-7210# show ip bgp vpnv4 all
Network          Nexthop       Metric       Localprf     Weight
     Path
Route Distinguisher : 100:2
*>i 192.168.0.1/32  192.168.0.2      0         100
0          10 ?
*>i 192.168.1.0/32  192.168.0.2      0     100
0          ?
Route Distinguisher : 100:30
*>i 192.168.0.1/32  192.168.0.2      0      100
0          10 ?
*> 192.168.4.0  192.168.4.1          0
0         20 ?
* 192.168.4.0    0.0.0.0             0
32768       ?
DES-7210# show ip bgp vpnv4 vrf vpn1 summary
BGP router identifier 192.168.0.4 , local AS num 100
BGP  VRF vrf1 Route  Distinguisher : 100 : 30
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries
Neibhbor   V   AS   MsgRcvd Msgsend  TblVer  IntQ
OutQ   Up/Down  State/PfxRcd
192.168.4.1 4  20    15      16    1       0    0
00:10:36   3
Total number of neighbors 1
```

***:** This route is valid..

s: This route is suppressed by the aggregate route.

S：This route is an old entry.

>: This route is optimized.

i: This route is learned from IBGP.

Nexthop: The next-hop route information.

Metric: The metric value of this route.

Localprf: The local priority attribute of this route.

Path： The AS-path included in this route.

i: The ORINGIN attribute of this route is IGP.

e: The ORINGIN attribute of this route is EGP.

?: The ORINGIN attribute of this route is the one other than IGP and EGP.

42.2.22 show ip route vrf

Use this command to show the routing table entry of the VRF

show ip route vrf *vrf-name* [*A.B.C.D mask* | **bgp | connected | isis | ospf | rip | static**]

Parameter description

Parameter	Description
vrf-name	VRF name
A.B.C.D mask	Show the entry of the prefix of the specified route.
bgp	Show the route entry generated from BGP.
connected	Show the entry of directly-connected route.
isis	Show the route entry generated from ISIS.
ospf	Show the route entry generated from OSPF.
rip	Show the route entry generated from RIP.
static	Show the static route entry.

Command mode Privileged mode

Examples

```
DES-7210# show ip route vrf vrf1
Codes: C - connected, S - static, R - RIP,B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2 ,
ia - IS-IS inter area
* - candidate default

B   192.168.0.1/32 , [200/0] via 192.168.0.2, 01:02:33
B   192.168.0.3/32 , [200/0] via 192.168.4.1 , 01:02:33
C   192.168.4.0/24 is directly connected ,eth1
```

Related commands

Command	Description
show ip vrf	Show the vrf configuration information

42.2.23 show ip vrf

Use this command to show the configured VRF information.

show ip vrf [*vrf-name*]

Parameter description

Parameter	Description
vrf-name	VRF name.

Command mode

Privileged mode

Usage guidelines

When the inputted parameter carries the VRF name, the command shows the VRF information. If no VRF name is specified, it shows the information of all VRFs.

Examples

```
DES-7210# show ip vrf vrf1
VRF pe1; default RD : 100:2
Interfaces:
Eth0
Export VPN route-target communities:
RT :100:30
No import VPN route-target community
No import route-map
```

Related commands

Command	Description
ip vrf	Create a VRF instance
rd	Configure the RD value
route-target	Configure the RT value
ip vrf forwarding	Bind the VRF with an interface

42.3 L2 VPN Commands

Caution

In this chapter, VC and PW are of the same understanding.

42.3.1 show mpls l2transport vc

Use this command to display the VPWS VC information.

show mpls l2transport vc [*vc_id*] | [**interface** *interface_name*] [**detail**]

Parameter description

Parameter	Description
vc_id	Show the specified PW ID only.
interface *interface_name*	Show the VPWS PW binded on the interface only.

	detail	Show the detailed PW information.

Command mode	Privileged mode.
Usage guidelines	N/A

Examples

```
DES-7210# show mpls l2transport vc 1 detail
Local interface : VLAN 1, AC state: up
Peer address: 192.168.0.1 ,VC ID: 1, VC status: up
VC type: vlan     VC mode:tagged
Group id: 0    MTU: 1500
Control Word not support
Output interface: VLAN 300 , imposed label stack { 21 ,501 }
MPLS VC label:  local 21, remote 21
```

```
DES-7210# show mpls l2transport vc detail
Local interface : VLAN 1, AC state: up
Peer address: 192.168.0.1 ,VC ID: 1, VC status: up
VC type: vlan     VC mode:tagged
Group id: 0    MTU: 1500
Control Word not support
Output interface: VLAN 300 , imposed label stack { 21 ,501 }
MPLS VC label:  local 21, remote 21
Local interface : VLAN 2, AC state: up
Peer address: 192.168.0.1 ,VC ID: 2, VC status: up
```

```
VC type: vlan     VC mode:tagged

Group id: 0    MTU: 1500

Control Word not support

Output interface: VLAN 300 , imposed label stack {22 ,501 }

MPLS VC label:  local 22, remote 22
```

Field	Description
Local interface	VC-binding local interface.
AC state	AC state, up or down.
Peer address	VC Peer IP address.
VC ID	Sole identifier for VC.
VC status	VC state, up or down.
VC type	VC type, ethernet or vlan.
VC mode	VC mode, tag or raw.
Group id	Local group ID for VC.
MTU	Locally-configured VC MTU.
Control Word	Whether the control word is support or not.
Output interface	The output interface for transmitting the local VC in the public network.
imposed label stack	The imposed label stack.
MPLS VC label	MPLS VC label.

Related commands

Command	Description
xconnect	Interface-VPWS PW bind, and create the VPWS PW instance.

42.3.2 show mpls l2vc ftn-table

Use this command to show the PW FTN table.

show mpls l2vc ftn-table

Parameter description	N/A.
Command mode	Privileged mode
Usage guidelines	N/A.

Examples

```
DES-7210#show mpls l2vc ftn-table
Local intf Dest address  VC ID  VC_label   Out intf
---------- ------------- ------ --------  --------
-          2.2.2.2       1     1024      GigabitEthernet 1/1
-          3.3.3.3       1     21        GigabitEthernet 1/2
```

Related commands

Command	Description
xconnect	Interface-VPWS PW bind, and create the VPWS PW instance.

42.3.3 show mpls ldp vc

Use this command to show the LDP PW information.

show mpls ldp vc [*vc-id*]

Parameter

Parameter	Description

description	*vc_id*	Use PW ID to filter the PW displaying.

Default configuration

N/A.

Command mode

Privileged mode

Usage guidelines

N/A.

Examples

```
DES-7210# show mpls ldp vc
Total VC Count: 1
VC: vcid: 1, peer: 3.3.3.3
  local info:
    vpn_id: 1, vc bind type: vpws vc
    Local vc type: Ethernet VLAN, local group id: 0, local mtu: 1500
    local prefer use Control Word: no, local use Control Word: no
  Remote info:
    remote vc type: Ethernet VLAN, remote group id: 0, remote mtu: 1500
    remote use Control Word: no
    remote label: 21
  VC info:
    state: (0x27) create | map_send | map_recv | AC up
    session: 3.3.3.3:0
    local_label: 1027
    last send message id: 398
```

```
    last recv message id: 105

    create time: 02:47:06, last change time: 01:17:29, up time:
01:17:29
```

Field	Description
Total VC Count	LDP VC count.
vcid	Sole identifier of VC
peer	Peer IP address for VC
local info	VC local configurations.
vpn id	ID of the VPN where the VC belongs. For VPWS VC, it is VC ID; For VPLS VC, it is VPLS ID.
vc bind type	Specify the VC bind type
local vc type	Local-configured VC type.
local group id	VC local group ID.
local mtu	VC local MTU.
local prefer use Control Word	Whether the local enables Control Word or not.
local use Control Word	Whether the negotiation result of Control Word is used or not.
Remote info	VC peer configurations.
remote vc type	Peer VC type.
remote group id	VC peer group ID.
remote mtu	VC peer MTU.
remote use Control Word	Whether the peer enables Control Word or not.
remote label	Label assigned from the peer to

	VC.
VC info	Other VC information.
state	VC states are: ● none ● create ● map_send ● map_recv ● withdraw_send ● req_send ● AC up ● AC down
session	LDP session of VC information interchange.
local label	Label assigned from the local to VC.
last send messsage id	Last send LDP message ID carried with the VC message.
last recv message id	Last received LDP message ID carried with the VC message.
create time	VC create time in the LDP layer.
last change time	Last change time for VC in the LDP layer.
up time	VC UP time in the LDP layer.

42.3.4 vc-withdraw-expect-release

Use this command to configure whether to expect the peer reply of the PW label release after the PW label withdraw messages have been sent by LDP.

[**no**] **vc-withdraw-expect-release**

Parameter description	N/A.
Default configuration	The PW label mapping messages expect the release messages of the peer reply label.
Command mode	**config-mpls-router** mode
Usage guidelines	With this command enabled, after the LDP sends the PW label withdraw messages, only if the the peer reply of the PW label release message has been received can the labels be truly released. For example, after enabling this command, the PW label withdraw messages are sent because the AC is down; if the peer reply of PW label release message is not received, when the AC is up again, LDP will not resend the PW label mapping message untill the peer reply of PW label release message is received, or use the **no vc-withdraw-expect-release** command to halt the waiting.
Examples	`DES-7210(config-mpls-router)#vc-withdraw-expect-release`

42.3.5 xconnect

Use this command to enable the VPWS service on the interface.

xconnect vc_id vc_peer **encapsulation mpls** [**ethernet** | **ethernetvlan**] [**raw** | **tagged**] [**send-vlanrewrite-req** | **not-send-vlanrewrite-req**] [*gourp_id*] [*mtu*]

Use the no form of this command to cancel the VPWS service.

no xconnect

Parameter

Parameter	Description

description	*vc_id*	PW service instance ID, in the range of 1-4294967295.
	vc_peer	*A.B.C.D*, the peer LSR ID.
	ethernet	Specify the PW type as **ethernet** and the encapsulation mode as **raw**.
	ethernetvlan	Specify the PW type as **vlan** and the encapsulation mode as **tag**.
	raw	Specify the encapsulation mode as **raw**.
	tagged	Specify the encapsulation mode as **tag**.
	send-vlanrewrite-req	Send the **vlanrewrite** request to the PW peer.
	not-send-vlanrewrite-req	Not send the **vlanrewrite** request to the PW peer.
	group_id	Specify the VC group ID, the default value is 0, in the range of 0-4294967295.
	mtu	Set the MTU size, the default value is 1500, in the range of 46-9216.

Default configuration	By default, no VPWS binding service on the interface. The default PW type is **ethernetvlan**, in **raw** encapsulation mode.

Command mode	Interface configuration mode

Usage guidelines

This command can only be used on the vlan interface. When modifying the PW MTU, the consistency of the actual interface MTU and the negotiated MTU shall be ensured. You can use the **mtu** command to modify the actual MTU value on the interface.

Caution:

The MTU configuration of both ends of PW must be consistent, so are the PW types; otherwise, the PW fails to be UP.

Examples

The following example binds vlan 2 with VPWS :

```
DES-7210(config)#int vlan 2

DES-7210(config-if)# xconnect 1.1.1.1 1 encapsulation mpls
```

Related commands

Command	Description
show mpls l2transport vc	Show the PW service instance information .

43 Port-based Flow Control Configuration Commands

43.1 Configuration Related Commands

Port security module configuration includes the following commands:

- **strom-control**
- **switchport protected**
- **protected-ports route-deny**
- **switchport port-security**
- **switchport port-security aging**
- **switchport port-security mac-address**
- **arp-check**

43.1.1 storm-control

Use this command to enable the storm suppression. Use the **no** form of the command to disable the storm suppression.

storm-control {broadcast | multicast | unicast} [{level *percent* | **pps** *packets*|*rate-bps***}]**

no storm-control {broadcast|multicast|unicast}[{level *percent* | **pps** *packets*|*rate-bps***}]**

Parameter description

Parameter	Description
broadcast	Enable the broadcast storm suppression function.
multicast	Enable the unknown unicast storm suppression function.
unicast	Enable the unknown unicast storm suppression function.

percent	According to the bandwidth percentage to set, for example, 20 means 20%
packets	According to the pps to set, which means packets per second
Rate-bps	rate allowed
64k-2M	In the unit of 64k
2-100M	in the unit of 1M
Above 100M	in the unit of 8M

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Too many broadcast, multicast or unicast packets received on a port may cause storm and thus slow network and increase timeout. Protocol stack implementation errors or wrong network configuration may also lead to such storms.

A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).

Use **show storm-control** to display configuration.

Examples

The following example enables the multicast storm suppression on GigabitEthernet 1/1 and sets the allowed rate to 4M.

```
DES-7210# configure terminal
DES-7210(config)# interface GigabitEthernet 1/1
DES-7210(config-if)# storm-control multicast 4096
DES-7210(config-if)# end
```

Related commands

Command	Description
show storm-control	Show storm suppression information.

Platform description	DES-7200 only supports the setting of **pps**

43.1.2 switchport protected

Use this command to configure the interface as protected. Use the **no** form of the command to disable the protected port.

switchport protected

no switchport protected

Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	After these ports are set as the protected ports, they cannot switch on L2 but can route on L3. A protected port can communicate with an unprotected port. Use **show interfaces** to display configuration.
Examples	`DES-7210(config)#interface gigabitethernet 1/1` `DES-7210(config-if)# switchport protected`

Related commands

Command	Description
show interfaces	Show the interface information.

43.1.3 protected-ports route-deny

Use this command to configure the L3 routing between the protected ports. Use the **no** form of the command to disable theL3 routing.

protected-ports route-deny

no protected-ports route-deny

Default configuration	Enabled.
Command mode	Global configuration mode.

Usage guidelines After setting some ports as the protected ports, they can route on L3. Use this command to deny the L3 communication between protected ports. Use **show running-config** to display configuration.

Examples

```
DES-7210(config)# protected-ports route-deny
```

Related commands

Command	Description
show running-config	Show whether the route-deny between protected ports has been configured.

43.1.4 switchport port-security

Use this command to configure port security and the way to deal with violation. Use the **no** form of the command to disable the port security or restore it to the default.

switchport port-security [violation {protect | restrict | shutdown}]

no switchport port-security [violation]

Parameter description

Parameter	Description
port-security	Enable interface security.
violation protect	Discard the packets breaching security.
violation restrict	Discard the packets breaching security and send the Trap message.
violation shutdown	Discard the packets breaching the security, send the Trap message and disable the interface.

Default configuration Disabled.

Command mode Interface configuration mode.

Usage guidelines

With port security, you can strictly control the input on a specific port by restricting access to the MAC address and IP address (optional) of the port on the switch. After you configure some secure addresses for the port security-enabled port, only the packets from these addresses can be forwarded. In addition, you can also restrict the maximum number of secure addresses on a port. If you set the maximum value to 1 and configure one secure address for this port, the workstation (whose address is the configured secure Mac address) connected to this port will occupy all the bandwidth of this port exclusively.

Examples

This example shows how to enable port security on interface gigabitethernet 1/1, and the way to deal with violation is **shutdown**:

```
DES-7210(config)#interface gigabitethernet 1/1
DES-7210(config-if)# switchport port-security
DES-7210(config-if)# switchport port-security violation shutdown
```

Related commands

Command	Description
show port-security	Show port security settings.

43.1.5 switchport port-security aging

Use this command to set the aging time for all secure addresses on a interface. To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the switch automatically add or delete the secure addresses on the interface. Use the **no** form of the command to apply the aging time on automatically learned address or to disable the aging.

switchport port-security aging {static | time *time* }

no switchport port-security aging {static | time }

Parameter description

Parameter	Description
static	Apply the aging time to both manually configured secure addresses and automatically learned addresses. Otherwise, apply it to only the automatically learned secure addresses.
time *time*	Specify the aging time for the secure address on this port. Its range is 0-1440 in minutes. If you set it to 0, the aging function is disabled actually.

Default configuration	No secure address is aged.
Command mode	Interface configuration mode.
Usage guidelines	In interface configuration mode, use **no switchport port-security aging time** to disable the aging for security addresses on the port. Use the **no switchport port-security aging static** to apply the aging time to only the dynamically learned security address. Use **show port-security** to display configuration.

Examples	`DES-7210(config)# interface gigabitethernet 1/1`
	`DES-7210(config-if)# switchport port-security aging time 8`
	`DES-7210(config-if)# switchport port-security aging static`

Related commands

Command	Description
show port-security	Show port security settings.

43.1.6 switchport port-security mac-address

Use this command to configure the secure address table. Use the **no** form of the command to remove the configuration or restore it to the default setting.

switchport port-security [**mac-address** *mac-address* [**ip-address** {*ip-address*| *ipv6-address}*]] | [**maximum** *value*]

no switchport port-security [**mac-address** *mac-address* [**ip-address** {*ip-address* |*ipv6-address*}]] | **maximum**]

Parameter description

Parameter	Description
mac-address *mac-address*	Set the secure MAC address.
ip-address *ip-address*	Set the secure IP address.
ip-address *ipv6-address*	Set the secure ipv6 address.
maximum *value*	Set the maximum number of the addresses in the secure address table.

Default configuration	N/A.

Command mode Interface configuration mode.

Usage guidelines The secure address of IP address and MAC address shares hardware with the ACL. Once the ACL or 802.1x is applied on the port, the number of the secure addresses indicating IP address should decrease.

Examples The example below describes how to configure a secure address for interface gigabitethernet 1/1: 00d0.f800.073c and bind it with an IP address:192.168.12.202:

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# switchport mode access
DES-7210(config-if)# switchport port-security
DES-7210(config-if)# switchport port-security
mac-address 00d0.f800.073c ip-address 192.168.12.202
```

Related commands

Command	Description
show port-security	Show port security settings.

Platform description DES-7200 series supports up to 1000 secure addresses globally or up to 84 secure addresses (IP address binding) per port.

43.1.7 arp-check

Use this command to enable the ARP check function. Use the **no** form of the command to disable this function. Use **default** to restore the mode by default.

[**no|default] arp-check [cpu|auto]**

Parameter description

Parameter	Description
cpu	check the packets sent to the CPU.
auto	Restore the mode by default.

Default configuration Auto mode.

Command mode Interface configuration mode.

Usage guidline	Arp-check have three modes: auto, disabled and enabled. In the auto mode, only if the port is address-binding can it check ARP packet. In the disabled mode, it does not check ARP packet. In the enabled mode, it checks ARP packet regardless of whether the port is address-bingding or not.

Examples

```
DES-7210(config-if)# arp-check
```

Related commands

Command	Description
show port-security	Show the port security configuration

43.2 Show Related Command

The following commands are used to show the security configuration of the port:

show storm-control

show port-security

43.2.1 show storm-control

Use this command to show storm suppression information.

show storm-control [*interface-id*]

Parameter description

Parameter	Description
interface-id	Interface on which the storm suppression is enabled

Default configuration All information is displayed.

Command mode Privileged mode.

Examples

```
DES-7210# show storm-control gigabitethernet 1/1
Interface Broadcast Control Multicast Control Unicast Control
---------- --------------- ---------------- ---------------
Gi1/1 Disabled Disabled Disabled
```

Related commands

Command	Description
storm-control	Enable storm suppression.

43.2.2 show port-security

Use this command to show port security settings.

show port-security [address] [interface *interface-id***]**

Parameter description

Parameter	Description
address	Show all the secure addresses or the secure address on the specified interface.
Interface *interface-id*	Show the port security configuration of the specified interface.

Command mode

Privileged mode.

Usage guidelines

This command shows all the port security configurations, secure addresses and the way to deal with violation if no parameter is configured .

Examples

```
DES-7210# show port-security
Secure Port MaxSecureAddr(count) CurrentAddr(count) Security Action
-------- -------------- ----------- -----------
Gi1/1 128 1 Restrict
Gi1/2 128 0 Restrict
Gi1/3 8 1 Protect
```

Related commands

Command	Description
switchport port-security	Enable port security and configure the way to deal with violation.
switchport port-security aging	Specify the aging time fpr the secure address on the interface.
switchport port-security mac-address	Configure the secure address table.

44 802.1X Configuration Commands

44.1 dot1x Active Authentication Command

The dot1x active authentication commands include:

- **dot1x auto-req**
- **dot1x auto-req packet-num**
- **dot1x auto-req req-interval**
- **dot1x auto-req user-detect**

44.1.1 dot1x auto-req

Use this command to configure 802.1X active authentication function in the global configuration command. The **no** form of this command disables the automatic authentication function.

[**no**] **dot1x auto-req**

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	This command is used to actively initiate 802.1x authentication on the device. Use the **show dot1x auto-req** command to view the setting of this function.

Examples	The following example sets the device to automatically initiate 802.1x authentication:
	`DES-7210# configure terminal`
	`DES-7210(config)# dot1x auto-req`
	`DES-7210(config)# end`
	`DES-7210(config)# show dot1x auto-req`
	`Auto-Req: Enabled`

```
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Second
```

Related commands

Command	Description
show dot1x auto-req	Show the automatic authentication request information.

44.1.2 dot1x auto-req packet-num

Use this command to set the number of authentication request messages that the device automatically sends. The **no** form is used to specify the default value.

dot1x auto-req packet-num *num*

no dot1x auto-req packet-num

Parameter description

Parameter	Description
num	Number of authentication request messages that the device sends automatically.

Default

num = 0; namely the packets are sent continuously.

Command mode

Global configuration mode.

Usage guidelines

Use the **show dot1x auto-req** command to view the setting of this function.

Examples

The following example sets the device to automatically initiate 802.1x authentication continuously:

```
DES-7210# configure terminal
DES-7210(config)# dot1x auto-req packet-num 0
DES-7210(config)# end
DES-7210# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Second
```

Related

Command	Description

commands	**show dot1x auto-req**	Show the authentication request information.

44.1.3 dot1x auto-req req-interval

Use this command to set the interval of sending authentication request messages. The **no** form is used to specify the default value.

dot1x auto-req req-interval *interval*

no dot1x auto-req req-interval

Parameter description	**Parameter**	**Description**
	interval	The time interval of actively sending authentication request messages by the device, in second.

Default	30 seconds.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x auto-req** command to view the setting of this function.

Examples

The following example sets the time interval of sending authentication request message to 60s:

```
DES-7210# configure terminal
DES-7210(config)# dot1x auto-req req-interval 60
DES-7210(config)# end
DES-7210# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 60 Second
```

Related commands	**Command**	**Description**
	show dot1x auto-req	Show the authentication request information.

44.1.4 dot1x auto-req user-detect

Use this command to disable the device to send authentication request message after receiving the response. The **no** form is used to specify the default value.

dot1x auto-req user-detect

no dot1x auto-req user-detect

Parameter description	N/A.
Default	Enabled.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x auto-req** command to view the setting of this function.

Examples	The following example sets the device to stop sending authentication request messages after the user gets on line:
	`DES-7210# configure terminal`
	`DES-7210(config)# dot1x auto-req user-detect`
	`DES-7210(config)# end`
	`DES-7210# show dot1x auto-req`
	`Auto-Req: Enabled`
	`User-Detect : Enabled`
	`Packet-Num : 0`
	`Req-Interval: 60 Second`

Related commands

Command	Description
show dot1x auto-req	Show the authentication request information.

44.2 dot1x Timeout Parameter Setting Commands

The dot1x timeout parameter setting commands include:

- **dot1x timeout quiet-period**
- **dot1x timeout re-authperiod**

- **dot1x timeout server-timeout**
- **dot1x timeout supp-timeout**
- **dot1x timeout tx-period**

44.2.1 dot1x timeout quiet-period

Use this command to set the time (in seconds) for the device to wait before reauthentication after the authentication failure (for example, incorrect authentication password). Use the **no** form of the command to restore it tothe default setting.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameter description

Parameter	Description
seconds	Time (in seconds) for the device to wait before reauthentication after the authentication failure The range is from 0 to 65535, in seconds.

Default

10 seconds.

Command mode

Global configuration mode.

Usage guidelines

When authentication fails, the solicitator must wait for a period of time before reauthentication.

Examples

The following example sets the time for waiting re-authentication to 1000s:

```
DES-7210# configure terminal
DES-7210(config)# dot1x timeout quiet-period 1000
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:          Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       3600 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
```

```
Maximum Request:       3 times
Client Oline Probe:    Disabled
Eapol Tag Enable:      Disabled
Authorization Mode:    Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.2.2 dot1x timeout re-authperiod

Use this command to set re-authentication interval when re-authentication is enabled. Use the **no** form of the command to restore it to the default value.

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Parameter description

Parameter	Description
seconds	Period of authentication. The range is from 0 to 65535 seconds.

Default

3600 seconds.

Command mode

Global configuration mode.

Usage guidelines

Use **show dot1x** command to show the 802.1X configuration.

Examples

The following example sets the period of re-authentication to 1000s:

```
DES-7210# configure terminal
DES-7210(config)# dot1x timeout re-authperiod 1000
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:         Enabled
Authentication mode    EAP-MD5
Authed User Number:    0
Re-authen Enabled:     Disabled
Re-authen Period:      1000 sec
Quiet Timer Period:    1000 sec
Tx Timer Period:       3 sec
Supplicant Timeout:    3 sec
Server Timeout:        5 sec
```

```
Re-authen Max:          3 times
Maximum Request:        3 times
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.2.3 dot1x timeout server-timeout

Use this command to set the authentication timeout between the device and the authentication server. Use the **no** form of the command to restore it to the default setting.

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameter description

Parameter	Description
seconds	Authentication timeout between the device and the authentication server. The range is 0 to 65535 seconds.

Default

5 seconds.

Command mode

Global configuration mode.

Usage guidelines

Use **show dot1x** command to show 802.1X configuration.

Examples

The following example sets the authentication timeout of the authentication server to 10s:

```
DES-7210# configure terminal
DES-7210(config)# dot1x timeout server-timeout 10
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:          Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
```

```
Tx Timer Period:       3 sec
Supplicant Timeout:    3 sec
Server Timeout:        10 sec
Re-authen Max:         3 times
Maximum Request:       3 times
Client Oline Probe:    Disabled
Eapol Tag Enable:      Disabled
Authorization Mode:    Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.2.4 dot1x timeout supp-timeout

Use this command to set the authentication timeout between the device and the supplicant. Use the **no** form of the command to restore it to the default setting.

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameter description

Parameter	Description
seconds	Authentication timeout between the device and the supplicant The range is from 0 to 65535 seconds.

Default 3 seconds.

Command mode Global configuration mode.

Usage guidelines Use **show dot1x** command to show 802.1X configuration.

Examples

The following example sets the authentication timeout between the device and the supplicant to 10s:

```
DES-7210# configure terminal
DES-7210(config)# dot1x timeout supp-timeout 10
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:          Enabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
```

```
Re-authen Enabled:      Disabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     10 sec
Server Timeout:         10 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.2.5 dot1x timeout tx-period

Use this command to set the interval of transmitting packets after the maximum number of retransmission times is configured. Use the **no** form of the command to restore it to the default setting.

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameter description

Parameter	Description
seconds	Period of retransmission. The range is from 0 to 65535 seconds.

Default

3 seconds.

Command mode

Global configuration mode.

Usage guidelines

Use **show dot1x** command to show 802.1X configuration.

Examples

The following example sets the interval of retransmission to 10s:

```
DES-7210# configure terminal
DES-7210(config)# dot1x timeout tx-period 10
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:       Enabled
```

```
Authentication mode: EAP-MD5
Authed User Number:  0
Re-authen Enabled:   Disabled
Re-authen Period:    1000 sec
Quiet Timer Period:  1000 sec
Tx Timer Period:     10 sec
Supplicant Timeout:  10 sec
Server Timeout:      10 sec
Re-authen Max:       3 times
Maximum Request:     3 times
Client Oline Probe:  Disabled
Eapol Tag Enable:    Disabled
Authorization Mode:  Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.3 dot1x Re-authentication Commands

Re-authentication commands include:

- **dot1x re-authentication**
- **dot1x reauth-max**

44.3.1 dot1x re-authentication

Use this command to enable periodic re-authentication. Use the **no** form of the command to restore it to the the default setting.

[**no**] **dot1x re-authentication**

Parameter description

N/A.

Default

By default, it is not required to re-authenticate the supplicant periodically.

Command mode

Global configuration mode.

Usage guidelines

This command will reauthenticate the supplicant periodically after he passes the authentication. Use **show dot1x** command to show 802.1X configuration.

Examples

The following example enables the re-authentication function:

```
DES-7210# configure terminal
DES-7210(config)# dot1x re-authentication
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:        Enabled
Authentication mode:  EAP-MD5
Authed User Number:   0
Re-authen Enabled:    Enabled
Re-authen Period:     1000 sec
Quiet Timer Period:   1000 sec
Tx Timer Period:      10 sec
Supplicant Timeout:   10 sec
Server Timeout:       10 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.3.2 dot1x reauth-max

Use this command to set the maximum number of supplicant reauthentication. Use the **no** form of the command to restore it to the default value.

dot1x reauth-max *count*

no dot1x reauth-max

Parameter description

Parameter	Description
count	Maximum number of re-authentications

Default

The default value is 3.

Command mode

Global configuration mode.

Usage guidelines

Use this command to specify the maximum number of supplicant reauthentications. Use **show dot1x** command to show 802.1X

configuration.

Examples

The following example sets the maximum number of re-authentications:

```
DES-7210# configure terminal
DES-7210(config)# dot1x reauth-max 5
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:          Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Enable
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        10 sec
Supplicant Timeout:     10 sec
Server Timeout:         10 sec
Re-authen Max:          5 times
Maximum Request:        3 times
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.4 dot1x Detection Function Commands

The detection function commands include:

- **dot1x probe-timer**
- **dot1x client-probe enable**

44.4.1 dot1x probe-timer

Use this command to enable the probe timer on the client.

dot1x probe-timer{**interval** | **alive**}*interval*

no dot1x probe-timer

Parameter description

Parameter	Description
no	Restore the setting to the default value.
interval	Interval of sending the Hello message.

	alive	Alive interval
	interval	Timer value

Default

The default Hello interval is 20 seconds.

Default user alive interval is 250 seconds

Command mode

Global configuration mode.

Usage guidelines

Configure the alive detection timer for the client. You can use the **show dot1x** command to show the 802.1x setting.

Examples

The following example sets the Hello interval to 30 seconds and the alive interval to 120 seconds:

```
DES-7210# configure terminal
DES-7210(config)# dot1x probe-timer interval 30
DES-7210(config)# dot1x probe-timer alive 120
DES-7210(config)# end
DES-7210# show dot1x probe-timer
Hello Interval: 30 Seconds
Hello Alive: 120 Seconds
```

Related commands

Command	Description
Show dot1x probe-timer	Show the probe timer information.

44.4.2 dot1x client-probe enable

Use this command to enable the online probe function of the client

[**no**] **dot1x client-probe enable**

Parameter description

N/A.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines	Use this command to enable the online probe function of the client.
Examples	Enable the online probe function of the client. DES-7210# **configure terminal** DES-7210(config)# **dot1x client-probe enable** DES-7210(config)# **end** DES-7210# **show dot1x** 802.1X Status: Enabled Authentication mode: EAP-MD5 Authed User Number: 0 Re-authen Enabled: Enabled Re-authen Period: 1000 sec Quiet Timer Period: 1000 sec Tx Timer Period: 10 sec Supplicant Timeout: 10 sec Server Timeout: 10 sec Re-authen Max: 5 times Maximum Request: 3 times Client Oline Probe: Enabled Eapol Tag Enable: Disabled Authorization Mode: Group Server

Related commands

Command	Description
show dot1x	Show the 802.1x configurations.

44.5 Other dot1x Configuration Commands

Other dot1x configuration commands include:

- **dot1x authentication**
- **dot1x auth-address-table**
- **dot1x auth-mode**
- **dot1x default**
- **dot1x dynamic-vlan enable**
- **dot1x guest-vlan enable**
- **dot1x eapol-tag**
- **dot1x max-req**
- **dot1x private-supplicant-only**
- **dot1x port-control auto**
- **dot1x port-control-mode**

- **dot1x stationarity enable**

44.5.1 dot1x authentication

In case the AAA is enabled, the authentication with the AAA server must be performed for logon. Use this command to associate logon authentication method list. The **no** form of this command is used to delete the logon authentication method list.

dot1x authentication {**default** | *list-name*}

no dot1x authentication {**default** | *list-name*}

Parameter description

Parameter	Description
default	Name of the default authentication method list
list-name	Name of the method list available

Default

If AAA is enabled, the AAA service is used for login authentication by default.

Command mode

Interface configuration mode.

Usage guidelines

If the AAA security server is enabled, this command is used for the login authentication with the specified method list.

Examples

The following command demonstrates how to associate a method list on the interface and use **group radius** for authentication.

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
DES-7210(config)# aaa authentication dot1x default group radius
DES-7210(config)# interface fastEthernet0/1
DES-7210(config-if)# dot1x authentication default
DES-7210(config-if)# end
DES-7210#
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authentication dot1x	Configure the logon authentication method list.

44.5.2 dot1x auth-address-table

Use this command to set the IP address list that 802.1X authentication allows. Use the **no** form of the command to remove the allowed IP address list.

dot1x auth-address-table address *mac-addr* **interface** *interface*

no dot1x auth-address-table address *mac-addr* **interface** *interface*

Parameter description

Parameter	Description
mac-addr	Physical IP address that can be authenticated.
interface	Interface number.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

Only the IP address in this list can be authenticated by 802.1X. Use **show dot1x auth-address table** command to show the authentication address list.

Examples

The following example demonstrates how to add an authentication address on the interface.

```
DES-7210# configure terminal
DES-7210(config)# dot1x auth-address-table address
00d0f8000000 interface ehternet 1/1
DES-7210(config)# end
DES-7210#
```

Related commands

Command	Description
show dot1x auth-address-table	Show the information about the IP address list that the 802.1x can authenticate.

44.5.3 dot1x auth-mode

Use this command to specify the 802.1x authentication mode.

dot1x auth-mode {**eap-md5** | **chap** | **pap**}

no dot1x auth-mode

Parameter description

Parameter	Description
eap-md5	Use EAP-MD5 for authentication.
chap	Use CHAP for authentication.
pap	Use PAP for authentication.

Default EAP-MD5 mode.

Command mode Global configuration mode.

Usage guidelines Use the **show dot1x** command to show the 802.1X configurations.

Examples This example shows how to configure the 802.1X authentication mode:

```
DES-7210# configure terminal
DES-7210(config)# dot1x auth-mode chap
DES-7210(config)# end
DES-7210#
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.5.4 dot1x default

Use this command to restore part of 802.1x parameters to the default value..

dot1x default

Parameter description N/A.

Default N/A.

Command mode Global configuration mode.

Usage guidelines Use the **show dot1x** command to show the 802.1X configuration.

Examples

The following example sets the default parameters of 802.1x:

```
DES-7210# configure terminal
DES-7210(config)# dot1x default
DES-7210(config)# end
DES-7210# end
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.5.5 dot1x dynamic-vlan enable

Use this command to enable dynamic VLAN. Use the **no** form of the command to disable the function.

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

Parameter description

N/A.

Default

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Use the **show dot1x dynamic-vlan** command to show the 802.1X configuration.

Examples

The following example enables dynamic VLAN:

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 4/5
DES-7210(config-if)# dot1x dynamic-vlan enable
DES-7210(config)# end
DES-7210#
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.5.6 dot1x guest-vlan

Use this command to set whether to allow **guest vlan** jump. Use the **no** form of the command to disable the function.

dot1x guest-vlan *vid*

no dot1x guest-vlan

Parameter description

Parameter	Description
vid	In the range from 1 to 4094.

Default

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

1. Before using guest vlan, you need to execute **dot1x dynamic-vlan enable** command first，or the configured guest vlan does not take effect.

2. When configuring guest vlan, it is recommended not to modify L2 attribute of the port, especially not to add the port to a VLAN manually.

3. Execute **show running-config** to view 802.1x configuration.

Examples

The following example sets 802.1x guest vlan jumping:

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 4/5
DES-7210(config-if)# dot1x guest-vlan 10
DES-7210(config)# end
DES-7210#
```

Related commands

Command	Description
show running-config	Show the configuration information about 802.1x.

44.5.7 dot1x eapol-tag

Use this command to tag the EAPOL frames. Use the **no** form of the command to disable the function.

dot1x eapol-tag

no dot1x eapol-tag

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x** command to show the 802.1X configuration.

Examples	The following example tags the EAPOL frames:
	`DES-7210# configure terminal`
	`DES-7210(config)# dot1x eapol-tag`
	`DES-7210(config)# end`
	`DES-7210#`

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.5.8 dot1x max-req

During interaction between the dot1x and the server, the dot1x will send a request to the server again if it does not receive a response from the server within a certain period of time. Use this command to set the maximum number of authentication requests sent to the server. Use the **no** form of the command to restore it to the default value.

dot1x max-req *count*

no dot1x max-req

Parameter description

Parameter	Description
count	Maximum number of authentication requests sent to the server.

Default	The default value is 3.
Command mode	Global configuration mode.
Usage guidelines	Use the **show dot1x** command to show the 802.1X configuration.

Examples	The following example demonstrates how to set the maximum number of authentication requests to 7:
	`DES-7210# configure terminal`
	`DES-7210(config)# dot1x max-req 7`
	`DES-7210(config)# end`
	`DES-7210#`

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.5.9 dot1x private-supplicant-only

Use this command to support the private supplicant in the global configuration mode. The **no** form of this command restores it to the default value.

dot1x private-supplicant-only

no dot1x private-supplicant-only

Parameter description	N/A.
Default configuration	The private supplicant is supported.
Command mode	Global configuration mode.

Usage guidelines	You can use **show dot1x private-supplicant-only** to check the 802.1x setting.

Examples	Example
	This example configures to use the private supplicant only:
	`DES-7210# configure t`
	`DES-7210(config)# dot1x private-supplicant-only`
	`DES-7210(config)# end`
	`DES-7210#`

Related commands	**Command**	**Function**
	show dot1x private-supplicant-only	Show the information about the private supplicant.

44.5.10 dot1x port-control auto

In the interface configuration mode, use this command to allow the port to participate in authentication. Use the **no** form of the command to restore it to the default value.

dot1x port-control auto

no dot1x port-control

Parameter description	N/A.
Default	By default, the port does not participate in 802.1x authentication.
Command mode	Interface configuration mode.
Usage guidelines	Use the **show dot1x** command to show the 802.1X configuration.

Examples	The following example sets the port to participate in authentication:
	`DES-7210# configure terminal`
	`DES-7210(config)# interface g0/1`
	`DES-7210(config-if)# dot1x port-control auto`
	`DES-7210(config-if)# end`

```
DES-7210#
```

Related commands

Command	Description
show dot1x	Show the information about 802.1x.

44.5.11 dot1x port-control-mode

By default, 802.1x adopts MAC address-based control mode. In this mode, only authenticated users have access to the network, while other users that connect to the same port cannot access the network. In the port-based control mode, however, if one user that connects to the port passes the authentication, this port becomes an authenticated port and all the users that connect to this port have access to the network. In the port-based single-user control mode, the port is authenticated when it allows only one authenticated user who is enable to use the network normally. If you find other users on the port, you should clear all the users on the port and reauthenticate.The authentication mode can be configured using the following commands:

dot1x port-control-mode {**mac-based** | {**port-based [single-host]**}}

no dot1x port-control-mode

Parameter description

Parameter	Description
mac-based	Enable the MAC address-based control.
port-based	Enable port-based control.
single-host	Enable singlehost-based control.

Default

MAC address-based access control is used by default.

Command mode

Interface configuration mode.

Usage guidelines

Use the **show dot1x port-control** command to show the 802.1X configuration for the port.

Single-host is port-based single-user 802.1x access control. Use **show dot1x port-control** to display port-based and use **show running-config** to display dot1x port-control-mode port-based single-host.

Since single-host only supports the single-user form, setting default-user-limit on the port manually does not take effect in single-host mode. If you set default-user-limit on the port after setting

single-host, only one user can be permitted to use the network still.

Examples

The following example sets the port to participate in authentication and enable port-based authentication:

```
DES-7210(config)# interface g0/1
DES-7210(config-if)# dot1x port-control auto
DES-7210(config-if)# dot1x port-control-mode
port-based
DES-7210(config-if)# end
DES-7210#
```

The following example sets 802.1x authentication of single user port:

```
DES-7210(config)# interface g 0/1

DES-7210(config-if)# dot1x port-control auto

DES-7210(config-if)# dot1x port-control-mode

port-based single-host

DES-7210(config-if)# end

DES-7210#
```

Related commands

Command	Description
show dot1x port-control	Show the port control mode.
Show running-config	Show the configuration.

44.5.12 dot1x stationarity enable

In the port-based 802.1X control mode, dynamic users can transit freely among the ports by default. In special cases, if you want to prevent the user from transiting from 802.1X port to other port, you can use the following commands:

dot1x stationarity enable

no dot1x stationarity enable

Parameter description

N/A.

Default configuration	Dynamic users can transit freely among the ports.
Command mode	Global configuration mode.
Usage guidelines	This command must be configured before user authentication. Otherwise, you need re-authenticate all the users.

Examples	The following example prevents the user from transiting from 802.1X port to other port:
	`DES-7210# configure terminal`
	`DES-7210(config)# dot1x stationarity enable`
	`DES-7210(config)# end`
	`DES-7210#`

Related commands	N/A.

44.6 Show Related Commands

- **show dot1x**
- **show dot1x auth-address-table**
- **show dot1x auto-req**
- **show dot1x private-supplicant-only**
- **show dot1x max-req**
- **show dot1x port-control**
- **show dot1x probe-timer**
- **show dot1x re-authentication**
- **show dot1x reauth-max**
- **show dot1x summary**
- **show dot1x timeout**
- **show dot1x user id**

44.6.1 show dot1x

Use this command to display the information about 802.1x setting.

show dot1x

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about 802.1x:
	`DES-7210# show dot1x`
	
	`802.1X Status: Enabled`
	`Authentication Mode: EAP-MD5`
	`Authed User Number: 0`
	`Re-authen Enabled: Disabled`
	`Re-authen Period: 3600 sec`
	`Quiet Timer Period: 10 sec`
	`Tx Timer Period: 3 sec`
	`Supplicant Timeout: 3 sec`
	`Server Timeout: 5 sec`
	`Re-authen Max: 3 times`
	`Maximum Request: 3 times`
	`Client Oline Probe: Disabled`
	`Eapol Tag Enable: Disabled`
	`Authorization Mode: Group Server`
	`DES-7210#`

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions.
dot1x port-control auto	Set the port to participate in authentication.

dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

44.6.2 show dot1x auth-address-table

Use this command to display 802.1X authentication-allowed address table.

show dot1x auth-address-table[**address** *mac-addr*][**interface** *interface-id*]

Parameter description

Parameter	Description
mac-addr	Physical IP address that can be authenticated
interface	Interface number

Default N/A.

Command mode Privileged mode.

Usage guidelines N/A.

Examples The following example shows the 802.1x authentication-allowed address table.:

```
DES-7210# show dot1x auth-address-table
interface:g3/1
-----------------------------------
mac-addr 00D0.F800.0001
DES-7210#
```

	Command	Description
Related commands	**dot1x auth-mode**	Set the 802.1x authentication mode.
	dot1x max-req	Set the maximum number of authentication request retransmissions.
	dot1x port-control auto	Set the port to participate in authentication.
	dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Set the re-authentication attribute.
	dot1x timeout quiet-period	Set the time the device waits before reauthentication.
	dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

44.6.3 show dot1x auto-req

Use this command to show the configuration information of automatic 802.1x authentication.

show dot1x auto-req

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples

The following example shows the information about automatic 802.1x authentication:

```
DES-7210# show dot1x auto-req
Auto-Req: Disabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Seconds
DES-7210#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions.
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

44.6.4 show dot1x private-supplicant-only

Use this command to show the information about the private supplicant.

show dot1x private-supplicant-only

Parameter description N/A.

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about the private supplicant:
	`DES-7210# show dot1x private-supplicant-only`
	`private-supplicant-only:: disabled`
	`DES-7210#`

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions.
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

44.6.5 show dot1x max-req

Use this command to show the maximum number of authentication request retransmissions to the client.

show dot1x max-req

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the maximum number of authentication request retransmissions:
	`DES-7210# show dot1x max-req`
	`max-req: 2 times`
	`DES-7210#`

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions.
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.

	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

44.6.6 show dot1x port-control

Use this command to show the ports that participate in authentication.

show dot1x port-control [**interface** *interface*]

Parameter description	**Parameter**	**Description**
	interface	Specified interface

Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples

The following example shows the ports that participate in the authentication:

```
DES-7210# show dot1x port-control
interface dyn-user static-user max-user qos     ctrl-mode status
--------- -------- ----------- -------- ------- --------  ------
Gi0/1    0        1           6000     dscp: 0 mac-base Authed
DES-7210#
```

Related commands	**Command**	**Description**
	dot1x auth-mode	Set the 802.1x authentication mode.
	dot1x max-req	Set the maximum number of authentication request retransmissions**.**
	dot1x port-control auto	Set the port to participate in authentication.
	dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Set the re-authentication attribute.

	dot1x timeout quiet-period	Set the time the device waits before reauthentication.
	dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

44.6.7 show dot1x probe-timer

Use this command to show the online probing configurations.

show dot1x probe-timer

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the online probing configuration:
	`DES-7210# show dot1x probe-timer`
	`Hello Interval: 20 Seconds`
	`Hello Alive: 250 Seconds`
	`DES-7210#`

Related commands	**Command**	**Description**
	dot1x auth-mode	Set the authentication mode.
	dot1x max-req	Set the maximum number of authentication request retransmissions**.**
	dot1x port-control auto	Set the port to participate in authentication.

	dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Set the re-authentication attribute.
	dot1x timeout quiet-period	Set the time the device waits before reauthentication.
	dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

44.6.8 show dot1x re-authentication

Use this command to show re-authentication configuration.

show dot1x re-authentication

Parameter description	N/A
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about reauthentication:
	`DES-7210# show dot1x re-authentication`
	`eauth-enabled: disabled`
	`DES-7210#`

Related commands	**Command**	**Description**
	dot1x auth-mode	Set the authentication mode.

	dot1x max-req	Set the maximum number of authentication request retransmissions**.**
	dot1x port-control auto	Set the port to participate in authentication.
	dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Set the re-authentication attribute.
	dot1x timeout quiet-period	Set the time the device waits before reauthentication.
	dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

44.6.9 show dot1x reauth-max

Use this command to show the maximum number of re-authentications.

show dot1x reauth-max

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about the maximum number of re-authentications:
	`DES-7210# show dot1x reauth-max`
	`reauth-max: 2 times`

```
DES-7210#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

44.6.10 show dot1x summary

Use this command to display the 802.1X authentication summary.

show dot1x summary

Parameter description N/A

Default N/A.

Command mode Privileged mode.

Usage guidelines N/A.

Examples

The following example shows the summary of 802.1x authentication:

```
DES-7210# show dot1x summary
ID   MAC  Interface VLAN Auth-State  Backend-State Port-Status Type
- -------- ---------- ----------- ------------- ----------  -----
1 00d0f8000000 Gi0/1   1  Authenticated Idle    Authed    Static
DES-7210#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

44.6.11 show dot1x user id

Use this command to display the information about the 802.1X authentication user.

show dot1x user id <*id*>

Parameter description

Parameter	Description
id	User ID

Default N/A.

Command mode	Privileged mode.
Usage guidelines	N/A.

Examples

The following example shows the information about the 802.1x authentication user:

```
DES-7210# show dot1x user id 1
User name: caikov
id: 1
Type: static
Mac address is 0013.2049.8272
Vlan id is 217
Access from port Gi0/13
User ip address is 192.168.217.64
Max user number on this port is 6000
COS on this port is 5
Up-bandwidth is 1024 kbps
Down-bandwidth is 1024 kbps
Authorization vlan is dep7
Authorization seesion time is 1000000 seconds
Authorization ip address is 192.168.217.64
Start accounting
Permit proxy user
Permit dial user
IP privilige is 2

DES-7210#
```

Related commands

Command	Description
dot1x auth-mode	Set the 802.1x authentication mode.
dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.

	dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Set the retransmission period.

44.6.12 show dot1x timeout

The commands show the information about the 802.1X timeout.

show dot1x timeout quiet-period

show dot1x timeout re-authperiod

show dot1x timeout server-timeout

show dot1x timeout supp-timeout

show dot1x timeout tx-period

Parameter description	N/A.
Default	N/A.
Command mode	Privileged mode.
Usage guidelines	N/A.

Examples	The following example shows the information about the time for the device to wait before reauthentication:
	`DES-7210# show dot1x timeout quiet-period`
	`quiet-period: 60 sec`
	DES-7210#

Related commands	**Command**	**Description**
	dot1x auth-mode	Set the 802.1x authentication mode.

dot1x max-req	Set the maximum number of authentication request retransmissions**.**
dot1x port-control auto	Set the port to participate in authentication.
dot1x reauth-max	Set the maximum number of the supplicant re-authentications.
dot1x re-authentication	Set the re-authentication attribute.
dot1x timeout quiet-period	Set the time the device waits before reauthentication.
dot1x timeout re-authperiod	Set the re-authentication period for the supplicant.
dot1x timeout server-timeout	Set the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Set the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Set the retransmission period.

45 AAA Configuration Commands

45.1 ID Authentication Related Command

45.1.1 aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list. The **no** form of this command is used to delete the 802.1x user authentication method list.

aaa authentication dot1x {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication dot1x {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication.
list-name	Name of the 802.1x user authentication method list, which could be any character string.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS server group is supported.

Default N/A

Command mode	Global configuration mode.
Usage guidelines	If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use **aaa authentication dot1x** to configure a default or optional method list for 802.1x user authentication. The next method can be used for authentication only when the current method does not work.
Examples	The following example defines an AAA authentication method list named **RDS_D1X**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. `DES-7210(config)# aaa authentication dot1x rds_d1x group radius local`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
dot1x authentication	Associate a specific method list with the 802.1x user.
username	Define a local user database.

45.1.2 aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list. The **no** form of this command is used to delete the user authentication method list.

aaa authentication enable {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication enable default

Parameter description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description

	local	Use the local user name database for authentication.
	none	Do not perform authentication.
	group	Use the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.

Default	N/A
Command mode	Global configuration mode.
Usage guidelines	If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable authentication negotiation. You must use **aaa authentication enable** to configure a default or optional method list for Enable authentication. The next method can be used for authentication only when the current method does not work. The Enable authentication function automatically takes effect after configuring the Enable authentication method list.
Examples	The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. `DES-7210(config)# aaa authentication enable default group radius local`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
enable	Switchover the user level.
username	Define a local user database.

45.1.3 aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list. The **no** form of this command is used to delete the authentication method list.

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
list-name	Name of the user authentication method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use **aaa authentication login** to configure a default or optional method list for Login authentication.

The next method can be used for authentication only when the current method does not work.

You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

Examples

The following example defines an AAA Login authentication method list named **list-1**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for

	authentication. `DES-7210(config)# aaa authentication login list-1 group radius local`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
login authentication	Apply the Login authentication method to the terminal lines.
username	Define a local user database.

45.1.4 aaa authentication ppp

Use this command to enable AAA PPP user authentication and configure the PPP user authentication method list. The **no** form of this command is used to delete the authentication method list.

aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication ppp {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication.
list-name	Name of the user authentication method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS server group is supported.

Default	N/A
Command mode	Global configuration mode.

Usage guidelines	If the AAA PPP security service is enabled on the device, users must use AAA for PPP authentication negotiation. You must use **aaa authentication ppp** to configure a default or optional method list for PPP user authentication. The next method can be used for authentication only when the current method does not work.
Examples	The following example defines an AAA PPP authentication method list named **rds_ppp**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. `DES-7210(config)# aaa authentication ppp rds_ppp group radius local`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
ppp authentication	Associate a specific method list with the PPP user.
username	Define a local user database.

45.1.5 login authentication

Use this command to apply the Login authentication method list to the specified terminal lines. The **no** form of this command is used to remove the application of Login authentication method list.

login authentication {**default** | *list-name*}

no login authentication

Parameter description

Parameter	Description
default	Apply the default Login authentication method list to the terminal line.
list-name	Apply the defined Login authentication method list to the terminal line.

Default	N/A
Command mode	Line configuration mode.

Usage guidelines	Once the default login authentication method list has been configured, it will be applied to all the terminals automatically. If non-default login authentication method list has been applied to the terminal, it will replace the default one. If you attempt to apply the undefined method list, it will prompt a warning message that the login authentication in this line is ineffective till it is defined.

Examples	The following example defines an AAA Login authentication method list named **list-1**. In the authentication method list, first the local user database is used for authentication. Then apply this method to VTY 0-4.
	`DES-7210(config)# aaa authentication login list-1 local`
	`DES-7210(config)# line vty 0 4`
	`DES-7210(config-line)# login authentication list-1`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
login authentication	Configure the Login authentication method list.
username	Define a local user database.

45.2 Authorization Related Commands

At present, DES-7210 supports authorization to the network protocols.

45.2.1 aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI. The **no** form of this command is used to disable the aaa authorization command function.

aaa authorization commands *level* {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization commands *level* {**default** | *list-name*}

Parameter description

Parameter	Description
level	Command level to be authorized, 0-15.
default	When this parameter is used, the following defined method list is used as the default method for command authorization.

	list-name	Name of the user authorization method list, which could be any character strings.
	method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
none	Do not perform authorization.
group	Use the server group for authorization. At present, the RADIUS server group is supported.

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	DES-7200 supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny. It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level. The configured command authorization method must be applied to terminal line which requires for the command authorization. Otherwise, the configured command authorization method is ineffective.
Examples	The following example uses the TACACS+ server to authorize the level 15 command: `DES-7210(config)# aaa authorization commands 15 default group tacacs+`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
authorization commands	Apply the command authorization for to the terminal line.

45.2.2 aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode). The **no** form of this command is used to disable the configuration command authorization function.

aaa authorization config-commands

no aaa authorization config-commands

Parameter description	N/A
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.
Examples	The following example enables the configuration command authorization function: `DES-7210(config)# aaa authorization config-commands`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization commands	Define the AAA command authorization.

45.2.3 aaa authorization console

Use this command to authorize the commands of the users who has logged in the console. The **no** form of this command is used to disable the authorization function.

aaa authorization console

no aaa authorization console

Parameter description	N/A
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	DES-7200 supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.
Examples	The following example enables the aaa authorization console function: `DES-7210(config)# aaa authorization console`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization commands	Define the AAA command authorization.
authorization commands	Apply the command authorization to the terminal line..

45.2.4 aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level. The **no** form of this command is used to disable the aaa authorization exec function.

aaa authorization exec {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization exec {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec authorization.

	list-name	Name of the user authorization method list, which could be any character strings.
	method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authorization.
none	Do not perform authorization.
group	Use the server group for authorization. At present, the RADIUS server group is supported.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

DES-7200 supports authorization of users logged in the NAS CLI and assignment of CLI authority level(0-15). The aaa authorization exec function is effective on condition that Login authentication function has been enabled. It can not enter the CLI if it fails to enable the aaa authorization exec.

You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

Examples

The following example uses the RADIUS server to authorize Exec:

```
DES-7210(config)# aaa authorization exec default group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
authorization exec	Apply the command authorization to the terminal line .
username	Define a local user database.

45.2.5 aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network. The **no** form of this command is used to disable the authorization function.

aaa authorization network {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization network {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Network authorization.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
none	Do not perform authorization.
group	Use the server group for authorization. At present, the RADIUS server group is supported.

Default Disabled.

Command mode Global configuration mode.

Usage guidelines

DES-7200 supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically.

Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used.

The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

Examples The following example uses the RADIUS server to authorize network

services:

```
DES-7210(config)# aaa authorization network default group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accounting	Define AAA accounting .
aaa authentication	Define AAA authentication.
username	Define a local user database.

45.2.6 authorization commands

Use this command to apply the list of command authorization to the specific terminal line in the line configuration mode. The **no** form of this command is used to disable this function.

authorization commands *level* {**default** | *list-name*}

no authorization commands *level*

Parameter description

Parameter	Description
level	The authorized command level, 0-15.
default	Use the default command authorization command.
list-name	Apply a defined method list of the command authorization.

Default Disabled.

Command mode Line configuration mode.

Usage guidelines

Once the default command authorization method list has been configured, it is applied to all terminals automatically. Once the non-default command authorization method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the command authorization in this line is ineffective tilll the authorization method list is defined.

Examples

The following example configures the command authorization method list with name cmd, authorizes command level 15, uses the TACACS+ server. If the security server does not response, it does not perform authorization. After configuration, the authorization command is applied to VTY 0-4 lines:

```
DES-7210(config)# aaa authorization commands 15 cmd group tacacs+ none

DES-7210(config)# line vty 0 4

DES-7210(config-line)# authorization commands 15 cmd
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization commands	Define the method list of the AAA command authorization.

45.2.7 aaa authorization exec

Use this command to apply the Exec authorization methos list to the specified terminal lines in the line configuration mode. The **no** form of this command is used to disable the authorization function.

authorization exec {**default** | *list-name*}

no authorization exec

Parameter description

Parameter	Description
default	Use the default method of Exec authorization.
list-name	Apply a defined method list of Exec authorization.

Default

Disabled.

Command mode

Line configuration mode.

Usage guidelines

Once the default execauthorization method list has been configured, it is applied to all terminals automatically. Once the non-default

command authorization method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the exec authorization in this line is ineffective tilll the authorization method list is defined.

Examples

The following example configures the exec authorization method list with name exec-1, uses the RADIUS server. If the security server does not response, it does not perform authorization. After configuration, the authorization command is applied to VTY 0-4 lines:

```
DES-7210(config)# aaa authorization exec exec-1 group radius none

DES-7210(config)# line vty 0 4

DES-7210(config-line)# authorization exec exec-1
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization commands	Define the method list of AAA Exec authorization.

45.3 Accounting Related commands

At present, DES-7210 supports network accounting using RADIUS.

45.3.1 aaa accounting commands

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting commands *level* {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting commands *level* {**default** | *list-name*}

Parameter description

Parameter	Description
level	The accounting command level, 0-15. The message shall be recorded before determing which command level is executed.
default	When this parameter is used, the following defined method list is used as the default method for command

	accouting.
list-name	Name of the command accouting method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
none	Do not perform accouting.
group	Use the server group for acouting, the TACACS+ server group is supported.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

DES-7200 enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service.

The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Examples

The following example performs accounting of the network service requests from users using TACACS+, and configures the accounting command level to 15:

```
DES-7210(config)# aaa accounting commands 15 default start-stop
group tacacs+
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authentication	Define AAA authentication.
accouting commands	Apply the accouting commands to the terminal line.

45.3.2 aaa accounting exec

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting exec {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting exec {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec accouting.
list-name	Name of the Exec accouting method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
none	Do not perform accouting.
group	Use the server group for acouting, the RADIUS and TACACS+ server group is supported.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

DES-7200 enables the exec accounting function after enabling the login authentication.

After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user loggs in, it does not send the account stop information to the security server when a user loggs out, either.

The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Examples

The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access:

```
DES-7210(config)# aaa accounting network start-stop group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authentication	Define AAA authentication.
accouting commands	Apply the Exec accouting to the terminal line..

45.3.3 aaa accounting network

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting network {**default** | *list-name*} **start-stop group radius**

no aaa accounting network {**default** | *list-name*}

Parameter description

Parameter	Description
network	Perform accounting of the network related service requests, including dot1x, PPP, etc.
resource	Perform accounting of resource related service requests.
list-name	Name of the accounting method list
start-stop	Send accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
group	Use the server group for accounting.
radius	Use the RADIUS group for accounting.

Default

Disabled.

Command mode

Global configuration mode.

Usage

DES-7200 performs accounting of user activities by sending record

guidelines	attributes to the security server. Use the keyword **start-stop** to set the user accounting option.
Examples	The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access: `DES-7210(config)# aaa accounting network start-stop group radius`

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization network	Define a network authorization method list.
aaa authentication	Define AAA authentication.
username	Define a local user database.

45.3.4 aaa accounting update

Use this command to enable the accounting update function The **no** form of this command is used to disable the accounting update function.

aaa accounting update

no aaa accounting update

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.
Examples	The following example demonstrates how to enable the accounting update function. `DES-7210(config)# aaa new-model`

Related commands	**Command**	**Description**
	aaa new-model	Enable the AAA security service.
	aaa accounting network	Define a network accounting method list.

45.3.5 aaa accounting update periodic

If the accounting update function has been enabled, use this command to set the interval of sednign the accounting update message. The **no** form of this command is used to restore it to the default value.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter description	**Parameter**	**Description**
	interval	Interval of sending the accounting update message, in minute. The shortest interval is 1 minute.

Default	5 minutes.
Command mode	Global configuration mode.
Usage guidelines	If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Examples	The following example demonstrates how to set the interval of accounting update to 1 minute.
	`DES-7210(config)# aaa new-model`
	`DES-7210(config)# aaa accounting update`
	`DES-7210(config)# aaa accounting update periodic 1`

Related commands	**Command**	**Description**
	aaa new-model	Enable the AAA security service.
	aaa accounting network	Define a network accounting method list.

45.3.6 accounting commands

Use this command to apply the accounting command list to the specified terminal lines. The **no** form of this command is used to disable the accounting function.

accounting commands *level* {**default** | *list-name*}

no accounting commands *level*

Parameter description

Parameter	Description
level	The accounting command level, 0-15. The message shall be recorded before determing which command level is executed.
default	Use the default method of accouting commands.
list-name	Use a defined command accouting method list.

Default

Disabled.

Command mode

Line configuration mode.

Usage guidelines

Once the default command accouting method list has been configured, it is applied to all terminals automatically. Once the non-default command accounting method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the command authorization in this line is ineffective till the accounting command method list is defined.

Examples

The following example configures the accounting command method list with name cmd, accounts the level-15 command, uses the TACACS+ server. If the security server does not response, it does not perform accounting. After configuration, the accounting command is applied to VTY 0-4 lines:

```
DES-7210(config)# aaa accounting commands 15 cmd group tacacs+ none
DES-7210(config)# line vty 0 4
DES-7210(config-line)# accounting commands 15 cmd
```

Related

Command	Description

commands	**aaa new-model**	Enable the AAA security service.
	aaa accouting commands	Define the method list of AAA accouting command.

45.3.7 accounting exec

Use this command to apply the exec accouting method list to the specified terminal lines in the line configuration mode. The **no** form of this command is used to disable the exec accounting function.

accounting exec {**default** | *list-name*}

no accounting exec

Parameter description	**Parameter**	**Description**
	default	Use the default method of Exec accouting.
	list-name	Use a defined Exec accouting method list.

Default	Disabled.
Command mode	Line configuration mode.
Usage guidelines	Once the default exec accouting method list has been configured, it is applied to all terminals automatically. Once the non-default exec accounting method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the exec accounting in this line is ineffective till the exec accounting command method list is defined.

Examples	The following example configures the exec accounting method list with name exec-1, uses the RADIUS server. If the security server does not response, it does not perform accounting. After configuration, the exec accounting is applied to VTY 0-4 lines:
	`DES-7210(config)# aaa accounting exec exec-1 group radius none`
	`DES-7210(config)# line vty 0 4`
	`DES-7210(config-line)# accounting exec exec-1`

Related commands	Command	Description
	aaa new-model	Enable the AAA security service.
	aaa accouting commands	Define the method list of AAA Exec accouting.

45.4 AAA Server Group Commands

45.4.1 aaa group server

Use this command to configure the AAA server group. The **no** form of this command is used to delete the server group.

aaa group server {**radius** | **tacacs+**} *name*

no aaa group server {**radius** | **tacacs+**} *name*

Parameter description	Parameter	Description
	name	Name of the server group. It cannot be the keywords "**radius"** and "**tacacs+**".

Command mode	Global configuration mode.

Usage guidelines	This command is used to configure the AAA server group. Currently, the RADIUS and TACACS+ server groups are supported.

Examples

The following example configures an AAA server group.

```
DES-7210(config)# aaa group server radius ss
DES-7210(config-gs-radius)# end
DES-7210#show aaa group
Group-name:  ss
Group Type:  radius
Referred:    1
Server List:
```

Related commands	Command	Description
	show aaa group	Show the AAA server group information.

45.4.2 ip vrf forwarding

Use this command to select the **vrf** for the AAA server group. The **no** form of this command removes the setting.

ip vrf forwarding *vrf_name*

no ip vrf forwarding

Parameter description

Parameter	Description
vrf_name	VRF name

Default Configuration

N/A.

Command mode

Server group configuration mode.

Usage guidelines

This command selects VRF for the specified server groups.

Examples

The following example selects the VRF for the server group.

```
DES-7210(config)# aaa group server radius ss
DES-7210(config-gs-radius)# server 192.168.4.12
DES-7210(config-gs-radius)# server 192.168.4.13
DES-7210(config-gs-radius)# ip vrf forwarding vrf_name
DES-7210(config-gs-radius)# end
```

Related commands

Command	Description
aaa group server	Configure the AAA server group.
show aaa group	Show the AAA server group information.

45.4.3 server

Use this command to add a server to the AAA server group. The **no** form is used to delete a server.

server *ip-addr* [**authen-port** *port1*] [**acct-port** *port2*]

no server *ip-addr* [**authen-port** *port1*] [**acct-port** *port2*]

Parameter description

Parameter	Description
ip-addr	IP address of the server
port1	Authentication port of the server
port2	Accounting port of the server

Default

No server is configured.

Command mode

Server group configuration mode.

Usage guidelines

Add a server to the specified server group. The default value is used if no port is specified.

Examples

The following example adds a server to the server group.

```
DES-7210(config)# aaa group server radius ss
DES-7210(config-gs-radius)# server 192.168.4.12
acct-port 5 authen-port 6
DES-7210(config-gs-radius)# end
DES-7210# show aaa group
Group-name: ss
Group Type: radius
Referred:   2
Server List:
IP Address: 192.168.4.12
Authentication Port: 6
Accounting Port: 5
Referred: 1
```

Related commands

Command	Description
aaa group server	Configure the AAA server group.
show aaa group	Show the AAA server group information.

45.4.4 show aaa group

Use this command to show all the server groups configured for AAA.

show aaa group

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples	The following example shows all the server groups configured for AAA.
	`DES-7210# show aaa group`
	`Group Name: ss`
	`Group Type: radius`
	`Referred: 2`
	`Server List:`
	`IP Address: 192.168.217.64`
	`Authentication Port: 1812`
	`Accounting Port: 1813`
	`Referred: 1`

Related commands

Command	Description
aaa group server	Configure the AAA server group.

45.5 Other AAA Commands

45.5.1 aaa local authentication attempts

Use this command to configure login attempt times .

aaa local authentication attempts *max-attempts*

Parameter description	In the range of 1 to 2147483647.
Default	The default value is 3.

Command mode	Global configuration mode.
Usage guidelines	Use this command to configure login attempt times.
Examples	DES-7210 #**configure terminal** DES-7210 (config)#**aaa local authentication attempts** 6

Related commands	**Command**	**Description**
	show running-config	Show the current configuration of the switch.
	show aaa lockout	Show the lockout configuration parameter of current login.

45.5.2 aaa local authentication lockout-time

Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times .

aaa local authentication lockout-time *lockout-time*

Parameter description	In the range of 1 to 2147483647.
Default	15 hours.
Command mode	Global configuration mode.
Usage guidelines	Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times .
Examples	DES-7210#**configure terminal** DES-7210(config)#**aaa local authentication lockout-time** 5

Related	**Command**	**Description**

commands	**show running-config**	Show the current configuration of the switch.
	show aaa lockout	Show the lockout configuration parameter of current login.

45.5.3 aaa new-model

Use this command to enable the DES-7200 AAA security service. The **no** form of this command is used to disable the AAA security service.

aaa new-model

no aaa new-model

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.
Examples	The following example shows how to enable the AAA security service. `DES-7210(config)# aaa new-model`

Related commands	**Command**	**Description**
	aaa authentication	Define a user authentication method list.
	aaa authorization	Define a user authorization method list.
	aaa accouting	Define a user accouting method list.

45.5.4 clear aaa local user lockout

Use this command to clear the lockout user list.

clear aaa local user lockout {all | user-name <*word*>**}**

Parameter description

Parameter	Description
word	User ID.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines Use this command to clear all the user lists or the specified user list.

Examples

```
DES-7210(config)# clear aaa local user lockout all
```

Related commands

Command	Description
show running-config	Show the current configuration of the switch.
show aaa lockout	Show the lockout configuration parameter of current login.

45.5.5 debug aaa

Use this command to turn on the AAA service debugging switch. The **no** form of this command is used to turn off the debugging switch.

debug aaa event

no debug aaa event

Parameter description N/A.

Command mode Privileged EXEC mode.

45.5.6 show aaa method-list

Use this command to show all AAA method lists.

show aaa method-list

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to show all AAA method lists.

Examples	The following example shows the AAA method list.
	`DES-7210# show aaa method-list`
	`Authentication method-list`
	`aaa authentication login default group radius`
	`aaa authentication ppp default group radius`
	`aaa authentication dot1x default group radius`
	`aaa authentication dot1x san-f local group angel group rain none`
	`aaa authentication enable default group radius`
	`Accounting method-list`
	`aaa accounting network default start-stop group radius`
	`Authorization method-list`
	`aaa authorizating network default group radius`

Related commands

Command	Description
aaa authentication	Define a user authentication method list
aaa authorization	Define a user authorization method list
aaa accounting	Define a user accounting method list

45.5.7 show aaa user lockout

Use this command to show the lockout user list.

show aaa local user lockout {all | user-name <*word*>**}**

Parameter description

Parameter	Description
word	User ID.

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to show the lockout user list and show how long the lockout-time is.
Examples	`DES-7210# show aaa user lockout all`

Related commands

Command	Description
show running-config	Show the current configuration of the switch.
show aaa lockout	Show the lockout configuration parameter of current login.

46 RADIUS Configuration Commands

46.1 Configuration Related Commands

RADIUS configuration includes following commands:

- **ip raius source-interface**
- **radius-server host**
- **radius-server key**
- **radius-server retransmit**
- **radius-server timeout**
- **radius-server dead-time**
- **radius attribute**
- **radius set qos cos**
- **radius vendor-specific extend**

46.1.1 ip radius source-interface

Use this command to specify the source IP address for the RADIUS packets. Use the **no** form of this command to delete the source IP address for the RADIUS packet.

ip radius source-interface *interface*

no radius source-interface

Parameter description

Parameter	Description
Interface	Interface that the source IP address of the RADIUS packet belongs to.

Default

The source IP address of the RADIUS packet is set by the network layer.

Command mode

Global configuration mode.

Usage guidelines

In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

Examples

The following example specifies that the RADIUS packet obtains an IP address from the fastEthernet 0/0 interface and uses it as the source IP address of the RADIUS packet:

```
DES-7210(config)# ip radius source-interface fastEthernet 0/0
```

Related commands

Command	Description
radius-server host	Define the RADIUS server.
ip address	Configure the IP address of the interface.

46.1.2 radius-server host

Use this command to specify a RADIUS security server host. The **no** form of this command is used to delete the RADIUS security server host.

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

no radius-server host {*hostname* | *ip-address*}

Parameter description

Parameter	Description
hostname	DNS name of the RADIUS security server host.
ip-address	IP address of the RADIUS security server host.
auth-port	UDP port used for RADIUS authentication.
port-number	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
acct-port	UDP port used for RADIUS accounting.

	port-number	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.

Default No RADIUS host is specified.

Command mode Global configuration mode.

Usage guidelines In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server** command.

Examples The following example defines a RADIUS security server host:

```
DES-7210(config)# radius-server host 192.168.12.1
```

Related commands

Command	Description
aaa authentication	Define the AAA authentication method list
radius-server key	Define a shared password for the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server timeout	Define the timeout for the RADIUS packet.

46.1.3 radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server. The **no** form of this command is used to remove the shared password.

radius-server key [0 | 7] *text-string*

no radius-server key

Parameter description

Parameter	Description
text-string	Text of the shared password
0 | 7	Password encryption type.

		0: no encryption; 7: Simply-encrypted.

Default No shared password is specified.

Command mode Global configuration mode.

Usage guidelines A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

Examples The following example defines the shared password **aaa** for the RADIUS security server:

```
DES-7210(config)# radius-server key aaa
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server timeout	Define the timeout for the RADIUS packet.

46.1.4 radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond. The **no** form of this command is used to restore it to the default setting.

radius-server retransmit *retries*

no radius-server retransmit

Parameter description

Parameter	Description
retries	Number of retransmissions

Default The default number of retransmissions is 3.

Command mode	Global configuration mode.
Usage guidelines	AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.
Examples	The following example sets the number of retransmissions to 4: `DES-7210(config)# radius-server retransmit 4`

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the timeout for the RADIUS packet.

46.1.5 radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet. The **no** format of this command is used to restore it to the default setting.

radius-server timeout *seconds*

no radius-server timeout

Parameter description

Parameter	Description
seconds	Timeout in the range 1 to1000 seconds.

Default	5 seconds.
Command mode	Global configuration mode.

Usage guidelines

Use this command to change the timeout of packet retransmission.

Examples

The following example sets the timeout to 10 seconds:

```
DES-7210(config)# radius-server timeout 10
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of the RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.

46.1.6 radius-server deadtime

If the device has not received any response from the sever within the specified time, it considers the server dead. The time t is called deadtime. DES-7200 operating system supports to set the RADIUS deadtime. Use this command to set the deadtime. The **no** format of this command is used to restore it to the default setting.

radius-server deadtime *minnutes*

no radius-server deadtime

Parameter description

Parameter	Description
minutes	Dead time (in minutes). The value range is 1 to 1000 seconds.

Default

5 Minutes.

Command mode

Global configuration mode.

Usage guidelines

N/A.

Examples

The following example sets the deadtime to 10 minutes:

```
DES-7210(config)# radius-server deadtime 10
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of the RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the timeout for the packet retransmission.

46.1.7 radius attribute

radius attribute {*id* **| down-rate-limit | dscp | mac-limit | up-rate-limit**} **vendor-type** *type*

no radius attribute {*id* **|down-rate-limit | dscp | mac-limit | up-rate-limit**} **vendor-type**

Parameter description

Parameter	Description
id	Function ID in the range 1 to 255
type	Private attribute type

Default

Only the default configuration of private attributes in DES-7210 is recognized.

id	Function	Type
1	max down-rate	1
2	qos	2
3	user ip	3
4	vlan-id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-diractory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14

15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilige	22
23	login privilige	42

Extended attributes:

id	Function	Type
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan-id.	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-diractory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21

22	ip privilige	22
23	login privilige	42
24	limit to user number	50

Command mode Global configuration mode.

Usage guidelines Use this command to configure the type value of a private attribute.

Examples The following example sets the type of max up-rate to 211:

```
DES-7210(config)# radius attribute 16 vendor-type 211
```

Related commands

Command	Description
radius set qos cos	Set the qos value sent by the RADIUS server as the cos value of the interface.

46.1.8 radius set qos cos

Use this command to set the qos value sent by the RADIUS server as the cos value of the interface. Use the **no** form of this command to restore it to the default setting.

radius set qos cos

no radius set qos cos

Parameter description N/A.

Default Set the qos value sent by the RADIUS server as the dscp value.

Command mode Global configuration mode.

Usage guidelines Set the qos value sent by the RADIUS server as the cos value, and the dscp value by default.

Examples The following example sets the qos value sent by the RADIUS server as the cos value of the interface.:

	DES-7210(config)# **radius set qos cos**

	Command	Description
Related commands	**radius vendor-specific extend**	Extend RADIUS not to differentiate the IDs of private vendors.

46.1.9 radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors. Use the **no** form of this command to disable the function.

radius vendor-specific extend

no radius vendor-specific extend

Parameter description	N/A.
Default	Only the private vendor IDs of DES-7210 are recognized.
Command mode	Global configuration mode.
Usage guidelines	Use this command to identify the attributes of all vendor IDs by type.
Examples	The following example extends RADIUS not to differentiate the IDs of private vendors: DES-7210(config)# **radius vendor-specific extend**

	Command	Description
Related commands	**radius attribute**	Configure vendor type.
	radius set	Set the qos value sent by the RADIUS server as the cos value of the interface.

46.2 Show Related Commands

- **debug radius [event | detail]**
- **show radius-server**
- **show radius parameter**

- **show radius vendor-specific**

46.2.1 debug radius

Use this command to turn on the RADIUS debugging switch. The **no** form of this command is used to turn off the RADIUS debugging switch.

debug radius {**event | detail**}

no debug radius {**event | detail**}

Parameter Description	N/A.
Command mode	Privileged EXEC configuration mode.

46.2.2 show radius server

Use this command to show the configuration of the RADIUS server.

show radius server

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	DES-7210# **show radius server** server ip : 192.168.4.12 acct port: 23 authen port: 77 server state: ready server ip : 192.168.4.13 acct port: 45 authen port: 74 server state: ready

	Command	Description
Related commands	**radius-server host**	Define the RADIUS security server.
	radius-server retransmit	Define the number of RADIUS packet retransmissions.
	radius-server key	Define a shared password for the RADIUS server.
	radius-server timeout	Define the packet transmission timeout.

46.2.3 show radius parameter

Use this command to show the global parameters of the RADIUS server.

show radius parameter

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	DES-7210# **show radius parameter** Server Timout: 5 Seconds Server Deadtime: 5 Minutes Server Retries: 3 Server Key: ******

	Command	Description
Related commands	**radius-server host**	Define the RADIUS security server.
	radius-server retransmit	Define the number of RADIUS packet retransmissions.
	radius-server key	Define a shared password for the RADIUS server.
	radius-server	Define the packet transmission timeout.

	timeout	

46.2.4 show radius vendor-specific

Use this command to show the configuration of the private vendors.

show radius vendor-specific

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	DES-7210# **show radius vendor-specific** id vendor-specific type-value ----- -------------------- ---------- 1 max down-rate 76 2 qos 77 3 user ip 3 4 vlan id 4 5 version to client 5 6 net ip 6 7 user name 7 8 password 8 9 file-diractory 9 10 file-count 10 11 file-name-0 11 12 file-name-1 12 13 file-name-2 13 14 file-name-3 14 15 file-name-4 15 16 max up-rate 75 17 version to server 17 18 flux-max-high32 18 19 flux-max-low32 19 20 proxy-avoid 20 21 dailup-avoid 21 22 ip privilige 22 23 login privilige 42

```
24    limit to user number  50
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the packet transmission timeout.

47 TACACS+ Configuration Commands

47.1 Related Commands of TACACS+ Configuration

TACACS+ configuration includes the following related commands:

- **aaa group server tacacs+**
- **server(TACACS+)**
- **ip vrf forwarding(TACACS+)**
- **ip tacacs source-interface**
- **tacacs-server host**
- **tacacs-server key**
- **tacacs-server timeout**

47.1.1 aaa group server tacacs+

Use this command to configure TACACS+ group server, dividing different TACACS+ servers to the different groups.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Parameter description

Parameter	Description
group_name	TACACS+ server group name

Default Configuration

No TACACS+ server group is configured.

Command mode

Global configuration mode.

Usage

By dividing TACACS+ servers into several groups, the tasks of

guidelines	anthentication, authorization and accounting can be implemented by different server groups.

Examples

The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group:

```
DES-7210(config)#aaa group server tacacs+ tac1
DES-7210(config-gs-tacacs+)#server 1.1.1.1
```

Related commands

Command	Description
server	Configure server list of TACACS+ server group.
ip vrf forwarding	Configure VRF name supported by TACACS+ server group.

47.1.2 server(TACACS+)

Use this command to configure server address in TACACS+ group server.

server *ip-address*

no server *ip-address*

Parameter description

Parameter	Description
ip-address	server address in TACACS+ group server

Default Configuration	N/A
Command mode	TACACS+ group server configuration mode.
Usage guidelines	You must enter TACACS+ server group configuration mode to configure this command. To configure server address in TACACS+ group server, you must execute **tacacs-server host** in the global configuration mode. For the server address in TACACS+ group servers, when one server does not reply, it will send the request to the next server.

Examples

The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group:

```
DES-7210(config)#aaa group server tacacs+ tac1
DES-7210(config-gs-tacacs+)#server 1.1.1.1
```

Related commands

Command	Description
aaa group server tacacs+	Configure TACACS+ server group.
ip vrf forwarding	Configure VRF name supported by TACACS+ server group.

47.1.3 ip vrf forwarding(TACACS+)

Use this command to configure vrf name used by TACACS+ group server (this command exists in the device supporting VRF)

ip vrf forwarding *vrf-name*

no ip vrf forwarding

Parameter description

Parameter	Description
vrf-name	VRF name.

Default Configuration

N/A

Command mode

TACACS+ group server configuration mode.

Usage guidelines

Specify vrf name to the specified TACACS+ server.

Examples

The following example specifies VRF name as vpn1 to TACACS+ server group:

```
DES-7210(config)# aaa group server tacacs+ tac1
DES-7210(config-gs-radius)# server 1.1.1.1
DES-7210(config-gs-radius)# ip vrf forwarding vpn1
```

	Command	Description
Related commands	**aaa group server tacacs+**	Configure TACACS+ server group.
	server	Configure server list of TACACS+ server group.

47.1.4 ip tacacs source-interface

Use this command to configure the source address of TACACS+ packet:

ip tacacs source-interface *interface*

no ip tacacs source-interface

	Parameter	Description
Parameter description	*Interface*	Source address interface of TACACS+ packet

Default Configuration	The source address of TACACS+ packet is set on network layer.
Command mode	Global configuration mode.
Usage guidelines	To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to set the source address of TACACS+ packet. This command specifies the first ip address of the specified interface as the source address of TACACS+ packet and is used on L3 devices.
Examples	The following example specifies TACACS+ packet to obtain ip address from fastEthernet 0/0 as the source address of TACACS+ packet : `DES-7210(config)# ip tacacs source-interface fastEthernet 0/0`

	Command	Description
Related commands	**tacacs-server host**	Define TACACS+ server.
	ip address	Configure ip address of the interface.

47.1.5 tacacs-server host

Use this command to configure IP address of TACACS+ server host:

tacacs-server host *ip-address* [**port** *integer*] [**timout** *integer*] [**key [0|7]** *string*]

no tacacs-server host *ip-address*

Parameter description

Parameter	Description
Ip-address	IP address of TACACS+ server host.
port *integer*	TCP port used in TACACS+ communication.
timeout *integer*	Timeout time of TACACS+ host.
key *string*	Shared keyword of TACACS+ client and server.
0 | 7	Password encryption type. 0: no encryption; 7: simply-encrypted.

Default Configuration

No specified TACACS+ host.

Command mode

Global configuration mode.

Usage guidelines

To use TACACS+ to implement AAA security service, you must define TACACS+ secure server. You can define one or multiple TACACS+ secure servers by using **tacacs-server.**

Examples

The following example defines a TACACS+ secure server host:

```
DES-7210(config)# tacacs-server host 192.168.12.1
```

Related commands

Command	Description
aaa authentication	Define AAA identity authentication method list.

	tacacs-server key	Define the shared password of TACACS+ secure server globally.
	tacacs-server timeout	Define timeout timer of reply packet of TACACS+ server globally.

47.1.6 tacacs-server key

Use this command to configure global password of TACACS+ :

tacacs-server key [*0* | *7*] *string*

no tacacs-server key

Parameter description

Parameter	Description
string	Text of shared password.
***0*	*7***	Encryption type of password, 0 indicates no encryption ; 7 indicates being simply encrypted.

Default Configuration

No specified shared password.

Command mode

Global configuration mode.

Usage guidelines

The device and TACACS+ secure server communicates with each other successfully on the basis of the shared password. Therefore, in order to make the device and TACACS+ secure server communicate with each other, the same shared password must be defined on both of them. When we need to specify different passwords to every server, use key option in host command. We can set a key to all the servers that have not set key option in global configuration mode.

Examples

The following example defines the shared password of TACACS+ secure server as aaa:

```
DES-7210(config)# tacacs-server key aaa
```

Related commands

Command	Description
tacacs-server host	Define TACACS+ secure server host.

	tacacs-server timeout	Define the timeout timer of TACACS+ packet.

47.1.7 tacacs-server timeout

Use this command to configure the global timeout time waiting for the server when communicatin with TACACS+ server :

tacacs-server timeout *seconds*

no tacacs-server timeout

Parameter description

Parameter	Description
seconds	Timeout time (s) in the range 1 to 1000s.

Default Configuration

5s.

Command mode

Global configuration mode.

Usage guidelines

Use this command to adjust the timeout time of reply packet. When we need to specify different timeout time to every server, use timeout option in host command. We can set a timeout to all the servers that have not set timeout option in global configuration mode.

Examples

The following example shows how to define the timeout time as 10s:

```
DES-7210(config)# tacacs-server timeout 10
```

Related commands

Command	Description
tacacs-server host	Define TACACS+ secure server host.
tacacs-server key	Define the shared password of TACACS+.

47.2 TACACS+ Privileged Command

- **debug tacacs+**
- **show tacacs**

47.2.1 debug tacacs+

Use this command to turn on the TACACS+ debugging switch. The **no** form of this command turns off the TACACS+ debugging switch.

debug tacacs+

no debug tacacs+

Parameter description	N/A.
Command mode	Privileged EXEC mode.

47.2.2 show tacacs

Use this command to show the interoperation condition with each TACACS+ server.

show tacacs

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to show the interoperation condition with each TACACS+ server.
Examples	`DES-7210# show tacacs`

```
Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Related commands

Command	Description
tacacs-server host	Define and show TACACS+ secure server host which interacts with every TACACS+ server.

48 SSH Configuration Commands

48.1 Related Configuration Commands

SSH configuration includes following commands:

- **crypto key generate**
- **crypto key zeroize**
- **ip ssh version**
- **ip ssh time-out**
- **ip ssh authentication-retries**

48.1.1 crypto key generate

In global configuration mode, use this command to generate a public key on the SSH server:

crypto key generate {**rsa|dsa**}

Parameter description

Parameter	Description
rsa	Generate an RSA key.
dsa	Generate a DSA key.

Default configuration

By default, the SSH server does not generate a public key.

Command mode

Global configuration mode.

Usage guidelines

When you need to enable the SSH Server service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command **enable service ssh-server** at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a

RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.

Caution A key can be deleted by using the **crypto key zeroize** command. The **no crypto key generate** command is not available.

Examples

```
DES-7210# configure terminal
DES-7210(config)# crypto key generate rsa
```

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.
crypto key zeroize {rsa | dsa}	Delete DSA and RSA keys and disable the SSH Server function.

Version description

The software version must be R10.1 and later.

48.1.2 crypto key zeroize

In global configuration mode, use this command to delete the public key on the SSH server.

crypto key zeroize {**rsa | dsa**}

Parameter description

Parameter	Description
rsa	Delete the RSA key.
dsa	Delete the DSA key.

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

This command deletes the public key of the SSH Server. After the key is deleted, the SSH Server state becomes DISABLE. If you want to disable the SSH Server, run the **no enable service ssh-server** command.

Examples

```
DES-7210# configure terminal
DES-7210(config)# crypto key zeroize rsa
```

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.
crypto key generate {rsa|dsa}	Generate DSA and RSA keys.

Version description

The software version must be R10.1 and later.

48.1.3 ip ssh version

Use this command to set the version of the SSH server. Use the **no** form of this command to restore it to the default setting.

ip ssh version {**1** | **2**}

no ip ssh version

Parameter description

Parameter	Description
1	Support the SSH1 client connection request.
2	Support the SSH2 client connection request.

Default configuration

SSH1 and SSH2 are compatible by default. When a version is set, the connection sent by the SSH client of this version is accepted only. The **no ip ssh version** command can also be used to restore it to the default setting.

Command mode

Global configuration mode.

Usage guidelines

This command is used to configure the SSH connection protocol version supported by SSH Server. By default, the SSH Server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH Server. Use the **show ip ssh** command to show the current status of SSH Server.

Examples

The following example sets the version of the SSH Server:

```
DES-7210# configure terminal
DES-7210(config)# ip ssh version 2
```

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.

Version description

The software version must be R10.1 and later.

48.1.4 ip ssh time-out

Use this command to set the authentication timeout for the SSH Server. Use the **no** form of this command to restore it to the default setting.

ip ssh time-out *time*

no ip ssh time-out

Parameter description

Parameter	Description
time	Authentication timeout

Default configuration

The timeout value is 120s by default.

Command mode

Global configuration mode.

Usage guidelines

The authentication is considered timeout and failed if the authentication is not successful within 120s starting from receiving a connection request. Use the **show ip ssh** command to view the configuration of the SSH server.

Examples

The following example sets the timeout value as 100s:

```
DES-7210# configure terminal
DES-7210(config)# ip ssh time-out 100
```

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.

Version description	The software version must be R10.1 and higher.

48.1.5 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH Server. Use the **no** form of this command to restore it to the default setting.

ip ssh authentication-retries *retry times*

no ip ssh authentication-retries

Parameter description

Parameter	Description
retry times	Authentication retry times

Default configuration	The default authentication retry times is 3.
Command mode	Global configuration mode.
Usage guidelines	User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to view the configuration of the SSH Server.

Examples	The following example sets the authentication retry times to 2:
	`DES-7210# configure terminal`
	`DES-7210(config)# ip ssh ssh authentication-retries 2`

Related commands

Command	Description
show ip ssh	Show the current status of the SSH Server.

Version description	The software version must be R10.1 and higher.

48.2 Showing Related Commands

The showing and monitoring commands of the SSH Server include:

- **show ip ssh**

- **show ssh**
- **show crypto key mypubkey**
- **disconnect ssh**

48.2.1 show ip ssh

Use this command to show the information of the SSH Server.

show ip ssh

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the information of the SSH Server, including version, enablement state, authentication timeout, and authentication retry times. Note: If no key is generated for the SSH Server, the SSH version is still unavailable even if this SSH version has been configured.
Examples	`DES-7210# show ip ssh`

Related commands

Command	Description
ip ssh version {**1** | **2**}	Configure the version for the SSH Server.
ip ssh time-out time	Set the authentication timeout for the SSH Server.
ip ssh authentication-retries retry times	Set the authentication retry times for the SSH Server.

Version description	The software version must be R10.1 and higher.

48.2.2 show ssh

Use this command to show the information about the SSH connection.

show ssh

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the information about the established SSH connections, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.
Examples	`DES-7210# show ssh`
Related commands	N/A.
Version description	The software version must be R10.1 and higher.

48.2.3 show crypto key mypubkey

Use this command to show the information about the public key part of the public key on the SSH Server.

show crypto key mypubkey {rsa/dsa}

Parameter description

Parameter	Description
rsa	Show the public key part of the RSA key.
dsa	Show the public key part of the DSA key.

Default configuration N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to show the information about the public key part of the generated public key on the SSH Server, including key generation time, key name, contents in the public key part, etc.
Examples	`DES-7210# show crypto key mypubkey rsa`

Related commands

Command	Description
crypto key generate {rsa | dsa}	Generate DSA and RSA keys.

Version description	The software version must be R10.1 and higher.

48.2.4 disconnect ssh

Use this command to disconnect the established SSH connection.

disconnect ssh [vty] *session-id*

Parameter description

Parameter	Description
session-id	ID of the established SSH connection session.

Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	You can disconnect a SSH connection by entering the ID of the SSH connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.
Examples	`DES-7210# disconnect ssh 1 Or` `DES-7210# disconnect ssh vty 1`

	Command	Description
Related commands	**show ssh**	Show the information about the established SSH connection.
	clear line vty *line_number*	Disconnect the current VTY connection.

Version description	The software version must be R10.1 and higher.

49 CPU Protection Configuration Commands

49.1 Related Configuration Commands

Configuration commands for anti-attack includes:

- **cpu-protect type** *packet-tpye* **pps** *pps_value*
- **cpu-protect type** *packet-tpye* **pri** *pri_value*

49.1.1 cpu-protect type packet-type pps pps_value

Use this command to set the bandwidth for the CPU port to receive the specified type of packets.

cpu-protect type { **arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **ttl1** | **unknown-ipmc** | **dvmrp** } **pps** *pps_value*

Parameter description

Parameter	Description
pps_value	Packets per second.

Default

The default bandwidth that the CPU uses to receive various types of packets is 1000 pps.

Command mode

Global configuration mode.

Examples

The following example sets the bandwidth for the CPU to receive BPDU packets as 100pps:

```
DES-7210(config)# cpu-pr type bpdu pps 100
Set packet type bpdu pps 100.
```

Related commands

Command	Description
cpu-protect type packet-type pri *pri_num*	Set the priority for the packets the CPU port receives.

49.1.2 cpu-protect type packet-type pri *pri_num*

Use this command to set the priority for the specified type of packets the CPU port receives.

cpu-protect type { **arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **ttl1** | **unknown-ipmc** | **dvmrp** } **pri** *pri_num*

Parameter description

Parameter	Description
pri_num	Packet priority in the range 0 to 7

Default The default is 0 for various types of packets.

Command mode Global configuration mode.

Examples The following example sets the priority of the BPDU packets as 7:

```
DES-7210(config)# cpu-protect type bpdu pri 7
Set packet type bpdu pri 7.
```

Related commands

Command	Description
cpu-protect type packet-type pps *pps_value*	Set the bandwidth for the CPU to receive the specified type of packets.

49.2 Showing Related Command

The related commands for CPU protection include:

- **show cpu-protect mboard**
- **show cpu-protect slot** *slot-id*
- **show cpu-protect type** *packet-type*

49.2.1 show cpu-protect mboard

Use this command to show the statistics of various packets of CPU protection on the management board.

show cpu-protect mboard

Command mode	Privileged EXEC mode.
Usage guidelines	This command shows the statistics of the packets received by CPU on the management board.

Examples

```
DES-7210# show cpu-protect mboard
 Type            Pps      Total    Drop
 ------------    -------- ------- ---------
 arp             500       19       0
 bpdu            200       24       0
 dhcp            0         0        0
 gvrp            0         0        0
 ipv6-mc         0         0        0
 dvmrp           0         0        0
 igmp            0         0        0
 ospf            0         0        0
 pim             0         0        0
 rip             0         0        0
 vrrp            0         0        0
 unknown-ipmc    0         0        0
 ttl1            0         0        0
...
```

Related commands

Command	Description
show cpu-protect slot *slot-num*	Show the statistics of the CPU protection on the specified line card.

49.2.2 show cpu-protect slot

Use this command to show the CPP statistics on the specified line card.

show cpu-protect slot *slot_num*

Parameter description

Parameter	Description
slot_num	1-16.

Command mode	Privileged EXEC mode.

Usage guidelines

This command shows the CPP statistics on the specified line card.

Examples

The following example shows the CPU protection information on the line card in slot 2.

```
DES-7210(config)# show cpu-protect slot 2
 Type          Pps      Total     Drop
 -----------   --------- --------- ---------
 arp           200      200       15
 bpdu          200        8        0
 dhcp          200        0        0
 gvrp          200        0        0
 ipv6-mc       200        0        0
 dvmrp         200        0        0
 igmp          200        0        0
 ospf          200        0        0
 pim           200        0        0
 rip           200        0        0
 vrrp          200        0        0
 unknown-ipmc  200        0        0
 ttl1          20         3        0
```

Related commands

Command	Description
show cpu-protect mboard	Show the CPU protect information on the management board.

49.2.3 show cpu-protect type

Use this command to show the statistics of the specified type of packets:

show cpu-protect type { **arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **ttl1** | **unknown-ipmc** | **dvmrp** } *dvmrp*

Command mode

Privileged EXEC mode.

Usage guidelines

This command shows the statistics of the specified type of packets:

Examples

The following example shows the statistics of the BPDU packets by using the **show cpu-protect type bpdu** command:

```
DES-7210(config)# show cpu-protect type arp
 Slot        Type        Pps       Total     Drop
 ---------   ----------- --------- --------- ---------
 MainBoard   bpdu         100        30        0
 Slot-2      bpdu         100        30        0
```

Related commands

Command	Description
show cpu-protect type *packet-type*	Show the statistics of the packets of a specified type of CPU protection.

50 Anti-attack System Guard Configuration Commands

50.1 Configuration Related Commands

There are the following configuration commands for system attack guard:

- **system-guard enable**
- **system-guard isolate-time seconds**
- **system-guard same-dest-ip-attack-packets number**
- **system-guard same-dest-ip-attack-packets number**
- **system-guard detect-maxnum number**
- **system-guard exception-ip ip mask**
- **clear system-guard [interface** *interface-id* **[ip-address** *ip-address*]]

50.1.1 system-guard enable

Use this command to enable the anti-attack function. The **no** format of the command disables the anti-attack function.

system-guard enable

no system-guard enable

Parameter description	N/A.
Default	Disabled.
Command mode	Interface configuration mode.

Examples

Enable the anti-attack function:

```
DES-7210(config-if)# system-guard enable
```

Disable the anti-attack function:

```
DES-7210(config-if)# no system-guard enable
```

Related commands

Command	Description
show system-guard	Show the anti-attack configuration.

50.1.2 system-guard isolate-time seconds

Use this command to set the isolation time of the unauthorized users. Use the **no** form of the command to restore it to the default value.

system-guard isolate-time *seconds*

no system-guard isolate-time

Parameter description

Parameter	Description
seconds	Isolation time of the unauthorized users in the range 30s to 3600s, 120s by default. The isolated IP address will automatically recover the communications after the specified period of isolation time.

Default

The default isolation time is 120 seconds.

Command mode

Interface configuration mode.

Usage guidelines

No communication is allowed for the isolated IP address within the period of ***second***. The isolated IP address will automatically recover the communications after the specified period of time.

Examples

Configure the isolation time as 100 seconds:

```
DES-7210(config-if)# system-guard isolate-time 100
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function.

50.1.3 system-guard same-dest-ip-attack-packets number

Use this command to configure the maximum number of packets attacking an inexistent IP address. Use the **no** form of the command to restore it to the default value.

system-guard same-dest-ip-attack-packets *number*

no system-guard same-dest-ip-attack-packets

Parameter description

Parameter	Description
number	Maximum number of the IP packets attacking an inexistent IP address. The value range is 0 to 2000 packets per second, 20 packets by default. Zero indicates this attack is not monitored.

Default The default value is 20 packets per second.

Command mode Interface configuration mode.

Usage guidelines The less the threshold is set, the poorer the accuracy of the attack judgment is. It is easy to isolate the normal host online incorrectly. It is recommended that administrators configure a threshold according to the security degree of the actual network environment.

Examples Configure the maximum number of the packets as 100:

```
DES-7210(config-if)# system-guard
same-dest-ip-attack-packets 100
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function.

50.1.4 system-guard scan-dest-ip-attack-packets number

Use this command to configure the maximum number of IP packets attacking a batch of IP segments. Use the **no** form of the command to restore it to the default value.

system-guard scan-dest-ip-attack-packets *number*

no system-guard scan-dest-ip-attack-packets

Parameter description

Parameter	Description
number	Maximum number of the IP packets attacking a batch of IP network segment. The value range is 1 to 2000 IP packets per second, 10 IP packets by default. Zero indicates this attack is not monitored.

Default

The default value is 10.

Command mode

Interface configuration mode.

Usage guidelines

The less the threshold is set, the poorer the accuracy of the attack judgment is. It is easy to isolate the normal host online incorrectly. It is recommended that administrators configure a corresponding threshold according to the security degree of the actual network environment.

Examples

Configure the maximum number of IP packets as 100”

```
DES-7210(config-if)# system-guard
scan-dest-ip-attack-packets 100
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function.

50.1.5 system-guard detect-maxnum number

Use this command to set the maximum quantity of attacked hosts. Use the **no** form of the command to restore it to the default value.

system-guard detect-maxnum *number*

no system-guard detect-maxnum

Parameter description

Parameter	Description
number	Maximum number of the IP packets attacking a batch of IP network segment. The value range is 1 to 500 IP packets per second, 100 IP packets by default. Zero indicates this attack is not

		monitored.

Default The default value is 100.

Command mode Global configuration mode.

Usage guidelines In general, this quantity should be about the number of the active hosts divided by 20. However, when the isolated hosts reach or approach to the maximum number, you can increase the quantity of the monitored hosts to meet the requirement for better system guard. Note: If you reduce the quantity of the monitored hosts, it will clear the data of the currently monitored hosts.

Examples Set the maximum quantity of the attacked hosts as 200:

```
DES-7210(config)# system-guard detect-maxnum 200
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function.

50.1.6 system-guard exception-ip ip mask

Use this command to set the exceptional IP addresses free from monitoring. Use the **no** form of the command to restore it to the default value.

system-guard exception-ip *ip mask*

no system-guard exception-ip *ip mask* [**all-eip**]

Parameter description

Parameter	Description
ip	Dotted decimal IP address
mask	Dotted decimal mask
all-eip	Delete all exceptional IP addresses. This option is used for the **no** command only.

Default No exceptional IP address is defined.

Command mode	Global configuration mode.
Usage guidelines	This command is used to add an exceptional IP address for the anti-attack function to allow it to access the interface.
Examples	In the global configuration mode, set the exceptional IP address 192.168.5.145 255.255.255.0, which is not monitored. `DES-7210(config-if)# system-guard exception-ip 192.168.5.145/24`

Related commands

Command	Description
system-guard enable	Enable the anti-attack function.

50.1.7 clear system-guard [interface interface-id [ip-address]]

Use this command to clear the isolated IP address.

clear system-guard [**interface** *interface-id* [*ip-address*]]

Parameter description

Parameter	Description
interface *interface-id*	The interface.
ip-address	The IP address.

Default	N/A.
Command mode	Privileged EXEC mode.
Examples	Clear the isolated IP addresses of the port **fastethernet** 0/1: `DES-7210(config)# clear system-guard interface fastethernet 0/1`

Related commands

Command	Description
system-guard enable	Enable the anti-attack function.

50.2 Showing Related Command

Configuration commands for system attack protection include:

- **show system-guard [interface** *interface-id***]**
- **show system-guard isolate-ip [interface** *interface-id***]**
- **show system-guard detect-ip [interface** *interface-id***]**
- **show system-guard exception-ip**

50.2.1 show system-guard [interface *interface-id*]

Use this command to show the configuration of anti-attack.

show system-guard [**interface** *interface-id*]

Parameter description

Parameter	Description
interface *interface-id*	Show the anti-attack configuration on the interface.

Default N/A.

Command mode Privileged EXEC mode.

Examples

```
DES-7210# show system-guard
detect-maxnum number   : 100       //Maximum number of hosts
monitored by the device
isolated host number   : 11        //Number of hosts isolated by
the device
interface  state  isolate time  same-attack-pkts
scan-attack-pkts
---------------------- ---------------------------------
Fa 0/1    ENABLE    120            20                10
Fa 0/2    DISABLE   110            21                11
……
DES-7210# show system-guard interface Fa 0/1
detect-maxnum number   : 100       //Maximum number of hosts
monitored by the device
isolated host number   : 11        //Number of hosts isolated by
the device
inteface  state  isolate time  same-attack-pkts  scan-attack-pkts
----------------------- ----------------------------
Fa 0/1    ENABLE    120            20                10
```

Related commands	**Command**	**Description**
	system-guard enable	Enable the anti-attack function.

50.2.2 show system-guard isolate-ip [interface *interface-id*]

Use this command to show the anti-attack information of the isolated IP addresses.

show system-guard isolate-ip [**interface** *interface-id*]

Parameter description	**Parameter**	**Description**
	interface *interface-id*	Show the anti-attack information of the isolated IP addresses of the interface

Default N/A.

Command mode Privileged EXEC mode.

Examples

```
DES-7210# show system-guard isolated-ip
interface   ip-address    isolate reason   remain-time(second)
---------  -------------  ----------------------------
Fa 0/1    192.168.5.119   scan ip attack     110
Fa 0/1    192.168.5.109   same ip attack     61
```

Related commands	**Command**	**Description**
	system-guard enable	Enable the anti-attack function.

50.2.3 show system-guard detect-ip [interface *interface-id*]

Use this command to show the anti-attack information of the IP address being monitored.

show system-guard detect-ip [**interface** *interface-id*]

Parameter description	**Parameter**	**Description**
	interface *interface-id*	Show the anti-attack information of the IP addresses of the interface being monitored.

Default N/A.

Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show system-guard detect-ip
interface  ip-address  same ip attack packets  scan ip attack
packets
-----------------------------------------------------
Fa 0/1    192.168.5.118         0              8
Fa 0/1    192.168.5.108        12              2
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack functio.

50.2.4 show system-guard exception-ip [interface *interface-id*]

Use this command to show the anti-attack information of the exceptional IP addresses.

show system-guard exception-ip [**interface** *interface-id*]

Parameter description

Parameter	Description
interface *interface-id*	Show the anti-attack information of the exceptional IP addresses of the interface.

Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show system-guard exception-ip
Exception IP Address    Exception Mask
--------------------   ---------------
255.255.255.0
192.168.4.11           255.255.255.0
```

Related commands

Command	Description
system-guard enable	Enable the anti-attack function.

51 DAI Configuration Commands

51.1 Commands for Enabling and Disabling the DAI Inspection Function of the Specified VLAN

51.1.1 ip arp inspection vlan *vlan-id*

Use this command to enable the DAI inspection function of the specified VLAN. The **no** option of this command disables the function of the specified VLAN. If the parameter **vlan-id** is neglected, the DAI inspection function of all VLANs will be disabled.

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan [*vlan-id*]

Parameter description

Parameter	Description
vlan-id	VLAN ID

Default

The DAI inspection function of all VLANs is disabled.

Command mode

Global configuration mode.

Usage guidelines

To execute this command, enable the DAI function firstly.

Examples

The following configuration is to check the ARP message received from VLAN 1.

```
DES-7210(config)# ip arp inspection
DES-7210(config)# ip arp inspection vlan 1
```

Related

Command	Description

commands	**show ip arp inspection vlan**	Show the information of the DAI inspection function of the specified VLAN.

51.2 Commands for Configuring the L2 Port to a Trusted Port

51.2.1 ip arp inspection trust

Use this command to configure the L2 port to a trusted port.The **no** option of this command will restore the L2 port to a untrusted port.

ip arp inspection trust

no ip arp inspection trust

Default configuration	The L2 port is a untrusted port.
Command mode	Interface configuration mode.
Usage guidelines	If it is necessary to make the ARP message received by some interface pass the DAI inspection unconditionally, you can set the interface to a trusted port, indicating that you do not need to check whether the ARP message received by this interface is legal.

Examples	The configuration example below sets the gigabitEthernet 0/19 interface as the trusted port.
	`DES-7210(config)# interface gigabitEthernet 0/19`
	`DES-7210(config-if)# ip arp inspection trust`

Related commands

Command	Description
show ip arp inspection interface	Show related DAI information on the interface, including the trust state and rate limit of the interface.

Platform description	On the NFPP-supported switches, interface rate is limited by NFPP rather than DAI. Therefore, if you execute this command on NFPP-supported switches, only the interface trust state will be displayed.

51.3 DHCP Snooping Database Related Configuration

When the corresponding DAI funciton of the VLAN is enabled and the L2 port which receives the ARP message is configured to be a untrusted port, the validity of the ARP message is needed to check based on the DHCP Snooping database. If no configuration is carried out for the database, the ARP message passes the validity check. For the configuration on the DHCP Snooping, refer to the *DHCP Snooping Configuration*.

52 IP Source Guard Configuration Commands

52.1 IP Source Guard Global Command

In the global configuration mode, the command of IP Source Guard is:

- **ip source binding**

52.1.1 ip source binding

Use this command to add static user information to IP source address binding database. The **no** form of this command deletes the corresponding static user:

[**no**] **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

Parameter description	**Parameter**	**Description**
	mac-address	Add user MAC address statically.
	vlan-id	Add user vlan id statically.
	ip-address	Add user IP address statically.
	interface-id	Add user interface id statically.

Default configuration	No static binding user.
Command mode	Global configuration mode.

Examples

The following example shows how to configure a static user:

```
DES-7210# configure terminal
DES-7210(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface fastEthernet 0/1
DES-7210(config)# end
DES-7210# show ip source binding
MacAddress  IpAddress  Lease(sec) Type VLAN      Interface
------------------  ---------------  ------------  -------------
----- --------------------
00d0.f801.0101 192.168.4.243 infinite  static   1   FastEthernet
0/1  Total number of bindings: 1
```

Related commands

Command	Description
show ip source binding	View the binding information of IP source address and database.

52.2 IP Source Guard Command in the Interface Mode

In the interface configuration mode, the command of IP Source Guard is:

ip verify source

52.2.1 ip verify source

Use this command to enable IP Source Guard function on the interface, The **no** form of this command disable the function.

[**no**] **ip verify source** [**port-security**]

Parameter description

Parameter	Description
port-security	Configure IP Source Guard to do IP+MAC-based detection.

Default configuration

Disabled

Command mode

Interface configuration mode.

Usage guidelines	This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection. IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.

Examples

The following example configures IP Source Guard on fastEthernet 0/1:

```
DES-7210# configure terminal
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# ip verify source
DES-7210(config-if)# end
DES-7210# show ip verify source
Interface Filter-type Filter-mode  Ip-addressMac-address    VLAN
--------------------  -----------  -----------  ---------------
-------------- --------
FastEthernet           0/1  ip        active
192.168.4.243      00d0.f801.0101 1
```

Related commands

Command	Description
show ip verify source	View user filtering entry of IP Source Guard.

52.3 Other IP Source Guard Commands

Other IP Source Guard commands include:

- **show ip source binding**
- **show ip verify source**
- **debug ip source bind**

52.3.1 show ip source binding

Use this command to view the binding information of IP source address and database.

show ip binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter description

Parameter	Description
ip-address	Show user binding information of corresponding ip.
mac-address	Show user binding information of corresponding mac.
dhcp-snooping	Show binding information of dynamic user.
static	Show binding information of static user.
vlan-id	Show user binding information of corresponding vlan.
Interface-id	Show user binding information of corresponding interface.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
DES-7210#show ip source binding
MacAddress        IpAddress   Lease(sec)   Type  VLAN  Interface
------------------  ---------------  ------------  -------------
----- --------------------
00d0.f801.0101   192.168.4.243   infinite    static
1    FastEthernet  0/1   Total number of bindings: 1
```

Related commands

Command	Description
ip source binding	Set the binding static user.

52.3.2 show ip verify source

Use this command to view user filtering entry of IP Source Guard.

show ip verify source [**interface** *interface-id*]

Parameter description

Parameter	Description
Interface-id	Show user filtering entry of corresponding interface.

Command mode

Privileged EXEC mode.

Usage guidelines

If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: “IP source guard is not configured on the interface FastEthernet 0/10”

Now, IP Source Guard supports the following filtering modes:

inactive-no-snooping-vlan：the interface isn’t within the range of DHCP Snooping VLAN and IP Source Guard is inactive.

inactive-trust-port ：the interface is the trusted port controlled by DHCP Snooping and IP Source Guard is inactive.

active：the interface is the untrusted port ontrolled by DHCP Snooping and IP Source Guard is active.

Examples

```
DES-7210 # show ip verify source
Interface Filter-type Filter-mode Ip-address Mac-address    VLAN
--------------------  -----------  -----------  ---------------
-------------- --------
FastEthernet 0/1   ip  active  192.168.4.243   00d0.f801.0101 1
```

Related commands

Command	Description
ip verify source	Set IP Source Guard on the interface.

52.3.3 debug ip source bind

Use this command to turn on the debugging switch of IP Source Guard.

debug ip source bind

Default configuration

The debugging switch is turned off.

Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to view the debug information of IP Source Guard.
Examples	`DES-7210# debug ip source bind`

53 NFPP Configuration Commands

53.1 Related Configuration Commands

The NFPP configuration commands include:

- **cpu-protect sub-interface** {**manage|protocol|route**} **pps**
- **cpu-protect sub-interface** {**manage|protocol|route**} **percent**

The anti-arp configuration commands include:

- **arp-guard isolate timeout**
- **arp-guard rate-limit**
- **arp-guard attack-threshold**
- **arp-guard scan-threshold**
- **clear arp-guard users**
- **clear arp-guard scan**

53.1.1 cpu-protect sub-interface {manage | protocol | route} pps

Use this command to configure the traffic bandwidth of each type of packets.

cpu-protect sub-interface {**manage** | **protocol** | **route**} **pps** *pps_vaule*

Parameter description

Parameter	Description
pps_value	The rate limit threshold, ranging from 1 to 8192

Default

The default traffic bandwidths of each type of packets are:
Manage packets: 3000pps;
Route packets: 3000pps;
Protocol packets: 3000pps.

Command mode	Global configuration mode.

Examples

```
DES-7210(config)# cpu-protect sub-interface manage pps 200
```

Related commands

Command	Description
cpu-protect sub-interface {**manage** | **protocol** | **route**} **percent**	Configure the percent value of each type of packets occupied in the buffer area.

53.1.2 cpu-protect sub-interface {manage | protocol | route} percent

Use this command to configure the percent value of each type of packets occupied in the buffer area.

cpu-protect sub-interface {**manage** | **protocol** | **route**} **percent** *percent_vaule*

Parameter description

Parameter	Description
percent_value	The percent value, ranging from 1 to 100.

Default

The default percent values of each type of packets occupied in the buffer area are:

Manage packets: 30;

Route packets: 20;

Protocol packets: 45.

Command mode	Global configuration mode.

Examples

```
DES-7210(config)# cpu-protect sub-interface manage
percent 60
```

Related

Command	Description

commands	**cpu-protect sub-interface** {**manage** | **protocol** | **route**} **pps**	Configure the traffic bandwidth of each type of packets.

53.1.3 arp-guard isolate timeout

Use this command to configure the isolate time.

arp-guard isolate timeout [*seconds* | **permanent**]

Parameter description

Parameter	Description
seconds	Isolate time, in second. Range in 0 or [180, 86400], 0 indicates no isolation.
permanent	Permanent isolation.

Default

The default isolate time in the global configuration mode is 0, indicating no isolation.

No default isolate time in the interface configuration mode.

Command mode

Global or interface configuration mode.

Usage guidelines

The attack isolate time can be configured in the global or interface configuration mode. For a port, if the port-based isolate time is not configured, the isolate time is configured in the global configuration mode; and vice versa.

Examples

```
DES-7210(config)# arp-guard isolate timeout 180

DES-7210(config)# interface g 0/1

DES-7210(config-if)# arp-guard isolate timeout permanent
```

Related commands

Command	Description
show arp-guard configuration	View the arp-guard configuration.

53.1.4 arp-guard rate-limit

Use this command to set the arp-guard rate limit.

arp-guard rate-limit *pps* {**per-src-ip** | **per-src-mac** | **per-port**}

Parameter description

Parameter	Description
pps	Configure the rate limit value.
per-src-ip	Limit the rate of each source IP address.
per-src-mac	Limit the rate of each source MAC address.
per-port	Limit the rate of each port.

Default

The default rate limit of each IP address and MAC address is 4pps ; the default rate limit of each port is 100pps.

Command mode

Global configuration mode.

Examples

```
DES-7210(config)# arp-guard rate-limit 2 per-src-ip
DES-7210(config)# arp-guard rate-limit 3 per-src-mac
DES-7210(config)# arp-guard rate-limit 50 per-port
```

Related commands

Command	Description
show arp-guard configuration	View the arp-guard configuration.

53.1.5 arp-guard attack-threshold

Use this command to configure the attack threshold. The attack occurrs if the packet rate exceeds the attack-threshold.

arp-guard attack-threshold *pps* {**per-src-ip** | **per-src-mac** | **per-port**}

Default

The default attack threshold of each source IP address and source MAC address is 8pps; the default attack threshold of each port is 200pps.

Command mode	Global configuration mode.

Usage guidelines	When the packet transmission rate exceeds the value, the attack action is detected and it prompts the warning message and the TRAP packets are sent.
	The warning message will be prompted like :
	`*Dec 27 15:34:16: %ARPGUARD-4-DOS_DETECTED: ARP DoS attack was detected.`
	This message informs the administrator of detecting the ARP attack only, without the user attribute information. The administrator shall execute the **show arp-guard users** command to view the detailed informtion about the attackers. **Note that** it is not recommended for the administrator to set the isolated time to 0, because the attack attributes willnot be saved in the isolated user table if the isolated time is 0.
	If the administrator sets the isolated time to 0, the TRAP message sent when the attack action was detected contains the following information(if vlan=0, it is a route port.):
	`ARP DoS attack from user<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> detected.`
	If the administrator sets the isolated time to any value except for 0, it prompts the additional information of the sent TRAP message sent as follows when the hardware has been isolated successfully:
	`User<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> is isolated.`
	When it fails to isolate the hardware due to insufficient memory and hardware resources, it will prompt the additional information of the sent TRAP messages:
	`Failed to isolate user<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>.`
	You shall pay attention to:
	1. It is possible that the legal ARP packets are learnt

slowly on condition that a large number of attack packets exist when the number of hardware isolated users exceeds 127.

2. The upper limit of the table memory occupied is 1MB. It will prompt "%ARPGUARD-4-MEM_LIMIT:user table's size reached limit 1MB." to remind the administrator of this event.

3. A policy will be set to the hardware when isolating the attackers. It prompts "%ARPGUARD-4-ISOLATE_FAILED: failed to isolate ARP DoS attacker." to inform the administrator of insufficient hardware resources.

4. It prompts "%ARPGUARD-4-NO_MEMORY: failed to alloc memory" to inform the administrator of this event.

5. It is worth mentioning that in order to prevent the frequent printing from exhausting the CPU memory, you shall limit the message rate by printing the messages at 30s interval.

Examples

```
DES-7210(config)# arp-guard attack-threshold 2 per-src-ip
DES-7210(config)# arp-guard attack-threshold 3 per-src-mac
DES-7210(config)# arp-guard attack-threshold 50 per-port
```

Related commands

Command	Description
show arp-guard configuration	View the arp-guard configuration.
clear arp-guard users	Clear the arp-guard users.
show arp-guard users	Show the arp-guard users.

53.1.6 arp-guard scan-threshold

Use this command to scan the arp-guard threshold.

arp-guard scan-threshold pkt-cnt

Parameter description

Parameter	Description
pkt-cnt	The scan threshold value.

Default

15.

Command mode

Global configuration mode.

Usage guidelines

The attribute of the ARP scan is that the source MAC address of the link layer is constant while the source IP address is changing, or the source MAC address and IP address are constant while the destination IP address is changing. Now DES-7210 products only support the former ARP scan. If the ARP packets received within 10s are in accordance with the ARP scan attribute and the packet amount exceeds the scan-threshold, user with this MAC address is scanning the ARP packets.

When the ARP scan is detected, it will prompt:

```
*Dec 27 15:34:16: %ARPGUARD-4-SCAN: ARP scan was detected.
```

If the administrator wants to view the detailed information, please execute the **show arp-guard scan** command. The ARP scan table only save the latest 256 pieces of records. When the ARP scan table is full, it will prompt:

```
*Dec 27 15:34:16: %ARPGUARD-4-SCAN_TABLE_FULL: ARP scan table is full.
```

And it prompts the additional TRAP information:

```
ARP scan from user< MAC=0000.0000.0004,port=Gi4/1,VLAN=1> detected.
```

Note that the ARP scan table only save the latest 256 pieces of records. When the ARP scan table is full, the newest record will overwrite the oldest one.

Examples

```
DES-7210(config)# arp-guard scan-threshold 20
```

Related commands	**Command**	**Description**
	show arp-guard configuration	View the arp-guard configuration.
	clear arp-guard scan	Clear the arp-guard scan table.
	show arp-guard scan	Show the arp-guard scan table.

53.1.7 clear arp-guard users

Use this command to clear the arp-guard users.

clear arp-guard users [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]

Parameter description	**Parameter**	**Description**
	vid	VLAN ID.
	interface-id	Interface name and interface id.
	ip-address	The IP address.
	mac-address	The MAC address.

Command mode	Privileged EXEC mode.

Usage guidelines	Use the command without any parameters to clear all isolated users.

Examples	The example below shows how to clear the isolated users on interface gigabitEthernet 0/1 in VLAN 1: `DES-7210(config)# clear arp-guard users vlan 1 interface gigabitEthernet 0/1`

Related commands	**Command**	**Description**
	arp-guard attack-threshold	Configure the arp-guard attack-threshold.
	show arp-guard users	Show the isolated users.

53.1.8 clear arp-guard scan

Use this command to clear the arp-guard scan table.

clear arp-guard scan

Command mode	Privileged EXEC mode.

Examples

```
DES-7210(config)# clear arp-guard scan
```

Related commands

Command	Description
arp-guard scan-threshold	Configure the arp-guard scan-threshold.
show arp-guard scan	Show the arp-guard scan table.

53.2 Showing and Monitoring Commands

53.2.1 show arp-guard configuration

Use this command to show the arp-guard configuration.

show arp-guard configuration

Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show arp-guard configuration
Rate limit: 10000 pps per-src-ip, 1 pps per-src-mac, 100 pps per-port
Attack threshold:10000 pps per-src-ip, 1 pps per-src-mac, 200 pps
per-port
Scan threshold:15 packets per 10 seconds
Global isolate timeout:10800 seconds
Local isolate timeout(second):Gi4/1    permanent
```

Related

Command	Description

commands	**arp-guard isolate timeout**	Configure the arp-guard isolate time.
	arp-guard rate-limit	Configure the arp-guard rate limit.
	arp-guard attack-threshold	Configure the arp-guard attack threshold.
	arp-guard scan-threshold	Configure the arp-guard scan threshold.

53.2.2 show arp-guard users

Use this command to show the isolated usres.

show arp-guard users [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistics of the isolated users.
vid	VLAN ID.
interface-id	Interface name and interface id.
ip-address	The IP address.
mac-address	The MAC address.

Command mode

Privileged EXEC mode.

Examples

The following example shows the statistics of the isolated users:

```
DES-7210# show arp-guard users statistics

Success:  100

Fail:     1

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

Total:    101
```

101 users are isolated, and 100 users have been isolated by the hardware successfully. That is to say, only one user failed due to insufficient memory or the hardware resources.

The following example shows how to show the isolated users. The

"**remian-time(seconds)**" refers to the isolated time remained

```
DES-7210# show arp-guard users

If column 1 shows '*', it means "hardware failed to isolate user".

VLAN     interface     Ip address     MAC address

 remain-time(seconds)

1       Gi0/1        1.1.1.1         -       110

2       Gi0/1        1.1.2.1         -        61

*3      Gi0/1          -      0000.0000.1111    110

4       Gi0/1          -      0000.0000.2222    61

Total: 4 users
```

Related commands

Command	Description
arp-guard attack-threshold	Configure the arp-guard attack threshold.
clear arp-guard users	Clear the isolated users.

53.2.3 show arp-guard scan

Use this command to show the arp-guard scan table.

show arp-guard scan [**statistics** | [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the record statistics in the arp-guard scan table.
vid	VLAN ID.
interface-id	Interface name and interface id.
mac-address	The MAC address.

Command mode

Privileged EXEC mode.

Examples

The following command shows the record number in the ARP scan

table.

```
DES-7210# show arp-guard scan statistics

ARP scan table has 4 record(s).


DES-7210# show arp-guard scan

VLAN    interface      MAC address    timestamp

1    Gi0/1      0000.0000.0001  2008-01-23 16:23:10

2    Gi0/2      0000.0000.0002  2008-01-23 16:24:10

3    Gi0/3      0000.0000.0003  2008-01-23 16:25:10

4    Gi0/4      0000.0000.0004  2008-01-23 16:26:10

Total: 4 record(s)
```

"timestamp" records the timestamp of the detected ARP scan. For example, "2008-01-23 16:23:10" indicates that the ARP scan was detected at 16:23:10, Jan 23rd, 2008.

```
DES-7210# show arp-guard scan vlan 1 interface g 0/1 0000.0000.0001

VLAN    interface      MAC address    timestamp

1     Gi0/1      0000.0000.0001  2008-01-23 16:23:10

Total: 1 record(s)
```

Related commands

Command	Description
arp-guard scan-threshold	Configure the arp-guard scan threshold.
clear arp-guard scan	Clear the arp-guard scan table.

54 ACL Configuration Commands

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

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

ID	Meaning
	63
flow-label 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 *precedence*	Packet precedence value (0 to 7)
time-range *tm-rng-name*	Time range of packet filtering, named *tm-rng-name*
tos *tos*	Type of service (0 to 15)
cos *cos*	Class of service (0-7)
cos inner *cos*	COS of the packet tag
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name (0 to 255)
operator port[*port*]	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range) *port* indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number
src-mac-addr	Physical address of the source host
dst-mac-addr	Physical address of the destination host
VID vid	VLAN ID
VID inner vid	VID of the tag
ethernet-type	Ethernet protocol type. 0x value can be entered.
match-all *tcpf*	Match all bits of the TCP flag.
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface
{*rule mask offset*}$^{+}$	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table "+" sign indicates at least one group

The fields in the packet are as follows:

```
AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD
```

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

The corresponding offset table is as follows:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol number	35
C	Data frame length field	12	Q	IP check sum	36
D	VLAN tag field	14	R	Source IP address	38
E	DSAP (Destination Service Access Point) field	18	S	Destination IP address	42
F	SSAP (Source Service Access Point) field	19	T	TCP soure port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version number	26	XY	IP header length and reserved bits	58
K	TOS field	27	Z	Resrved bits and flags bit	59
L	Length of IP packet	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

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

54.1 Configuration Related Commands

The Global configuration mode commands include :

- **access-list**
- **ip access-list**
- **mac access-list**
- **expert access-list**
- **ipv6 access-list**
- **ip access-list resequence**

The ACL configuration mode commands include:

- **deny**
- **permit**
- **list-remark text**
- **no sn**

The interface mode configuration commands include:

- **ip access-group**
- **mac access-group**
- **expert access-group**
- **ipv6 traffic-filter**

54.1.1 access-list

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

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

   access-list *id* {**deny** | **permit**} {**source** *source-wildcard* | **host** *source* | **any**}

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

   access-list *id* {**deny** | **permit**} **protocol** {**source** *source-wildcard* | **host** *source* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*]

3. Extended MAC access list (700 to 799)

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

4. Extended expert access list (2700 to 2899)

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

[fragments] [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*] [**fragments**]

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

Transmission Control Protocol (TCP)

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

User Datagram Protocol (UDP)

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

5. List remark

access-list *list-remark text*

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

Parameter description

Parameter	Description
id	Access list ID. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.

deny	If not matched, access is denied.
Permit	If matched, access is permitted.
Source	Specify the source IP address (host address or network address).
source-wildcard	It can be discontinuous, for example, 0.255.0.32.
protocol	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
destination	Specify the destination IP address (host address or network address).
destination-wildcard	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
fragments	Packet fragment filtering
precedence	Specify the packet priority .
precedence	Packet precedence value (0 to 7)
time-range	Time range of packet filtering
time-range-name	Time range name of packet filtering
tos	Specify type of service.
tos	ToS value (0 to 15)
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name
operator	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)
port [*port*]	Port number; *range* needs two port numbers, while other operators only need one port number.

host *source-mac-address*	Source physical address
host *destination-mac-address*	Destination physical address
VID *vid*	Match the specified VID.
ethernet-type	Ethernet type
match-all	Match all the bits of the TCP flag.
tcp-flag	Match the TCP flag.

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

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

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

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

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

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

The TCP Flag includes part or all of the following:

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

The packet precedence is as below:

- **critical**
- **flash**

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

The service types are as below:

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

The ICMP message types are as below:

- **administratively-prohibited**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **fragment-time-exceeded**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**

- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **redirect**
- **device-advertisement**
- **device-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **ttl-exceeded**
- **unreachable**

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

- **bgp**
- **chargen**
- **cmd**
- **daytime**
- **discard**
- **domain**
- **echo**
- **exec**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **ident**
- **irc**
- **klogin**
- **kshell**
- **ldp**
- **login**
- **nntp**
- **pim-auto-rp**

- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

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

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

- **xdmcp**

The Ethernet types are as below:

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

Examples

1. Example of the standard IP ACL

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

```
DES-7210 (config)#access-list 1 permit 192.168.1.64 0.0.0.63
```

2. Example of the extended IP ACL

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

```
DES-7210(config)#access-list 102 permit tcp any any eq domain
DES-7210(config)#access-list 102 permit udp any any eq domain
DES-7210(config)#access-list 102 permit icmp any any echo
DES-7210(config)#access-list 102 permit icmp any any echo-reply
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 0/1. The configuration procedure is as below:

```
DES-7210(config)#access-list 702 deny host 00d0f8000c0c any aarp
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the

source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
DES-7210(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
DES-7210(config)# access-list 2702 permit any any any any
DES-7210(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

The software version must be R10.0 and higher.

54.1.2 ip access-list

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

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

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

Parameter description

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

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

There are differences between a standard ACL and an extended ACL. The extended ACL is more precise. Refer to **deny** or **permit** in

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

Examples

Create a standard ACL:

```
DES-7210(config)# ip access-list extended 123
DES-7210(config-ext-nacl)# show access-lists
ip access-list extended 123
DES-7210(config-ext-nacl)#
```

Create an extended ACL:

```
DES-7210(config)# ip access-list standard std-acl
DES-7210(config-std-nacl)# show access-lists
ip access-list standard std-acl
DES-7210config-std-nacl)#
```

Related commands

Command	Description
show access-lists	Show the ACLs.

Platform description

The software version must be R10.0 and higher.

54.1.3 mac access-list

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

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

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

Parameter description

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

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

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

Examples

Create an extended MAC ACL**:**

```
DES-7210(config)# mac access-list extended mac-acl
DES-7210(config-mac-nacl)# show access-lists mac access-list extended mac-acl
DES-7210(config-mac-nacl)#
```

Create an extended ACL:

```
DES-7210(config)# mac access-list extended 704
DES-7210(config-mac-nacl)# show access-lists mac access-list extended 704
DES-7210(config-mac-nacl)#
Red-Giant(config-mac-nacl)#
```

Related commands

Command	Description
show access-lists	Show the extended MAC ACLs

Platform description

The software version must be R10.0 and higher.

54.1.4 expert access-list

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

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

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

Parameter description

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

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines

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

Examples

Create an extended expert ACL:

```
DES-7210(config)# expert access-list extended exp-acl
DES-7210(config-exp-nacl)# show access-lists expert access-list extended exp-acl
DES-7210(config-exp-nacl)#
```

Create an extended expert ACL:

```
DES-7210(config)# expert access-list extended 2704
DES-7210(config-exp-nacl)# show access-lists expert access-list extended 2704
DES-7210(config-exp-nacl)#
```

Related commands

Command	Description
show access-lists	Show the extended expert ACLs

Platform description

The software version must be R10.0 and higher.

54.1.5 ipv6 access-list

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

ipv6 access-list *name*

no mac access-list *name*

Parameter description

Parameter	Description
name	ACL name

Command mode

Global configuration mode.

Usage guidelines

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

Examples

Create an extended ipv6 ACL**:**

```
DES-7210(config)# ipv6 access-list extended v6-acl
DES-7210(config-ipv6-nacl)# show access-lists
ipv6 access-list v6-acl
DES-7210(config-ipv6-nacl)#
```

Related commands

Command	Description
show access-lists	Show the extended ipv6 ACLs

Platform description

The software version must be R10.0 and higher.

54.1.6 ip access-list resequence

Use this command to reassign the sequence of the IP ACL entries and create an extended IPv6 ACL. Use the **no** form of this command to restore it to the default configuration.

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

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

Parameter description

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

Default configuration

The start sequence is 10 and the sequence increment is 10.

Command mode

Global configuration mode

Usage guidelines

N/A.

Examples

Resequence the entries of the ACL:

```
DES-7210# show access-lists
ip access-list standard 1
```

```
10 permit host 192.168.4.12
20 deny any any
DES-7210# config
DES-7210# (config)#ip access-list resequence 1 21 43
DES-7210# (config)# exit
DES-7210# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
DES-7210#
```

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

Platform description	The software version must be R10.0 and higher.

54.1.7 deny

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

Use this command to set deny rules

1. Standard IP ACL

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

2. Extended IP ACL

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

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

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

Extended IP ACLs of some important protocols:

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

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

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

- **Transmission Control Prot** (TCP)

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

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

- **User Datagram Prot** (UDP)

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

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

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

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

- When you select the protocol field:

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

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

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

- **Transmission Control Protocol** (TCP)

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

  destination-mac-address | **any**} [*operator* **port** [*port*]] [**precedence**

  precedence] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*]

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

- **User Datagram Protocol** (UDP)

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

  destination-mac-address | **any**} [*operator* **port** [*port*]] [**precedence**

  precedence] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*]

5. Extended IPv6 ACL

  [*sn*] **deny protocol**{*source-ipv6-prefix*/*prefix-length* | **any** | **host**

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

  | *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label**

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

- **Transmission Control Protocol** (TCP)

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

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

- **User Datagram Protocol** (UDP)

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

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

Parameter description

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

Default configuration N/A.

Command mode ACL configuration mode.

Usage guidelines

N/A.

Examples

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

```
DES-7210(config)#expert access-list extended 2702
DES-7210(config-exp-nacl)#deny tcp  host  192.168.4.12 host
0013.0049.8272 any any
DES-7210(config-exp-nacl)#permit any any any any
DES-7210(config-exp-nacl)#show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
DES-7210(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 1. The configuration procedure is as below:

```
DES-7210(config)# ip access-list extended ip-ext-acl
DES-7210(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
DES-7210(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
DES-7210(config-ext-nacl)#exit
DES-7210(config)#interface gigabitethernet 1/1
DES-7210(config-if)#ip access-group ip-ext-acl in
DES-7210(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 1. The configuration procedure is as below:

```
DES-7210(config)#mac access-list extended mac1
DES-7210(config-mac-nacl)#deny host 0013.0049.8272 any aarp
DES-7210(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
DES-7210(config-mac-nacl)#exit
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(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 192.1.1.1 and apply the rule to Interface 1. The configuration procedure is as below:

```
DES-7210(config)#ip access-list standard 34
DES-7210(config-ext-nacl)# deny host 192.168.4.12
DES-7210(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
DES-7210(config-ext-nacl)#exit
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(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 192.1.1.1 and apply the rule to Interface 1. The configuration procedure is as below:

```
DES-7210(config)#ipv6 access-list extended v6-acl
DES-7210(config-ipv6-nacl)#11 deny ipv6 host 192.168.4.12 any
DES-7210(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
DES-7210(config-ipv6-nacl)# exit
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# ipv6 traffic-filter v6-acl in
```

Related commands

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

Platform description

The software version must be R10.0 and higher.

54.1.8 permit

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

Use this command to set the permit rules.

1. Standard IP ACL

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

2. Extended IP ACL

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

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

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

Extended IP ACLs of some important protocols:

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

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

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

  [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence**

  precedence] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*]

- **Transmission Control Protocol** (TCP)

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

- **User Datagram Protocol** (UDP)

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

3. Extended MAC ACL

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

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

4. Extended expert ACL

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

- **Transmission Control Protocol** (TCP)

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

- **User Datagram Protocol** (UDP)

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

5. Extended IPv6 ACL

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

- **Transmission Control Protocol** (TCP)

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

- **User Datagram Protocol** (UDP)

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

Parameter description	For those not listed below, see **deny**.

Default configuration	N/A.

Command mode	ACL configuration mode.
Usage guidelines	N/A.
Examples	The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
DES-7210(config)#expert access-list extended exp-acl
DES-7210(config-exp-nacl)#permit tcp  host  192.168.4.12 host
0013.0049.8272 any any
DES-7210(config-exp-nacl)#deny any any any any
DES-7210(config-exp-nacl)#show access-lists
expert access-list extended exp-acl
10 permit tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
DES-7210(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 1. The configuration procedure is as below:

```
DES-7210(config)# ip access-list extended 102
DES-7210(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
DES-7210(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
DES-7210(config-ext-nacl)#exit
DES-7210(config)#interface gigabitethernet 1/1
DES-7210(config-if)#ip access-group 102 in
DES-7210(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 1. The configuration procedure is as below:

```
DES-7210(config)#mac access-list extended 702
DES-7210(config-mac-nacl)#permit host 0013.0049.8272 any aarp
DES-7210(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
DES-7210(config-mac-nacl)#exit
```

```
DES-7210(config)#interface gigabitethernet 1/1
DES-7210(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 192.1.1.1 and apply the ACL to Interface 1. The configuration procedure is as below:

```
DES-7210(config)#ip access-list standard std-acl
DES-7210(config-std-nacl)#permit host 192.168.4.12
DES-7210(config-std-nacl)#show access-lists
ip access-list standard std-acl
  10 permit host 192.168.4.12
DES-7210(config-std-nacl)#exit
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(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 192.1.1.1 and apply the ACL to Interface 1. The configuration procedure is as below:

```
DES-7210(config)#ipv6 access-list extended v6-acl
DES-7210(config-ipv6-nacl)#11 permit ipv6 host ::192.168.4.12 any
DES-7210(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
DES-7210(config-ipv6-nacl)# exit
DES-7210(config)#interface gigabitethernet 1/1
DES-7210(config-if)#ipv6 traffic-filter v6-acl in
```

Related commands

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

Platform description	The software version must be R10.0 and higher.

54.1.9 list-remark text

Use this command to add remarks for the specified ACL. The **no** form deletes the remarks.

list-remark *text*

Parameter description

Parameter	Description
Text	Remark information

Command mode	ACL configuration mode.
Usage guidelines	N/A.

Examples

```
DES-7210# ip access-list extended 102
DES-7210(config-ext-nacl)# list-remark this acl is to filter the
host 192.168.4.12
DES-7210(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
DES-7210(config-ext-nacl)#
```

Related commands

Command	Description
show access-list	Show the ACLs.
ip access-list	Define the IP ACL.

Platform description	The software version must be R10.0 and higher.

54.1.10 no sn

Use this command to delete an entry of the ACL.

no *<sn>*

Parameter description

Parameter	Description
sn	Sequence number of the ACL entry

Command mode

ACL configuration mode.

Usage guidelines

N/A.

Examples

```
DES-7210(config)# ipv6 access-list extended v6-acl
DES-7210(config-ipv6-nacl)# permit ipv6 host ::192.168.4.12 any
DES-7210(config-ipv6-nacl)#12 deny ipv6 host any any
DES-7210(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
12 deny ipv6 any any
DES-7210(config-ipv6-nacl)# no 12
DES-7210(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
DES-7210(config-ipv6-nacl)#
```

Related commands

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

Platform description

The software version must be R10.0 and higher.

54.1.11 ip access-group

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

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

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

Parameter description

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

Default configuration

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage guidelines

N/A.

Examples

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

```
DES-7210(config)# interface fastEthernet 0/0
DES-7210(config-if)# ip access-group 120 in
```

Related commands

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

Platform description

The software version must be R10.0 and higher.

54.1.12 mac access-group

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

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

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

Parameter description

Parameter	Description
id	ID of the MAC ACL (700 to 799)
name	Name of the MAC ACL
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface

Default configuration

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage guidelines

N/A.

Examples

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

```
DES-7210(config)#interface GigaEthernet 1/1
DES-7210(config-if)#mac access-group
accept__00d0f8xxxxxx_only in
```

Related commands

Command	Description
show access-group	Show the ACL configuration.

Platform description

The software version must be R10.0 and higher.

54.1.13 expert access-group

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

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

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

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

Default configuration

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage guidelines

N/A.

Examples

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

```
DES-7210(config)# interface GigaEthernet 0/1
DES-7210(config-if)# expert access-group
accept_00d0f8xxxxxx_only in
```

Related commands

Command	Description
show access-group	Show the ACL configuration.

Platform description

The software version must be R10.0 and higher.

54.1.14 ipv6 traffic-filter

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

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

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

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

Default configuration

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage guidelines

Apply the specified IPV6 ACL on the specified interface to control the interface traffic. You can view the configuration by command **show ipv6 traffic-filter.**

Examples

The following example shows how to apply the **access-list v6-acl** to Gigabit interface 1:

```
DES-7210(config)# interface GigaEthernet 0/1
DES-7210(config-if)# ipv6 traffic-filter v6-acl in
```

Related commands

Command	Description
show access-group	Show the ACL configurations.

Platform description

The software version must be R10.0 and higher.

54.2 Showing Related Commands

The showing and monioring commands include:

- **show access-lists**
- **show ip access-group**
- **show expert access-group**

- **show mac access-group**
- **show ipv6 access-group**
- **show access-group**

54.2.1 show access-lists

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

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

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

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

Examples

```
DES-7210# show access-lists n_acl
ip access-list standard n_acl
DES-7210# show access-lists 102
ip access-list extended 102
DES-7210# show access-lists
ip access-list standard n_acl
ip access-list extended 101
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
```

Related commands

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

Platform description	The software version must be R10.0 and higher.

54.2.2 show ip access-group

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

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

Parameter description

Parameter	Description
<*interface*>	Interface ID

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

Examples

```
DES-7210# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

Related commands

Command	Description
ip access-list	Define the IP ACL.

Platform description	The software version must be R10.0 and higher.

54.2.3 show expert access-group

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

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

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode.
Usage guidelines	Show the expert ACL configured on the interface. If no interface is specified, the associated expert ACLs of all the interfaces will be shown.
Examples	DES-7210# **show expert access-group interface gigabitethernet** *0/2* expert access-group ee in Applied On interface GigabitEthernet 0/2.

Related commands

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

Platform description	The software version must be R10.0 and higher.

54.2.4 show mac access-group

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

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

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode.
Usage guidelines	Show the MAC ACL associated with the interface. If no interface is specified, the associated MAC ACLs of all associated interfaces will be shown.
Examples	DES-7210# **show mac access-group interface gigabitethernet** *0/3* mac access-group *mm* in Applied On interface GigabitEthernet 0/3.

Related

Command	Description

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

Platform description The software version must be R10.0 and higher.

54.2.5 show ipv6 traffic-filter

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

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

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode Privileged mode.

Usage guidelines Show the IPv6 ACL associated with the interface. If no interface is specified, the associated IPv6 ACLs of all the interfaces will be shown.

Examples

```
DES-7210# show ipv6 traffic-filter interface gigabitethernet 0/4
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/4.
```

Related commands

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

Platform description The software version must be R10.0 and higher.

54.2.6 show access-group

Use this command to show the ACL configuration of the interface.

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

Parameter description

Parameter	Description
<*interface*>	Interface ID

Command mode	Privileged mode.
Usage guidelines	Show the ACL applied to the interface. If no interface is specified, the ACLs applied to all the interfaces will be shown.
Examples	DES-7210# **show access-group** ip access-list standard ipstd3 Applied On interface GigabitEthernet 0/1. ip access-list standard ipstd4 Applied On interface GigabitEthernet 0/2. ip access-list extended 101 Applied On interface GigabitEthernet 0/3. ip access-list extended 102 Applied On interface GigabitEthernet 0/8.

Related commands

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

Platform description	The software version must be R10.0 and higher.

54.3 Security Channel

Note The security channel is not supported on the router platform.

The commands in the global configuration mode:

- **security global access-group**

The commands in the interface configuration mode:

- **security access-group**
- **security uplink enable**

54.3.1 security global access-group

Use this command to configure the global security channel.

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

no security global access-group

Parameter description

Parameter	Description
id	ACL ID
name	ACL name

Command mode Global configuration mode

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

Examples

```
DES-7210# security global access-group 1
```

Platform description The software version must be R10.2 and higher.

54.3.2 security access-group

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

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

no security access-group

Parameter description

Parameter	Description
id	ACL ID
name	ACL name

Command mode Interface configuration mode.

Usage guidelines	Use this command to configure the security channel on the interface.
Examples	`DES-7210# security access-group 1`
Platform description	The software version must be R10.2 and higher.

54.3.3 security uplink enable

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

security uplink enable

no security uplink enable

Command mode	Interface configuration mode.
Usage guidelines	Use this command to configure the uplink port of the security channel on the interface.
Examples	`DES-7210# security uplink enable`
Platform description	The software version must be R10.2 and higher.

55 VACL Configuration Commands

55.1 Configuring Related Commands

Vlan access map has 2 keywords. *map_name* is the major keyword and indispensable, while *map_sn* is the minor one which can be omitted. We define the collection of one or multiple submap(s) with the same name as hostmap.

- In fact, creating **vlan access map** is creating a submap. When *map_sn* is not specified, it will add 10 before the submap and on the basis of *map_sn* of the submap which belongs to the same hostmap.
- When *map_sn* is not specified, deleting **vlan access map,** all *Map_nam*e with the same *map_name* will be deleted, that is to say, the hostmap is deleted.
- When *map_sn* is not specified, deleting **vlan access map** will delete the specified submap. When the hostmap to which the specified submap belongs does not includes submaps, then the hostmap will be deleted automatically; and vice versa.
- One hostmap can include 6553 submaps at most.

55.1.1 vlan access-map

Use this command to create a submap in the global configuration mode. The **no** form of this command deletes the submap.

vlan access-map *map_name* [*map_sn*]

no vlan access-map *map_name* [*map_sn*]

Parameter description

Parameter	Description
map_name	Major keyword of submap which is indispensable and no more than 100 bytes.
map_sn	Minor keyword of submap which is optional in the range 0 to 65535.

Command mode	Global configuration mode.

Examples

The following example shows how to create **vlan access map**：

```
DES-7210(config)# vlan access-map ddd 20
DES-7210(config-access-map)#
```

55.1.2 match ip/mac address

Use this command to associate *ip acl* or *mac acl* with the specified sub**vlan access map.** The **no** form of this command removes the configuration.

match ip address { *acl_name* | *acl_id* }+
no match ip address { *acl_name* | *acl_id* }+
match mac address { *acl_name* | *acl_id* }+
no match mac address { *acl_name* | *acl_id* }+

Caution

+_indicates associating at least one acl. It can associate 8 acls at most.

Parameter description

Parameter	Description
acl_name	Name acl.
acl_id	Numbered acl

Command mode	Config-access-map mode, that is vacl mode.

Note

1..One submap can only be associated with ip acl or map acl. You can not associate a submap with both ip acl and map acl.

2..One submap can only be associated with at most 8 acls.

3. One submap can not be associated with an inexistent acl.

4. One submap can not be associated with acl without ace, which is null acl.

5. When a submap has been associated with ip acl (mac acl), you need to configure to associate ip acl (mac acl) again. And ip acl (mac acl) later configured is after the one first configured.

	6. When a submap has been associated with ip acl (mac acl), you need to configure to associate mac acl (ip acl) again and delete the configured ip acl (mac acl) automatically first and then configure mac acl (ip acl).

Examples

The following example shows how to set match content of submap:

```
DES-7210(config)# vlan access-map dd
DES-7210(config-access-map)# match ip address 10 20 sp1 30 sp2
DES-7210(config-access-map)# exit
DES-7210(config)# vlan access-map dd 20
DES-7210(config-access-map)# match mac address 710 720 m1 760
DES-7210(config-access-map)# exit
DES-7210(config)#
```

55.1.3 action forward/drop/redirect

Use this command to set forward action of submap in vacl mode. The **no** form of this command removes the configuration. By default, the action is forward.

action forward
no action forward

Use this command to set drop action of submap in vacl mode. The **no** form of this command removes the configuration. By default, the action is forward.

action drop
no action drop

Use this command to set redirect action of submap in vacl mode. The **no** form of this command removes the configuration. By default, the action is forward.

action redirect { **GigabitEthernet** | **Aggregateport | FastEthernet** } { *port_id* }
no action redirect { **GigabitEthernet** | **Aggregateport**| **FastEthernet** } { *port_id* }

Parameter description

Parameter	Description
port_id	Redirection port.

Default configuration

When there is no specific action of submap, the action is forward by default. One submap only has one action.

Command mode	VACL mode.

Examples	`DES-7210(config-access-map)# action forward`
	`DES-7210(config-access-map)# action drop`
	`DES-7210(config-access-map)# action redirect gigabitEthernet 0/50`

55.1.4 vlan filter

Use this command to apply hostmap in vlan. The **no** form of this command removes the configuration.

vlan filter *map_name* **vlan-list** *vlan_id*
no vlan filter *map_name* **vlan-list** *vlan_id*

Parameter description

Parameter	Description
map_name	Hostmap keyword.
vlan-id	Vlan id.

Command mode	Global configuration mode.
Usage guidelines	When applying vlan access map to multiple vlans, you shall separate the vlans in comma or input the vlan range. For example, vlan filter aa vlan-list 1-33 means applying map to vlans from 1 to 33.
Examples	The following example applies **vlan access map** of hostmap ff in vlan 5: `DES-7210(config)# vlan filter ff vlan-list 5`

55.2 Showing Related Commands

55.2.1 show vlan access-map

Use this command to view the configuration of all hostmaps in the privileged EXEC mode:

show vlan access-map

Use this command to view the configuration of a specified hostmap in the privileged EXEC mode:

show vlan access-map *map_name*

Parameter description

Parameter	Description
map_name	Hostmap keyword.

Command mode

Privileged EXEC mode.

Examples

The following example is a result of executing **show vlan access map***:*

```
DES-7210(config)# show vlan access-map
Vlan access-map aa  10
match mac address:   700, 710, m1, 720,
action: forward
Vlan access-map aa  20
match ip address:   10, 20, 30, sp1, sp2, 60, 50, 80,
action: drop
Vlan access-map dd  20
match mac address:   710, 720, m1, 760,
action: forward
DES-7210(config)#
```

The following example is a result of executing **show vlan access map** { *map_name* }*:*

```
DES-7210(config)# show vlan access-map dd
Vlan access-map dd  20
match mac address:   710, 720, m1, 760,
action: forward
DES-7210(config)#
```

55.2.2 show vlan filter

Use this command to view the application of all the hostmaps in vlan in the privilegedEXEC mode:

show vlan filter

Command mode	Privileged EXEC mode.

Examples	The following example is a result of executing Show vlan filter access-map aa:
	`DES-7210(config)# show vlan filter`
	`VLAN Map aa`
	`Configured on VLANs: 1, 5, 6,`
	`DES-7210(config)#`

Related commands

Command	Function
show vlan filter *access-map map_name*	View the application of a specified hostmap in vlan.
show vlan filter vlan *vlan_id*	View the hostmap application ina specified vlan.

56 QoS Configuration Command

56.1 Default Configuration

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

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

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

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

Default CoS to queue mapping table:

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

Default CoS to DSCP mapping table

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

Default IP Precedence to DSCP mapping table

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

Default DSCP to CoS mapping table

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

56.2 Related Configuration Commands

56.2.1 mls qos trust

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

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

no mls qos trust

Parameter description

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

Default configuration N/A.

Command mode	Interface configuration mode.
Examples	`DES-7210(config)# interface gigabitethernet 1/1` `DES-7210(config-if)# mls qos trust cos`
Related commands	**show mls qos interface** *interface-id*
Platform description	DES-7200 series support the parameter **cos dscp ip-precedence.**

56.2.2 mls qos cos

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

mls qos cos *default-cos*

no mls qos cos

Parameter description

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

Default configuration	The CoS value is 0.
Command mode	Interface configuration mode.
Examples	`DES-7210(config)# interface gigabitethernet 1/1` `DES-7210(config-if)# mls qos cos 7`
Related commands	**show mls qos interface** *interface-id*

56.2.3 class maps

Use the following command to creat an ACL:

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

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

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

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

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

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

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

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

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

Parameter description

Parameter	Description
acl-name	Name of the created ACL
acl-id	ID of the created ACL
class-map-name	Name of the class map to be created
no class-map *class-map-name*	Delete the existed class map.
no match access-group a*cl-name*| *acl-id*	Delete the match.

Command mode

Global configuration mode.

Examples

Create an extended MAC ACL named me.

```
DES-7210(config)# mac access-list extended me
```

Set ACL rules.

```
DES-7210(config-ext-macl)# permit host 1111.2222.3333 any
```

Exit the ACL setting.

```
DES-7210(config-ext-macl)# exit
```

Create a class map named **cm.**

```
DES-7210(config)# class-map cm
```

Associate the class map and the ACL.

```
DES-7210(config-cmap)# match access-group me
```

Exit the class map setting.

```
DES-7210(config-cmap)# exit
```

Related commands	**show mac access-lists**
	show ip access-lists
	show class-map

56.2.4 policy maps

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

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

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

[no] class *class-map-name*

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

set ip dscp *new-dscp*

no set ip dscp

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

police *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value*}]

no police

Parameter description

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

	dscp-value	Overwrite the DSCP value of the packets exceeding the bandwidth, whose range varies with products.

Command mode

Global configuration mode

Examples

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

```
DES-7210(config)# policy-map po
```

Associate class-map cm

```
DES-7210(config-pmap)# class cm
```

Set the DSCP value as 10

```
DES-7210(config-pmap-c)# set ip dscp 10
```

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

```
DES-7210(config-pmap-c)# police 1000000 4096 exceed-action dscp 16
```

Related commands

show policy-map

56.2.5 service-policy

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

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

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

Parameter description

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

Command mode

Interface configuration mode, and virtual-group configuration mode.

Examples

```
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# service-policy input po
DES-7210(config)# virtual-group 3
DES-7210(config-if)# service-policy input po
```

Related commands	**show mls qos interface.**

Platform description	DES-7200 series support the parameter **input** and **output.** The parameter **output** is not supported in the virtual-group.

56.2.6 priority-queue

Use this command to configure the output queue scheduling algorithm.

priority-queue

[no] priority-queue

Parameter description

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

Default configuration	The output queue scheduling algorithm is WRR.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# no priority-queue`
Related commands	**show mls qos queuing**

53.2.7 priority-queue cos-map

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

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

no priority-queue cos-map

Parameter description

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

Default configuration See default configuration.

Command mode Global configuration mode.

Examples

```
DES-7210(config)#priority-queue cos-map 1 0 1
```

Related commands **show mls qos queuing**

56.2.7 wrr-queue bandwidth

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

wrr-queue bandwidth *weight1 ... weightn*

no war-queue bandwidth

Parameter description

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

Default configuration weight1: ...: weightn = 1:..:1

Command mode Global configuration mode

Examples	`DES-7210(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8`
Related commands	**show mls qos queuing**

56.2.8 mls qos map cos-dscp

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

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

no mls qos map cos-dscp

Parameter description

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

Default configuration	See the default configuration.
Command mode	Global configuration mode
Examples	`DES-7210(config)# mls qo map cos-dscp 8 10 16 18 24 26 32 34`

Related commands

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

56.2.9 mls qos map dscp-cos

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

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

no mls qos map dscp-cos

Parameter description

Parameter	Description
dscp-list	DSCP list. Its range varies with

	products.
cos	COS value ranging 0 to 7
no	Restore to the default value.

Default configuration

See the default configuration.

Command mode

Global configuration mode.

Examples

```
DES-7210(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

Related commands

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

56.2.10 interface rate-limit

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

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

no rate-limit

Parameter description

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

Command mode

Interface configuration mode.

Examples

```
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# rate-limit input 1000000 4096
```

Related commands	**show mls qos interface.**

56.2.11 mls qos scheduler

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

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

no mls qos scheduler

Parameter description

Parameter	Description
sp	Absolute priority scheduling
rr	Round-robin scheduling
wrr	Frame count weighted round-robin scheduling
drr	Frame length weighted round-robin scheduling
no	Restore to the default value.

Default configuration	The queue scheduling algorithm is wrr by default.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# mls qos scheduler sp`
Related commands	**show mls qos scheduler.**

56.2.12 drr-queue bandwidth

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

drr-queue bandwidth *weight1...weight8*

no drr-queue bandwidth

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

Default configuration	See the default configuration.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# drr-queue bandwidth 1 2 3 4 5 6 7 8`
Related commands	**show mls qos queuing**

56.2.13 mls qos map ip-prec-dscp

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

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

no mls qos map ip-prec-dscp

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

Default configuration	See the default configuration.
Command mode	Global configuration mode.
Examples	`DES-7210(config)# mls qo map ip-prec -dscp 8 10 16 18 24 26 32 34`

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

56.2.14 wrr-queue bandwidth

Use this command to configure the corresponding queue on the condition that the queue uses wrf schedule algorithm.

wrf-queue *queue-id* **bandwidth** *min max*

no wrf-queue *queue-id* **bandwidth**

Parameter description	Parameter	Description
	queue-id	Queue ID.
	min	The minimum bandwidth..
	max	The maximum bandwidth.

Default configuration	Min: the minimum interface bandwidth, in kbps; Max; the maximum interface bandwidth, in kbps
Command mode	Interface configuration mode.
Usage guidelines	Use this command to configure the minimum and maximum interface bandwidth on the condition that the queue uses wrf schedule algorithm.

Examples

The following example sets the queue to use wrf schedule algorithm:

```
DES-7210(config)# mls qos scheduler wrf
DES-7210(config)# show mls qos scheduler
```

The following example configures the minimum and maximum bandwidth:

```
DES-7210(config-if)# wrf-queue 2 bandwidth 10 10240
DES-7210(config-if)# wrf-queue 4 bandwidth 7 10240
DES-7210(config-if)# show running
```

Related commands	Command	Description
	show mls qos	Show QOS schedule method.

	scheduler	

Platform description

The software version must be R10.1 and higher.

56.2.15 wrf-queue-sp

Use this command to configure whether to use strict priority(SP) or not for the queue, on the condition that the queue uses wfq schedule algorithm. **wrf-queue** *queue-id* **sp**

no wrf-queue *queue-id* **sp**

Parameter description

Parameter	Description
queue-id	Specify the DSCP value.
sp	Restore to the default value.

Default configuration

SP is not used.

Command mode

Global configuration mode.

Usage guidelines

Use this command to enable the queue to use sp+wrf schedule algorithm, on the condition that the queue uses wrf schedule algorithm.

Examples

The following example enables the queue to use wrf schedule algorithm:

```
DES-7210(config)# mls qos scheduler wrf
DES-7210(config)# show mls qos scheduler
```

The following example configures queue 1 and queue 3 to use SP:

```
DES-7210(config)# wrf-queue 1 sp
DES-7210(config)# wrf-queue 3 sp
DES-7210(config)# show running
```

Related commands

Command	Description
show mls qos scheduler	Show QOS schedule method.

Platform description	The software version must be R10.1 and higher.

56.2.16 virtual-group

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

virtual-group *virtual-group-number*

no virtual-group *virtual-group-number*

Parameter description

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

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

Examples	The following example sets the interface gigabitEthernet 1/3 as the member of virtual group 3:
	enables the queue to use wrf schedule algorithm:
	`DES-7210(config)# interface gigabitethernet 1/3`
	`DES-7210(config-if)# virtual-group 3`

Related commands

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

Platform description	The software version must be R10.1 and higher.

56.3 Showing Related Command

56.3.1 show class-map

Use this command to show the information of class maps.

show class-map [*class -name*]

Parameter description

Parameter	Description
class-name	Name of the class map

Default configuration	All class maps are shown by default.
Command mode	Privileged EXEC mode.
Examples	`DES-7210# show class-map`

56.3.2 show policy-map

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

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

Parameter description

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

Default configuration	All policy maps are shown by default.

Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show policy-map
```

56.3.3 show mls qos interface

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

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

Parameter description

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

Default configuration	The QoS information of all ports is shown.
Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show mls qos interface fastEthernet 0/1
```

56.3.4 show mls qos virtual-group

Use this command to display the police information associated with the virtual-group.

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

Parameter description

Parameter	Description
virtual-group-number	Virtual group number.
policers	Show the police associated with the interface

Default configuration	The QoS information of all ports is shown.
Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show mls qos virtual-group 1

DES-7210# show mls qos virtual-group policerss
```

56.3.5 show mls qos queuing

Use this command to show the QoS queuing information.

show mls qos queueing

Command mode Privileged EXEC mode.

Examples

```
DES-7210# show mls qos queueing
```

Platform description DES-7200 series show cos-to-queue map, wrr weight, and drr weight.

56.3.6 show mls qos scheduler

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

show mls qos scheduler

Command mode Privileged EXEC mode.

Examples

```
DES-7210# show mls qos scheduler
```

Platform description This command is supported on DES-7200 series.

56.3.7 show mls qos maps

Use this command to show QoS maps.

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

Parameter description

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

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

Default configuration All QoS maps are shown by default.

Command mode Privileged EXEC mode.

Examples

```
DES-7210# show mls qos maps
```

56.3.8 show mls qos rate-limit

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

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

Parameter description

Parameter	Description
interface	Interface ID

Command mode Privileged EXEC mode.

Examples

```
DES-7210# show mls qos rate-limit
```

56.3.9 show virtual-group

Use this command to show the virtual group information.

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

Parameter description

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

Command mode Privileged EXEC mode.

Examples

```
DES-7210# show virtual-group 1

DES-7210# show virtual-group summary
```

57 VRRP Configuration Commands

57.1 Configuration Related Commands

The VRRP configuration commands include:

- **vrrp authentication**
- **vrrp delay**
- **vrrp description**
- **vrrp ip**
- **vrrp preempt**
- **vrrp priority**
- **vrrp timers advertise**
- **vrrp timers learn**
- **vrrp track**

57.1.1 vrrp authentication

Use this command to enable VRRP authentication . The **no** format of this command disables the function.

vrrp *group* **authentication** *string*

no vrrp *group* **authentication**

Parameter description

Parameter	Description
group	VRRP group number
string	String for the VRRP group authentication (within 8 bytes, plaintext password)

Default configuration	By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, no authentication password is configured by default.
Command mode	Interface configuration mode.
Usage guidelines	The devices in the same VRRP group must have the same authentication password configured. The plaintext authentication password cannot provide security. It aims only to prevent/prompt the incorrect VRRP configuration.
Examples	The example below sets the authentication password for VRRP group 1. `vrrp 1 authentication x30dn78k`

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group ip ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.

57.1.2 vrrp delay

Use this command to set the reload latency of the VRRP group on the interface.

vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }

no vrrp delay

Parameter description

Parameter	Description
min-seconds	When the interface is up, VRRP group shall be reloaded after at least min-seconds.
reload-seconds	The reload latency of the VRRP group. If the configured min-seconds is more than reload-seconds, the actual reload latency of the VRRP group will be min-seconds.

Default configuration	By default, the VRRP reload delay function is not enabled on the interface.
Command mode	Interface configuration mode.
Usage guidelines	Use this command to set the reload latency of the VRRP group on the interface, when it is required that the VRRP group shall not be reloaded immediately after the system reloads or the interface is up. The reload latency range is 0-60.

Examples	The example below sets the VRRP reload latency on E0 to 10s. When E0 is up, VRRP group 1 shall be reloaded in 10s.
	`interface FastEthernet 0/0`
	`shutdown`
	`ip address 10.0.1.1 255.255.255.0`
	`vrrp delay minimum 10`
	`vrrp 1 ip 10.0.1.20`
	`no shutdown`
	`show vrrp 1`

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.

Plarform description	The software version must be R10.3(4) and higher.

57.1.3 vrrp description

Use this command to specify a descriptor for the VRRP. The **no** form of it restores it to the default.

vrrp *group* **description** *text*

no vrrp *group* **description**

Parameter description

Parameter	Description
group	VRRP group number
text	VRRP group descriptor

Default configuration

By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, no VRRP group descriptor is configured by default.

Command mode

Interface configuration mode.

Usage guidelines

This command will set the descriptor for the VRRP group to facilitate the identification of the VRRP group.

Examples

The example below labels the VRRP group 1 on Ethernet interface E0 as Building A – Marketing and Administration:

```
interface FastEthernet 0/0
ip address 10.0.1.1 255.255.255.0
vrrp 1 ip 10.0.1.20
vrrp 1 description "Building A - Marketing and Administration"
```

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group* ip *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device

57.1.4 vrrp ip

Use this command to enable VRRP on the interface and specify the related virtual IP address. The **no** format of the command disables the VRRP function and removes the setting of virtual IP address.

vrrp *group* **ip** *ipaddress* [**secondary**]

no vrrp *group* **ip** *ipaddress* [**secondary**]

Parameter description

Parameter	Description
group	VRRP group number of the virtual device
ipaddress	IP address of the virtual device
secondary	Specify the secondary IP address of the

		virtual device.

Default configuration	Disabled.
Command mode	Interface configuration mode.
Usage guidelines	If the **secondary** parameter is not used, the IP address set here will become the master IP address of the virtual device. Note that if the VRRP group is using the IP address of the Ethernet interface, an error occurs when you remove the IP address of the VRRP group with the **no** command, because there are duplicated IP address in the LAN.

Examples	The example below enables the VRRP function on Ethernet interface 0. The VRRP group number is 1, primary IP address of the virtual device is 10.0.1.20 and secondary IP address is 10.0.2.20.
	`interface FastEthernet 0/0`
	`no switchport`
	`ip address 10.0.1.1 255.255.255.0`
	`ip address 10.0.2.1 255.255.255.0 secondary`
	`vrrp 1 ip 10.0.1.20`
	`vrrp 1 ip 10.0.2.20 secondary`

Related commands

Command	Description
DES-7210# **show vrrp** [**brief | group**]	Show the VRRP configuration.

57.1.5 vrrp preempt

Use this command to set the preemption mode of the VRRP group. The **no** command disables the VRRP preemption function.

vrrp *group* **preempt** [**delay** *seconds*]

no vrrp *group* **preempt**[**delay**]

Parameter description

Parameter	Description
group	VRRP group number
delay *seconds*	(Optional)Specify the delay before a

		device declares itself master. The default value is 0s.

Default configuration	By default, the VRRP function is not enabled on the interface. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.
Command mode	Interface configuration mode.
Usage guidelines	If the VRRP group is working in the preemption mode, once a device finds its priority is higher than the priority of the master, it will become the master device of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the master's priority, it will not become the master device of the VRRP group. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because that VRRP group has the highest priority and thus automatically becomes the master device in the VRRP group.

Examples	In the example below, once the VRRP group finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 s:
	`vrrp 1 preempt delay 15`
	`vrrp 1 priority 200`

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7210(config-if)# **vrrp** *group* **priority** *level*	Set the VRRP group priority.

57.1.6 vrrp priority

Use this command to specify the priority of the VRRP group. The **no** form of this command restores it to the default.

vrrp *group* **priority** *level*

no vrrp *group* **priority**

Parameter description

Parameter	Description
group	VRRP group number
level	VRRP group priority

Default configuration

By default, the VRRP function is not enabled on the interface. Once the VRRP function is enabled, the default priority of the VRRP group is 100.

Command mode

Interface configuration mode.

Usage guidelines

None.

Examples

The example below sets the priority of VRRP group 1 as 254.

```
vrrp 1 priority 254
```

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7210(config-if)# **vrrp** *group* **preempt** [**delay** *seconds*]	Set the VRRP in the preemption mode.

57.1.7 vrrp timers advertise

Use this command to specify the interval for the master device to send the VRRP advertisement. The **no** form of this command restores it to the default.

vrrp *group* **timers advertise** *interval*

no vrrp *group* **timers advertise**

Parameter description

Parameter	Description
group	VRRP group number
interval	Advertisement interval (in seconds)

Default configuration	By default, the VRRP function is not enabled on the interface. Once the VRRP function is enabled, the default advertisement interval of the master device is 1 second.
Command mode	Interface configuration mode.
Usage guidelines	If the current device becomes the master device in the VRRP group, it will notify its VRRP status, priority and other information by sending the VRRP advertisement in the set interval.
Examples	The example below sets the VRRP advertisement interval as 4 seconds. `vrrp 1 timers advertise 4`

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7210(config-if)# **vrrp group timers learn**	Enable the timer learning function.

57.1.8 vrrp timers learn

Use this command to enable the timer learning function. The **no** format of it disables the function.

vrrp *group* **timers learn**

no vrrp *group* **timers learn**

Parameter description

Parameter	Description
group	VRRP group number

Default configuration	By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, the timer learning function is disabled by default.
Command mode	Interface configuration mode.

Usage guidelines	Once the timer learning function is enabled, if the current device is a VRRP backup device, it will learn the VRRP advertisement interval from the VRRP advertisement of the master device, with which it calculates the master device's failure interval instead of the VRRP advertisement interval configured locally. This command may synchronize the VRRP advertisement timer with the master device.
Examples	The example below enables the timer learning function on VRRP group 1. `vrrp 1 timers learn`

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7210(config-if)# **vrrp** *group* **timers advertise** [**msec**] *interval*	Set the VRRP advertising interval.

57.1.9 vrrp track

Use the **vrrp** *group* **track** *interface-type number* command to enable the VRRP track in the interface configuration mode. Use the **vrrp** *group* **track** *ip_address* command to enable the VRRP IP address track. Use the **vrrp** *group* **track bfd** command to track the specified neighbor IP addrss via BFD. Use the **no** form of this command to disable this function.

vrrp *group* **track [***interface-type number* | **bfd** *interface-type number ipv4-address***]** [*priority*]

vrrp *group* **track** *ip-address* [[[**interval** *interval-value*] **timeout** *timeout-value*] *priority*]

vrrp *group* **track [***interface-type number* | **bfd** *interface-type number ipv4-address***]** [*ip-address*]

Parameter description

Parameter	Description
group	VRRP group number
interface-type	Type of monitored interface
number	Number of the monitored interface
Ipv4-address	Monitored IPv4 address. With BFD configured, it refers to the neighbor IP address.

interval-value	The interval of time to probe whether the monitored ip address is reachable or not. If this parameter is not selected, the default value is 3s.
timeout-value	The timeout time of the unreachable monitored ip address. If this parameter is not selected, the default value is 1s.
interface-priority	VRRP priority change range when the interface or ip address reachability status changes. If this parameter is not selected, the default value is 10.

Default configuration

By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, no interface or ip address is specified.

Command mode

Interface configuration mode.

Usage guidelines

This command can be used to monitor the outlet links. Note that layer-3 routable logical interfaces can be monitored (such as Routed Port, SVI, Loopback and Tunnel). This command can also be used to monitor the reachability of the specified IP address.

Examples

The example below enables the VRRP group 1 to monitor the routed port Fa1/1. If the Fa1/1 link is disconnected, the priority of the VRRP group decreases by 30. When the Fa1/1 link recovers, the priority of VRRP group 1 is restored.

```
vrrp 1 track FastEthernet 1/1 30
```

The example below shows how to set the VRRP to track the specified neighbor IP address 192.168.1.3 through BFD:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#interface FastEthernet 0/1
DES-7210(config-if)#no switchport
DES-7210(config-if)#ip address 192.168.1.1 255.255.255.0
DES-7210(config-if)#bfd interval 50 min_rx 50 multiplier 3
DES-7210(config)#interface FastEthernet 0/2
```

```
DES-7210(config-if)#no switchport
DES-7210(config-if)#ip address 192.168.201.17 255.255.255.0
DES-7210(config-if)#vrrp 1 priority 120
DES-7210(config-if)#vrrp 1 ip 192.168.201.1
DES-7210(config-if)#vrrp 1 track bfd FastEthernet 0/1 192.168.1.3
30
DES-7210(config-if)#end
```

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.
DES-7210(config-if)# **vrrp** *group* **priority** *level*	Set the VRRP group priority.

57.2 VRRP Monitoring and Maintenance Commands

VRRP monitoring and maintenance commands include:

- **debug vrrp**
- **debug vrrp errors**
- **debug vrrp events**
- **debug vrrp packets**
- **debug vrrp state**

57.2.1 debug vrrp

Use this command to turn on the VRRP error prompt, VRRP event, VRRP message and status debug switches. The **no** form of this command turns off the switches.

debug vrrp

no debug vrrp

Default configuration By default, the debug switches are turned off.

Command mode Privileged mode.

Examples

In the example below, the user turns on the VRRP debug switch.

```
DES-7210# debug vrrp
DES-7210#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Master -> Backup
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual
address 192.168.1.1
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Backup -> Master
DES-7210#
```

Related commands

Command	Description
DES-7210# **debug vrrp errors**	Turn on the VRRP error prompt debugging switch.
DES-7210# **debug vrrp events**	Turning on the VRRP event debugging switch.
DES-7210# **debug vrrp state**	Turning on the VRRP state debugging switch.

57.2.2 debug vrrp errors

Use this command to turn on the VRRP error prompt debug switch. The **no** form of this command turns off the switch.

debug vrrp errors

no debug vrrp errors

Default configuration

By default, the VRRP error debug switch is turned off.

Command mode

Privileged mode.

Examples

In the example below, the user turns on the VRRP error debug switch.

```
DES-7210# debug vrrp errors
DES-7210#
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual
address 192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual
address 192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual
address 192.168.1.1
```

57.2.3 debug vrrp events

Use this command to turn on the VRRP event debug switch. The **no** form of this command turns off the switch.

debug vrrp events

no debug vrrp events

Default configuration	By default, the VRRP event debug switch is turned off.
Command mode	Privileged mode.

Examples	In the example below, the user turns on the VRRP event debug switch.
	`DES-7210# debug vrrp events`
	`VRRP: Grp 1 Event - Advert higher or equal priority`
	`VRRP: Grp 1 Event - Advert higher or equal priority`
	`VRRP: Grp 1 Event - Advert higher or equal priority`

57.2.4 debug vrrp packets

Use this command to turn on the VRRP packet debug switch. The **no** form of this command turns off the switch.

debug vrrp packets

no debug vrrp packets

Default configuration	By default, the VRRP packet debug switch is turned off.
Command mode	Privileged mode.

Examples	In the example below, the user turns on the VRRP packet debug switch, where the checksum of the packets of VRRP group 1 is displayed.
	`DES-7210# debug vrrp packets`
	`DES-7210#`
	`VRRP: Grp 2 sending Advertisement checksum DD4D`
	`VRRP: Grp 2 sending Advertisement checksum DD4D`
	`VRRP: Grp 2 sending Advertisement checksum DD4D`

	In the example below, the user turns on the VRRP packet debug switch, where the source IP address of the VRRP group 1 packets and the priority of VRRP group 1 are displayed. DES-7210# **debug vrrp packets** DES-7210# VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213 VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213 VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213

57.2.5 debug vrrp state

Use this command to turn on the VRRP status debug switch. The **no** form of this command turns off the switch.

debug vrrp state

no debug vrrp state

Default configuration	By default, the VRRP debug switch is turned off.
Command mode	Privilege mode.
Examples	In the example below, the user turns on the VRRP status debug switch. DES-7210# **debug vrrp state** DES-7210# %VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Backup %VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Backup -> Master DES-7210# **config terminal** Enter configuration commands, one per line. End with CNTL/Z. DES-7210(config)# interface fastethernet *0/0* DES-7210 (config-if)#**no shutdown** DES-7210(config-if)# **end** DES-7210# %VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Init

57.3 Showing Related Command

57.3.1 show vrrp

Use this command to show the VRRP information.

show vrrp [**brief** | *group*]

Parameter description

Parameter	Description
brief	(Optional) Show the brief of the VRRP group.
group	Number of the VRRP group to be displayed

Command mode

Privileged mode.

Usage guidelines

If no optional parameter is used, the information of all VRRP groups is displayed.

Examples

Show the information of all VRRP groups:

```
DES-7210# show vrrp
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Device is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
DES-7210#
```

Show the brief information of the VRRP group:

```
DES-7210# show vrrp brief
Interface    Grp Pri Time  Own Pre State   Master addr   Group addr
FastEthernet 0/0  1  100   -  -  P  Backup  192.168.201.213 192.168.201.1
FastEthernet 0/0  2  120   -  -  P  Master  192.168.201.217 192.168.201.2
DES-7210#
```

	Command	Description
Related commands	DES-7210(config-if)# **vrrp** *group ip ipaddress* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device.

57.3.2 show vrrp interface

Use this command to show the information of the VRRP on the interface.

show vrrp interface *type number* [**brief**]

	Parameter	Description
Parameter description	*type*	Interface type
	number	Interface number
	brief	(Optional) Show the brief of the VRRP group on the interface.

Command mode	Privileged mode.

Examples

The example below shows the VRRP information on Ethernet interface E1/0

```
DES-7210# show vrrp interface fastethernet 0/0
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Device is 192.168.201.217 (local), priority is 120
```

```
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
```

Related commands

Command	Description
DES-7210(config-if)# **vrrp** *group* **ip** *ip address* [**secondary**]	Enable the VRRP function and set the IP address for the virtual device

58 RERP Configuration Commands

58.1 Related Configuration Commands

The RERP configuration commands include global configuration commands and RERP region mode configuration commands.

The global mode configuration commands include:

- **rerp enable**
- **rerp hello-interval**
- **rerp fail-interval**
- **rerp region**

The RERP region mode configuration commands include:

- **ring**
- **edge-ring**
- **major-ring**

58.1.1 rerp enable

Use this command to enable RERP globally. Use the **no** form of this command to disable the function.

rerp enable

no rerp enable

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.

Usage guidelines

Only when the global RERP is enabled, the configuration of other parameters will take effect.

Examples

The following example shows how to enable RERP:

```
DES-7210(config)# rerp enable
```

Related commands

Command	Description
rerp region	Create a RERP domain.

58.1.2 rerp hello-interval

Use this command to configure the interval at which the RERP sends the Hello message on the primary port. Use the **no** form of this command to restore it to the default value.

rerp hello-interval *interval*

no rerp hello-interval

Parameter description

Parameter	Description
interval	Interval of sending the Hello message, in the range 1 to 6 seconds

Default

1 seconds.

Command mode

Global configuration mode.

Usage guidelines

The detection interval must be less than the failure time.

Examples

The following example shows how to set the interval as 2s:

```
DES-7210(config)# rerp hello-interval 2
```

Related commands

Command	Description
rerp fail-interval	Configure the timeout time.

58.1.3 rerp fail-interval

Use this command to configure the maximum time for the RERP to wait on the secondary port to receive the Hello message from the primary port. This time is also used for the backup and transit device to wait before receiving the master IP address and clear packets. Use the **no** form of this command to restore it to the default value.

rerp fail-interval *num*

no rerp fail-interval

Parameter description

Parameter	Description
num	Maximum waiting time in the range 3 to 18 seconds

Default 3 seconds.

Command mode Global configuration mode.

Usage guidelines This command is used together with the detection interval and must be larger than the detection interval.

Examples The following example shows how to set the failure interval as 6 seconds:

```
DES-7210(config)# rerp fail-interval 6
```

Related commands

Command	Description
rerp hello-interval	Configure detection interval.

58.1.4 rerp region

Use this command to create a RERP region and enter the RERP region configuration mode. Use the **no** form of this command to restore it to the default value.

rerp region *num*

no rerp region *num*

Parameter description

Parameter	Description
num	Region ID in the range 1 to 64

Default	N/A.
Command mode	Global configuration mode.
Usage guidelines	When a region is created, this device is allowed to enter this region.
Examples	The example below demonstrates how to use this command: `DES-7210# rerp region 1`

Related commands

Command	Description
rerp enable	Enable RERP globally.

58.1.5 ring

Use this command to configure the role of device in the specified region.

ring *num* **role** [**master** | **backup** | **transit**] **ctrl-vlan** *vid* **primary-port interface** *interface-id* **secondary-port interface** *interface-id*

no ring *num*

Parameter description

Parameter	Description
num	Ring ID.
master|backup|transit	Configure the device as a master/ backup/slave device.
vid	Control vlan ID.
Interface-id	Interface identifier.

Default	N/A.
Command mode	RERP region configuration mode.
Usage guidelines	Each device plays only one role in a RERP ring. One RERP ring can configure only one master device and one backup device. The port joined the RERP ring is configured as the trunk port automatically, and native vlan is configured as the control vlan automatically.

Examples

```
DES-7210(config)# rerp region 1
DES-7210(config-rerp)# ring 1 role master ctrl-vlan 100
primary-port interface GigabitEthernet 0/1
secondary-port interface GigabitEthernet 0/2
```

Related commands

Command	Description
rerp region	Create a RERP region.

58.1.6 edge-ring

Use this command to configure the sub-ring. One RERP ring shall be configured before this command execution.

edge-ring *num* **role** [**primary-edge|secondary-edge**] **ctrl-vlan** *vid* **shared-port interface** *interface-id* **sub-port interface** *interface-id*

no ring *num*

Parameter description

Parameter	Description
num	Ring ID.
primary-edge|secondary-edge	The device on the primary/secondary edge.
vid	Control VLAN ID.
Interface-id	Interface identifier.

Default N/A.

Command mode RERP region configuration mode.

Usage guidelines The shared port must have been configured in a RERP ring before. That is to say, one RERP ring shall be configured before this command execution.

Examples

```
DES-7210(config)# rerp region 1
DES-7210(config-rerp)# edge-ring 2 role primary-edge ctrl-vlan 200
shared-port interface GigabitEthernet 0/1 sub-port interface
GigabitEthernet 0/3
```

Related commands

Command	Description
rerp region	Create a RERP domain.
ring	Configure a RERP ring.

58.1.7 major-ring

Use this command to configure the edge-ring for the specified major-ring in order to enable the messages in the edge-ring to be transmitted on the major-ring interface.

major-ring *num* **edge-ring-vlan** *vid*

Parameter description

Parameter	Description
num	Major-ring ID.
vid	Control VLAN ID.

Default N/A.

Command mode RERP region configuration mode.

Usage guidelines Major-ring must have been configured before this command execution.

Examples The example below demonstrates how to use this command:

```
DES-7210(config)# rerp region 1
DES-7210(config-rerp)# major-ring 1 edge-ring-vlan 100
```

Related commands

Command	Description
rerp eanble	Enable RERP globally.

58.2 Showing and Monitoring Commands

The following commands are included:

- **show rerp**
- **show rerp statistics**
- **clear rerp statistics**

- **debug rerp**

58.2.1 show rerp

Use this command to show the RERP parameter and status.

show rerp

Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show rerp
rerp state                 : enable
rerp admin hello interval  : 1(*1s)
rerp admin fail interval   : 3(*1s)
rerp edge interval         : 1(*300 ms)
rerp local bridge          : 001a.a902.fe0b
-----------------------------------
region 1
ring                       : 1
rerp oper hello interval   : 1
rerp oper fail  interval   : 3
ring master                    : 001a.a902.fe0b
ctrl-vlan                      : 100
edge-vlan                      :
role                       : master
primary-port                   : Gi 0/4(forwarding)
secondary-port                 : Gi 0/21(down)
```

58.2.2 show rerp statistics

Use this command to show the RERP message statistics.

show rerp statistics region *num* **ring** *ring_id*

Command mode	Privileged EXEC mode.

Examples

```
DES-7210# sh rerp statistics regiong 1 ring 1
The statistics for region 1 ring 1 GigabitEthernet 0/4
```

```
TX hello packets       23, RX hello packets         0
TX edge-hello packets   0, RX edge-hello packets      0
TX flush packets        0, RX flush packets         0
TX down packets       0, RX down packets          0
TX up packets             0, RX up packets            0
TX major fail packets   0, RX major fail packets      0
TX major resume packets   0, RX major resume packets  0
TX sub complete packets   0, RX sub complete packets  0

The statistics for region 1 ring 1 GigabitEthernet 0/5
TX hello packets       23, RX hello packets         0
TX edge-hello packets   0, RX edge-hello packets      0
TX flush packets        0, RX flush packets         0
TX down packets       0, RX down packets          0
TX up packets             0, RX up packets            0
TX major fail packets   0, RX major fail packets      0
TX major resume packets   0, RX major resume packets  0
TX sub complete packets   0, RX sub complete packets  0
```

58.2.3 clear rerp statistics

Use this command to clear the RERP message statistics.

clear rerp statistics

Command mode	Privileged EXEC mode.

58.2.4 debug rerp

Use this command to turn on the RERP service debugging switch. The **no** form of this command is used to turn off the debugging switch.

debug rerp [**packet** | **event**]

undebug rerp [**packet** | **event**]

Parameter description

Parameter	Description
packet	Turn on the incoming/outgoing packet debugging switch.
event	Turn on the event debugging switch.

Command mode	Privileged EXEC mode.

59 REUP Configuration Commands

59.1 Related Configuration Commands

The REUP configuration commands include global configuration commands and interface mode configuration commands.

The global mode configuration commands include:

- **mac-address-table move update receive**
- **mac-address-table move update transmit**

The interface mode configuration commands include:

- **switchport backup interface** *interface-id* [**preemption** {**mode** { **forced** | **bandwidth** | **off** } | **delay** *delay-time*}]
- **mac-address-table update group**

59.1.1 switchport backup interface *interface-id*

Use this command to configure the REUP dual link backup interface.

switchport backup interface *interface-id*

no switchport backup

Parameter description	**Parameter**	**Description**
	Interface-id	Interface ID of the backup link.

Default	N/A.
Command mode	Interface configuration mode.
Usage guidelines	Enter the primary interface configuration mode, the interface-id in the

parameter is for the backup interface. When the active link fails, the backup link transmission is restored rapidly.

Examples

The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as primary interface and backup interface:

```
DES-7210(config)# interface fa 0/1

DES-7210(config-if)# switchport backup interface fa 0/2
```

Related commands

Command	Description
show interface switchport backup	View the dual link backup configuration on the switch.

59.1.2 switchport backup interface *interface-id* preemption

Use this command to configure the REUP link preemption function.

switchport backup interface *interface-id* **preemption mode** {**forced** | **bandwidth** | **off** }

switchport backup interface *interface-id* **preemption delay** *delay-time*

no switchport backup interface *interface-id* **preemption delay**

Parameter description

Parameter	Description
interface-id	The interface id of the backup link.
delay-time	The preemption delay time.

Default

The preemption function is disabled by default.
The default preemption delay time is 35s.

Command mode

Interface configuration mode.

Usage guidelines

The preemption mode includes **forced, bandwidth and off**. In the **bandwidth** preemption mode, the interface with high bandwidth has priority over other interfaces to transmit the data. In the **forced** preemption mode, the primary has priority over backup interfaces to transmit the data. No preemption event occurrs in the **off** preemption

	mode. By default, the preemption mode is off. The preemption delay refers to the delay time of the link reswitch after the restoration of the link failure.

Examples	The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as the primary interface and backup interface, set the bandwidth preemption mode and 40s preemption delay:
	`DES-7210(config)# interface fa 0/1`
	`DES-7210(config-if)# switchport backup interface fa 0/2`
	`preemption mode bandwitdh`
	`DES-7210(config-if)# switchport backup interface fa 0/2`
	`preemption delay 40`

Related commands

Command	Description
show interface switchport backup	View the dual link backup configuration.

59.1.3 mac-aadress-table move update receive

Use this command to enable REUP to receive the mac-address-table update messages.

mac-address-table move update receive

no mac-address-table move update receive

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	The dual link backup switchover will lead to the loss of downstream data flow, for the MAC address for the uplink switch has not been updated in time. Therefore, it is necessary to update the MAC address table of the uplink switch, to reduce the loss of L2 data flow. You need to enable the switch of receiving the MAC address update messages on the uplink switch.

Examples	`DES-7210(config)# mac-address-table move update receive`

Related commands

Command	Description
mac-address-table move update transit	Enable REUP to transmit the mac-address-table update messages.

59.1.4 mac-address-table move update transit

Use this command to enable REUP to transmit the mac-address-table update messages.

mac-address-table move update transit

no mac-address-table move update transit

Default	Disabled.
Command mode	Global configuration mode.
Usage guidelines	In order to reduce the link switchover and the loss of the downstream data flow, it is necessary to enable the switch of receiving the MAC address update messages on the uplink switch.
Examples	`DES-7210(config)# mac-address-table move update transit`

Related commands

Command	Description
mac-address-table move update transit	Enable REUP to receive the mac-address-table update messages.

59.1.5 mac-address-table update group

Use this command to set the mac-address-table update group.

mac-address-table update group [*group-num*]

no mac-address-table update group

Parameter description

Parameter	Description
group-num	The mac-address-table update group

	ID.

Default

The default group number is 1.

By default, no mac-address-table update group is configured.

Command mode

Interface configuration mode.

Usage guidelines

In order to reduce the flood due to the MAC address update and the influence on the normal data transmission of the switch, DES-7210 products add a configuration of MAC address update group. Only if all the interfaces are added to a MAC address update group, the downstream data transmission be restored rapidly.

Examples

```
DES-7210(config-if)# mac-address-table update group 2
```

Related commands

Command	Description
show mac-address-table update group detail	Show the mac-address-table update group information.

59.2 Showing and Monitoring Commands

The following commands are included:

- **show interfaces** [*interface-id*] **switchport backup** [**detail**]
- **show mac-address-table update group** [**detail**]

59.2.1 show interfaces [*interface-id*] switchport backup [detail]

Use this command to show the dual link backup information on the interfaces.

show interfaces [*interface-id*] **switchport backup** [**detail**]

Parameter description

Parameter	Description
Interface-id	The interface id of the dual link backup.
detail	Show the detailed information about the

	dual link backup.

Default Show the dual link backup information on all interfaces.

Command mode Privileged EXEC mode.

Examples

```
DES-7210 # show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface     Backup Interface      State

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

Gi0/23                 Gi0/24                 Active Up/Backup
Standby

Interface Pair : Gi0/23, Gi0/24

Preemption Mode : Off

Preemption Delay : 35 seconds

Bandwidth : Gi0/23(1000 Mbits), Gi0/24(1000 Mbits)
```

59.2.2 show mac-address-table update group [detail]

Use this command to show the mac-address-table update group information.

show mac-address-table update group [detail]

Parameter description

Parameter	Description
detail	Show the detailed information about the mac-address-table update group.

Default Show the mac-address-table update group information.

Command mode Privileged EXEC mode.

Examples

```
DES-7210# show mac-address-table update group detail

Mac-address-table Update Group:1

Received mac-address-table update message count:0

Group member  Receive Count    Last Receive Switch-ID    Receive
Time

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

Gi0/1         0              0000.0000.0000

Gi0/2         0              0000.0000.0000
```

60 RLDP Configuration Command

60.1 Configuration Related Commands

The RLDP configuration commands include global configuration commands, interface mode configuration commands and privilege mode configuration commands.

The global mode configuration commands include:

- **rldp enable**
- **rldp detect-interval**
- **rldp detect-max**

The interface mode configuration commands include:

- **rldp port** {**unidirection-detect | bidirection-detect | loop-detect**} {**warning | shutdown-svi | shutdown-port | block**}

The privilege mode commands include:

- **rldp reset**

60.1.1 rldp enable

Use this command to enable RLDP globally. Use the **no** form of this command to disable the function.

rldp enable

no rldp enable

Parameter description	N/A.
Default	Disabled.
Command mode	Global configuration mode.

Usage guidelines

You can enable RLDP on the interface only when the global RLDP is enabled.

Examples

The following example shows how to enable RLDP:

```
DES-7210(config)# rldp enable
```

Related commands

Command	Description
rldp port	Enable the RLDP function on the port.

60.1.2 rldp detect-interval

Use this command to configure the interval at which the RLDP sends the detection message on the port. Use the **no** form of this command to restore it to the default value.

rldp detect-interval *interval*

no rldp detect-interval

Parameter description

Parameter	Description
interval	Detection interval in the range 2 to 15 seconds

Default

3 seconds.

Command mode

Global configuration mode.

Usage guidelines

In the environment where STP is enabled, it is recommended that the product of interval multiplying the maximum number of detections is less than the topology convergence time of STP.

Examples

The following example shows how to set the detection interval as 5s:

```
DES-7210(config)# rldp detect-interval 5
```

Related commands

Command	Description
rldp detect-max	Set the maximum number of detections.

60.1.3 rldp detect-max

Use this command to set the maximum number of sending detection packets on the port. If the neighboring port does not respond when this detection number is exceeded, the link is considered faulty. Use the **no** form of this command to restore it to the default value.

rldp detect-max *num*

no rldp detect-max

Parameter description

Parameter	Description
num	Maximum number of detections in the range 2 to 10

Default

2.

Command mode

Global configuration mode.

Usage guidelines

This command is used together with the detection interval to specify the maximum number of detections.

Examples

The following example shows how to set the maximum number of detections as 5:

```
DES-7210(config)# rldp detect-max 5
```

Related commands

Command	Description
rldp detect-interval	Set the detection interval.

60.1.4 rldp port

Use this command to enable RLDP on the port and specify detection type and troubleshooting method. Use the **no** form of this command to disable the function.

rldp port {**unidirection-detect | bidirection-detect | loop-detect** } **{warning | shutdown-svi | shutdown-port | block}**

no rldp port { **unidirection-detect | bidirection-detect | loop-detect** }

Parameter description

Parameter	Description
unidirection-detect	Set unidirectional link detection.

bidirection-detect	Set bidirectional link detection.
loop-detect	Set loop detection type.
warning	Warn the user.
shutdown-svi	Shutdown the SVI the port belongs to.
shutdown-port	Shutdown the port.
block	Disable the learning-forwarding function of the port.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines The RLDP detection on the port takes effect only when the global RLDP is enabled.

Examples The following example demonstrates how to configure RLDP detection on fas 0/1, specify the detection type as loop detection, and troubleshooting method as block.

```
DES-7210(config)# interface fas 0/1
DES-7210(config-if)# rldp port loop-detect block
```

Related commands

Command	Description
rldp enable	Enable RLDP globally.

60.1.5 rldp reset

Use this command to make all the ports that have been handled using **rldp shutdown** or **disable** to perform RLDP detection again.

rldp reset

Parameter description N/A.

Default N/A.

Command mode	Privileged EXEC mode.

Examples

The example below demonstrates how to use this command:

```
DES-7210# rldp reset
```

Related commands

Command	Description
rldp eanble	Enable RIDP globally.

60.2 Showing and Monitoring Commands

The following commands are included:

- **show rldp** [**interface** *intervace-id*]
- **debug rldp** {**packet | event | error**}

60.2.1 show rldp

Use this command to show the RLDP information.

show rldp [**interface** *interface-id*]

Parameter description

Parameter	Description
interface-id	Interface ID

Command mode	Privileged EXEC mode.

60.2.2 debug rldp

Use this command to turn on the RLDP service debugging switch. The **no** form of this command is used to turn off the debugging switch.

- **debug rldp** [**packet | event | error**]
- **undebug rldp** [**packet | event | error**]

Parameter description

Parameter	Description
packet	Turn on the incoming/outgoing RLDP packet debugging switch.
event	Turn on the event debugging switch.
error	Turn on the error debugging switch.

Command mode	Privileged EXEC mode.

61 TPP Configuration Commands

61.1 Configuration Related Commands

61.1.1 topology guard

In the global configuration command mode, use this command to enable the topology protection function. Use the **no** form of this command to disable the topology protection function.

[no] topology guard

Default configuration	Enabled.
Command mode	Global configuration mode.
Usage guidelines	The topology protection function is enabled by default, so as to protect the network against topology oscillation due to attacks. It should be used with the **cpu topology-limit** command.

Examples	The following example shows how to enable and disable the global topology protection function:
	`DES-7210(config)# topology guard`
	`DES-7210(config)# no topology guard`

Related commands

Command	Description
tp-guard port enable	Enable the topology protection function on the interface.
cpu topology-limit	Set the CPU utilization limitation.

61.1.2 tp-guard port enable

Use this command to enable the topology protection function on the port. Use the **no** form of this command to disable the function.

[**no**] **tp-guard port enable**

Parameter description	N/A.
Default configuration	N/A.
Command mode	Interface configuration mode.
Usage guidelines	If both the global topology protection function and the topology protection function of the port are enabled, the remote device of this port will be notified when the CPU utilization of the local device is too high or there are other problems with the local device. This command is applicable to the layer 2 switching interfaces and routing interfaces. Other interfaces (including AP member port) do not support this command.

Examples	The following example shows how to configure the topology protection function for the port:
	`DES-7210(config-if)# tp-guard port enable`
	`DES-7210(config-if)# no tp-guard port enable`

Related commands

Command	Description
topology guard	Enable the topology protection function globally.

61.2 Showing Related Commands

61.2.1 show tpp

Use this command to show the configuration of topology protection.

show tpp

Parameter description	N/A.
Default configuration	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command is used to view the current TPP configuration and port detection.
Examples	The following example shows how to display information about the topology protection function: `DES-7210# show tpp`

Related commands

Command	Description
topology guard	Enable the topology protection function globally.

62 Supervisor Engine Redundancy Configuration Commands

62.1 Related Configuration Commands

The configuration commands for supervisor engine redundancy include the redundant mode commands and privileged mode commands.

The global configuration mode commands include:

- **redundancy**

The redundant mode commands include:

- **auto-sync**
- **auto-sync time-period**
- **switchover timeout**

The privileged mode commands include:

- **redundancy reload**
- **redundancy forceswitch**

62.1.1 redundancy

Use this command to enter redundancy configuration mode in the global configuration mode.

redundancy

Command mode	Global configuration mode.
Usage guidelines	Enter the redundancy configuration mode in the global configuration mode to execute the redundant mode commmands like auto-sync、

auto-sync time-period、switchover timeout,etc, to do the related redundancy configuration.

Examples

```
DES-7210# config terminal
DES-7210(config)# redundancy
DES-7210(config-rdnd)# exit
DES-7210(config)#
```

62.1.2 auto-sync

Use this command to synchronize runing-config and startup-config in the case of redundancy of dual supervisor engines. Use the **no** form of this command to disable the function.

auto-sync { **standard | running-config | startup-config}**

no auto-sync { **standard | running-config** | **startup-config**}

Parameter description

Parameter	Description
standard	Synchronize all the system files.
running-config	Synchronize the runtime configuration files.
startup-config	Synchronize the startup configuration files.

Default

All the files are synchronized by default.

Command mode

Redundancy configuration mode.

Usage guidelines

Generally the **standard** synchronization should be used if there is no special requirement.

Examples

The following example only synchronizes the **startup-config** files

```
DES-7210(config)# redundancy
DES-7210(config-rdnd)# auto-sync startup-config
DES-7210(config-rdnd)# exit
```

The following example synchronizes all the files other than the starup-config files.

```
DES-7210(config)# redundancy
DES-7210(config-rdnd)# no auto-sync startup-config
DES-7210(config-rdnd)# exit
```

62.1.3 auto-sync time-period

Use this command to configure the auto-sync time-period of runing-config and startup-config when the dual supervisor engines is redundant. Use the **no** form of this command to disable the function.

auto-sync time-period *value*

no auto-sync time-period

Parameter description

Parameter	Description
value	Auto-sync time-period interval (second).

Default

Auto-sync with 1 hour (3600 seconds) time-period interval

Command mode

Redundancy configuration mode.

Usage guidelines

Use standard synchronization if there is no particular demand.

Examples

The following example only synchronizes startup-config file:

```
DES-7210(config)# redundancy
DES-7210(config-rdnd)# auto-sync time-period 60
Redundancy auto-sync time-period: enabled (60 seconds).
DES-7210(config-rdnd)# exit
DES-7210(config)#
```

The following example disables auto-sync:

```
DES-7210(config)# redundancy
DES-7210(config-rdnd)# no auto-sync time-period
Redundancy auto-sync time-period: disabled. DES-7210(config-rdnd)#
exit
DES-7210(config)#
```

62.1.4 switchover timeout

In the redundancy configuration mode, use the **switchover timeout** command to configure the switchover timeout value for the supervisor engine. Use the **no** form of this command to restore the timeout to the default value.

switchover timeout *timeout-period*

no switchover timeout

Parameter description

Parameter	Description
timeout-period	Switchover timeout in the range 160 to 25,000 seconds (25 seconds).

Default 6000s.

Command mode Redundancy configuration mode.

Usage guidelines When the slave device has not received a heartbeat message of the master device within the timeout period, the switchover will occur. If you are not sure, do no modify the default value.

Examples

```
DES-7210# config terminal
DES-7210(config)# redundancy
DES-7210(config-rdnd)#
DES-7210(config-rdnd)# switchover timeout 4000
DES-7210(config-rdnd)# exit
DES-7210(config)# exit
DES-7210(config)#
```

62.1.5 redundancy reload

In the privileged EXEC mode, use the **redundancy reload** command to reset slave device or reset both master and slave devices.

redundancy reload {**peer** | **shelf**}

Parameter description

Parameter	Description
peer	Reset the slave device only.
shelf	Reset the master and slave devices.

Default N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	The **redundancy reload peer** does not affect the data transfer. During the resetting of the Slave, the data transfer is not disconnected and the user session information is not lost.
Examples	DES-7210# r**edundancy reload peer** Reload peer? [confirm] **y** Preparing to reload peer

Related commands

Command	Description
reload	Reset the master supervisor engine.

62.1.6 redundancy forceswitch

In privileged EXEC mode, use this command to enforce Slave supervisor engine to switchover.

redundancy forceswitch

Parameter description	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command allows you to select the slot in which the supervisor engine serves as the master supervisor engine and that as the slave supervisor engine, or the slot in which the supervisor engine is superior to that in another slot as the master board.
Examples	The current master supervisor engine is that in the M1 slot. After you execute the following command, the supervisor engine will degrade as the slave supervisor engine, and that in slot M2 upgrades as the master supervisor engine: DES-7210# **redundancy forceswitch** Proceed with switchover to standby PRE? [confirm]**y**

Related commands	**Command**	**Description**
	reload	Reset the master supervisor engine.

62.2 Showing and Monitoring Commands

It includes the following commands:

- **show redundancy** [**state | auto-sync | switchtimeout**]

62.2.1 show redundancy states

Use this command to show the current redundancy in the user mode or privileged EXEC mode.

Parameter description	**Parameter**	**Description**
	states	Show the redundancy status of the master or the slave devices.

Default	N/A.
Command mode	User mode or privileged EXEC mode
Usage guidelines	N/A.

Examples

```
DES-7210> enable
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210# show redundancy states
Redundancy stats:
         My state = 19 -ACTIVE
       peer state = 37 -STANDBY HOT
...
```

62.2.2 show redundancy auto-sync

Use command **show redundancy auto-sync** to show the current redundancy auto-sync mode in user EXEC or privileged EXEC mode. For the detailed information, please refer to auto-sync description in previous text.

Default	N/A
Command mode	User mode or Privileged EXEC mode.
Examples	DES-7210> **enable** DES-7210# **show redundancy auto-sync** Redundancy auto-sync mode: auto-sync standard. ...

62.2.3 show redundancy switchtimeout

Use **show redundancy switchtimeout** command to show current redundanct switchover timeout time in user EXEC or privileged EXEC mode.

Default	N/A
Command mode	User mode or Privileged EXEC mode.
Examples	DES-7210> **enable** DES-7210# **show redundancy switchtimeout** redundancy switch timeout is : 4000 ms. ...

63 File System Configuration Commands

63.1 Configuration Related Commands

The file system provides the following commands:

- **cd**
- **cp**
- **is**
- **makefs**
- **mkdir**
- **mv**
- **pwd**
- **rm**
- **rmdir**

63.1.1 cd

Use this command to enter the specified directory.

cd *directory*

Parameter description

Parameter	Description
directory	Specified directory

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines	Change the above parameter to the directory you want to enter. Use the ".." to represent the upeer-level directory and the "." to represent the current-level directory. Others can be determined according to the current location. This command supports relative directories and absolute directories. After entering the specified directory, you can verify it by using the **ls** command described above.
Examples	Enter the tmp sub-directory of the current directory: `DES-7210# cd tmp`

Related commands

Command	Description
ls	Show the contents in the current directory.

63.1.2 cp

Use this command to copy a file to the specified file or directory.

cp dest { *destine_file* | *directory* } **sour** *source_file*

cp sour *source_file* **dest** { *destine_file* | *directory* }

Parameter description

Parameter	Description
destine_file	Destination file
directory	Destination file or directory
source_file	Name of the file to copy (including the path)

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Copy the specified file to a new file or a directory. If the file already exists, the system will prompt whether to overwrite to cancel the operation.

Caution The current **cp** command does not support the wildcard and directory copy.

Examples	The following command copies the log.txt in the current directory to the higher-level directory: `DES-7210# cp sour log.txt dest ../log_bak.txt`

63.1.3 ls

Use this command to show the files in the current directory.

ls *pathname*

Parameter description

Parameter	Description
pathname	Optional, the path of the directory to show, defaulted to the contents in the current directory

Default	By default, only the information under the current working path is shown.
Command mode	Privileged EXEC mode.
Usage guidelines	Enter the specified directory to show the information of all the files in that directory. If no parameter is specified, the information of the files in the current directory is shown by default. This command does not support wildcard.

Examples	Show the information of all the files in the current directory:
	`DES-7210# ls`
	Show the information of all the files in the tmp directory:
	`DES-7210# ls tmp`

63.1.4 makefs

Use this command to format the device that the file system is to be loaded or the device that is to be managed by the file system.

makefs dev *devname* **fs** *fsname*

makefs fs *fsname***dev** *devname*

Parameter description

Parameter	Description
devname	Name of the device to be formatted (including the path)

	fsname	Name of the file system to be used on the device

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command is usually used in the following two cases: a. The device has never used in this file system. In order to normally use the file system on the device, you need to format the device the first time you use it; b. After the file system has been used for a period of time, if you want to delete all the files on the devices, you can use this command to clear all the data on the device.

Examples See the following example: If the jffs2 is the file system to be used, and the dev/mtdblock/1 is the device to be managed by the file system:

```
DES-7210# makefs dev /dev/mtdblock/1 fs jffs2
```

63.1.5 mkdir

Use this command to create a directory.

mkdir *directory*

Parameter description

Parameter	Description
directory	Name of the directory to be created.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines Simply enter the name of the directory you want to create (including the path).
If the path contains any directory that does not exist, the creation will fail.

Examples Create the test directory at the root directory:

	DES-7210# **mkdir** *test*

63.1.6 mv

Use this command to move the specified file to another file or directory.

mv sour *source_file* **dest** {*destine_file* | *directory*}

mv dest {*destine_file* | *directory*} **sour** *source_file*

Parameter description

Parameter	Description
source_file	The file to move
destine_file / directory	Destination file or directory

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines

This command outputs the contents of the specified file to the standard output device according to the parameters inputted on the command line.

Pay attention to the following two points: a. Input of the keywords (for example, **type and file**); b. Use of the '?' help key. If you are not sure which parameter to input, you can press the "?" key to show the prompt message.

Examples

The following example moves the log.txt to the upeer-level directory and renames it to config.txt. If a file with the same name already exists, the existing file will be replaced:

```
DES-7210# mv sour tmp/log.txt dest ../config.txt
```

The following example moves the log.txt to the tmp directory:

```
DES-7210# mv dest /mnt/tmp sour tmp/log.txt
```

63.1.7 pwd

Use this command to show the working path.

pwd

Default N/A.

Command mode	Privileged EXEC mode.
Usage guidelines	This command shows the current working path
Examples	The following example shows the current working path. `DES-7210# pwd`

63.1.8 rm

Use this command to delete the specified file.

rm *file*

Parameter description

Parameter	Description
file	Name of the file to be deleted (including the path)

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	This command does not support the wildcard and the deletion across file systems and across partitions. In addition, if a hard connection or symbol connection is deleted, the contents of the file are not affected.
Examples	Delete the log.txt file in the current directory: `DES-7210# rm log.txt`

Related commands

Command	Description
rmdir	Delete the specified empty directory. Since the command supports abbreviations, you can use the **rm** command to delete directories.

63.1.9 rmdir

Use this command to delete an empty directory.

rmdir *directory*

Parameter description

Parameter	Description
directory	Name of the directory to be deleted, which must be empty

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command does not support the wildcards, and the directory to be deleted must be empty. Since this command supports abbreviations, you can also use the **rm** command to delete empty directories.

Examples

If there is tmp directory in the current directory and the directory does not contain any files:

```
DES-7210# rmdir tmp
DES-7210# ls
```

64 Memory Configuration Commands

64.1 Showing Commands

64.1.1 show memory

Use this command to show the current memory usage information.

show memory

Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to view the current system memory state and usage information, including the system physical memory amount, the number of free pages in the current system, the free memory statistics.

Examples

```
DES-7210#show memory
System Memory Statistic:
  Free pages: 13031
  watermarks : min 378, lower 756, low 1534, high 1912
  System Total Memory : 128MB, Current Free Memory : 54892KB
  Used Rate : 58%
```

The above information includes the following parts:

1. Free pages: the memory size of one free page is about 4k;

2. Watermarks(see the following table)

Parameter	Description

min	The memory resources are extremely insufficient. It can only keep the kernel running. All application modules fails to run if the minimum watermark has been reached.
lower	The memory resources are severely insufficient. One route protocol will auto-exit and release the memory if the lower watermark has been reached. For the details, see the **memory-lack exit-policy** command.
low	The memory resources are insufficient. The route protocol will be in OVERFLOW state if the low watermark has been reached. In the overflow state, the routers do not learn new routes any more. The commands are not allowed to be executed when the memory lacks.
high	A plenty of memory resources. Each route protocol attempts to restore the state from OVERFLOW to normal.

3. System total memory, current free memory and used rate.

64.1.2 memory-lack exit-policy

Use this command to set the exit-policy of the upper route protocol when the memory reaches the lower threshold. The upper route protocol includes BGP,OSPF,RIP,PIM-SM.

memory-lack exit-policy {**lbgp** | **ospf** | **pim-sm** | **rip**}

no memory-lack exit-policy

Parameter description

Parameter	Description
bgp|ospf|pim-sm|rip	Specify the route protocol: BGP, OSPF, PIM or RIP.
no	Restore to the default action.

Defaults Exit from the route protocol which occupies the largest memory.

Command mode	Global configuration mode.
Usage guidelines	When the memory size reaches the lower threshold, a route protocol will be disabled to release the memory resources to ensure the operation of other protocols. The user shall know that what route protocols support the major services in the network. When the memory lacks, the user is able to disable the least important protocol to ensure the operation of major services. For example, in a user network, BGP route is irrelevant to the network core services. The user can configure the BGP exit-policy when the memory lacks. Specifying the disabled route protocol to take precedence to exit the policy can not help the system obtain enough memory resources. **Note** The exit-policy is used to protect the important network services to some degree. All route protocols will exit if more memory resources are exhausted. 2 minutes later, the route protocol will be attempting to restart.
Examples	This example shows how to enable the BGP to exit from the policy prior to other protocols: `DES-7210(config)# memory-lack exit-policy bgp`

Related commands

Command	Description
show memory	Show the current memory usage information.

64.1.3 show memory protocols

Use this command to display the usage of the memory for the route protocols.

show memory protocols

Parameter description

Parameter	Description
-	-

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to display the usage of the memory for the route protocols.

Note	Different switches and versions support different route protocols. The main route protocols are BGP,OSPF,RIP,LDP,PIM,ISIS, ect.

Examples

This example shows the result of the command **show memory protocols**:

```
DES-7210(config)# show memory protocols

=====================================================

protocol      |memory(byte)

BGP            102000000

OSPF           24000000

RIP            10000000

PIM            50000000

LDP            20000000

Total          206000000
```

Related commands

Command	Description
show memory	Show the current memory usage information.

65 CPU-LOG Configuration Commands

65.1 Related System Management commands

The following commands are included:

- **show cpu**
- **cpu-log**

65.1.1 show cpu

Use this command to show the CPU utilization information.

show cpu

Command mode	Privileged EXEC mode.
Usage guidelines	Use this command to show the system CPU utilization information in 5sec, 1 min and 5 min, and the CPU utilization of every task in 5sec, 1 min and 5 min.

Examples

```
DES-7210# show cpu
=====================================
    CPU Using Rate Information
CPU utilization in five seconds: 25%
CPU utilization in one minute  : 20%
CPU utilization in five minutes: 10%
  NO   5Sec   1Min   5Min   Process
  0     0%     0%     0%    LISR INT
  1     7%     2%     1%    HISR INT
  2     0%     0%     0%    ktimer
  3     0%     0%     0%    atimer
  4     0%     0%     0%    printk_task
```

```
 5    0%    0%    0%   waitqueue_process
 6    0%    0%    0%   tasklet_task
 7    0%    0%    0%   kevents
 8    0%    0%    0%   snmpd
 9    0%    0%    0%   snmp_trapd
10    0%    0%    0%   mtdblock
11    0%    0%    0%   gc_task
12    0%    0%    0%   Context
13    0%    0%    0%   kswapd
14    0%    0%    0%   bdflush
15    0%    0%    0%   kupdate
16    0%    3%    1%   ll_mt
17    0%    0%    0%   ll main process
18    0%    0%    0%   bridge_relay
19    0%    0%    0%   d1x_task
20    0%    0%    0%   secu_policy_task
21    0%    0%    0%   dhcpa_task
22    0%    0%    0%   dhcpsnp_task
23    0%    0%    0%   igmp_snp
24    0%    0%    0%   mstp_event
25    0%    0%    0%   GVRP_EVENT
26    0%    0%    0%   rldp_task
27    0%    2%    1%   rerp_task
28    0%    0%    0%   reup_event_handler
29    0%    0%    0%   tpp_task
30    0%    0%    0%   ip6timer
31    0%    0%    0%   rtadvd
32    0%    0%    0%   tnet6
33    2%    0%    0%   tnet
34    0%    0%    0%   Tarptime
35    0%    0%    0%   gra_arp
36    0%    0%    0%   Ttcptimer
37    8%    1%    0%   ef_res
38    0%    0%    0%   ef_rcv_msg
39    0%    0%    0%   ef_inconsistent_daemon
40    0%    0%    0%   ip6_tunnel_rcv_pkt
41    0%    0%    0%   res6t
42    0%    0%    0%   tunrt6
43    0%    0%    0%   ef6_rcv_msg
44    0%    0%    0%   ef6_inconsistent_daemon
45    0%    0%    0%   imid
46    0%    0%    0%   nsmd
47    0%    0%    0%   ripd
```

```
48    0%    0%    0%   ripngd
49    0%    0%    0%   ospfd
50    0%    0%    0%   ospf6d
51    0%    0%    0%   bgpd
52    0%    0%    0%   pimd
53    0%    0%    0%   pim6d
54    0%    0%    0%   pdmd
55    0%    0%    0%   dvmrpd
56    0%    0%    0%   vty_connect
57    0%    0%    0%   aaa_task
58    0%    0%    0%   Tlogtrap
59    0%    0%    0%   dhcp6c
60    0%    0%    0%   sntp_recv_task
61    0%    0%    0%   ntp_task
62    0%    0%    0%   sla_deamon
63    0%    3%    1%   track_daemon
64    0%    0%    0%   pbr_guard
65    0%    0%    0%   vrrpd
66    0%    0%    0%   psnpd
67    0%    0%    0%   igsnpd
68    0%    0%    0%   coa_recv
69    0%    0%    0%   co_oper
70    0%    0%    0%   co_mac
71    0%    0%    0%   radius_task
72    0%    0%    0%   tac+_acct_task
73    0%    0%    0%   tac+_task
74    0%    0%    0%   dhcpd_task
75    0%    0%    0%   dhcps_task
76    0%    0%    0%   dhcpping_task
77    0%    0%    0%   dhcpc_task
78    0%    0%    0%   uart_debug_file_task
79    0%    0%    0%   ssp_init_task
80    0%    0%    0%   rl_listen
81    0%    0%    0%   ikl_msg_operate_thread
82    0%    0%    0%   bcmDPC
83    0%    0%    0%   bcmL2X.0
84    3%    3%    3%   bcmL2X.0
85    0%    0%    0%   bcmCNTR.0
86    0%    0%    0%   bcmTX
87    0%    0%    0%   bcmXGS3AsyncTX
88    0%    2%    1%   bcmLINK.0
89    0%    0%    0%   bcmRX
90    0%    0%    0%   mngpkt_rcv_thread
```

```
 91     0%     0%     0%    mngpkt_recycle_thread
 92     0%     0%     0%    stack_task
 93     0%     0%     0%    stack_disc_task
 94     0%     0%     0%    redun_sync_task
 95     0%     0%     0%    conf_dispatch_task
 96     0%     0%     0%    devprob_task
 97     0%     0%     0%    rdp_snd_thread
 98     0%     0%     0%    rdp_rcv_thread
 99     0%     0%     0%    rdp_slot_change_thread
100     4%     2%     1%    datapkt_rcv_thread
101     0%     0%     0%    keepalive_link_notify
102     0%     0%     0%    rerp_msg_recv_thread
103     0%     0%     0%    ip_scan_guard_task
104     0%     0%     0%    ssp_ipmc_hit_task
105     0%     0%     0%    ssp_ipmc_trap_task
106     0%     0%     0%    hw_err_snd_task
107     0%     0%     0%    rerp_packet_send_task
108     0%     0%     0%    idle_vlan_proc_thread
109     0%     0%     0%    cmic_pause_detect
110     1%     1%     1%    stat_get_and_send
111     0%     1%     0%    rl_con
112    75%    80%    90%    idle
```

In the list above, the first 3 lines indicates the system CPU utilization in 5sec, 1min and 5min, including LISR, HISR and task. Then, it describes the detailed CPU utilization distribution:

- No：Sequence number
- 5Sec：CPU utilization of the tasks in 5sec.
- 1Min：CPU utilization of the tasks in 1min.
- 5Min：CPU utilization of the tasks in 5min.

The first 2 lines in the list above indicate the CPU utilization of all LISRs and HISRs. From the 3rd line, it begins to refer to the CPU utilization of the tasks. The last line refers to the CPU utilization of the idle task, which is the same as the "System Idle Porcess" in the Windows. In the example above, CPU utilization of idle task within 5s is 75%, indicating that 75% CPU is idle.

65.1.2 cpu-log

Use this command to configure the low and high threshold of the cpu log utilization limit manually.

cpu-log *log-limit low_num high_num*

Parameter description

Parameter	Description
log-limit	The command descriptor prompting the log limit.
low_num	Set the low threshold of the cpu log utilization limit.
high_num	Set the high threshold of the cpu log utilization limit.

Default

By default, the high and low threshold of the cpu log utilization limit are 100% and 90%.

Command mode

Global configuration mode.

Usage guidelines

Use this command to configure the low and high threshold of the cpu log utilization limit manually. When the CPU using rate is more than the high threshold, it prompts the message; but if the CPU using rate exceeds the high threshold continuously, it only prompts the message for one time. When the CPU using rate is less than the low threshold, it prompts the message and advertises that the current CPU using rate has been down only when the CPU high and low threshold switches over.

Examples

This example shows how to set the low and high threshold of the cpu log utilization limit to 70% and 80% respectively.

```
DES-7210(config)# cpu-log log-limit 70 80
```

The console prompts as follows when the CPU utilization rate is more than 80%:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one
```

```
minute : 95% , Using most cpu's task is ktimer : 94%
```

The console prompts as follows when the CPU utilization rate is less than 70%:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU

utilization in one minute :68% , Using most cpu's task

is ktimer : 60%

Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: The CPU

using rate has down!
```

66 Syslog Configuration Commands

66.1 Related Configuration Commands

66.1.1 logging on

Use this command to record logs on different devices. The **no** form of this command disables the fucntion.

logging on

no logging on

Parameter description	N/A
Default configuration	Logs are allowed to be displayed on different devices.
Command mode	Global configuration mode.
Usage guidelines	DES-7200 can not only show the log information in the Console window and VTY window, but also record it in different equipments such as the memory buffer, the FLASH and Syslog Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is greater than 1.
Examples	The following example disables the log switch in the equipment. `DES-7210(config)# no logging on`

Related commands

Command	Description
logging buffered	Record the logs to an internal buffer.

logging	Record logs to the Syslog server.
logging file flash:	Record logs on the FLASH.
logging console	Set the log level to be displayed on the console.
logging monitor	Set the log level to be displayed on the VTY window (such as telnet window) .
logging trap	Set the log level to be sent to the Syslog server.

66.1.2 terminal monitor

Use this command to show logs on the current VTY. The **no** form of this command is used to disable the function.

terminal monitor

terminal no monitor

Default configuration	By default, no logs are displayed on the VTY window.
Command mode	Privileged EXEC mode.
Usage guidelines	This command only sets the temporary attributes of the current VTY. As the temporary attribute, it is not stored permanently. At the end of the VTY terminal session, the system will use the default setting, and the temporary setting is lost.

Note For easy management, the DES-7200 allows the use the command on the console. The **no** form of the command executed on the console allows only the emergent log messages with severities 0 and 1.

Examples

The example below allows log information to be printed on the current VTY window.

```
DES-7210# terminal monitor
DES-7210#
```

66.1.3 logging buffered

Use this command to set the memory buffer parameters (log severity, buffer size) for logs. The **no** form of the command disables recording logs in memory buffer.

logging buffered [*buffer-size* | *level*]

no logging buffered

Parameter description

Parameter	Description
buffer-size	Size of the buffer, 4K to 128K bytes
levell	Severity of logs, 0 to 7. The name of the severity or the numeral can be used.

Default configuration

The default buffer size is 4k bytes.

The log severity is 7.

Command mode

Global configuration mode.

Usage guidelines

The memory buffer for log is used in recycled manner. That is, when it is full, the oldest information will be overwritten. To show the log information in the memory buffer, run **show logging** at the privileged user level.

The logs in the memory buffer are temporary, and will be cleared in case of device restart or the execution of command **clear logging** by privileged user. To trace a problem, it is required to record logs in flash or send them to Syslog Server.

The log information of the DES-7200 is classified into the following 8 levels:

Table-1

Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy
Critical	2	Critical conditions
Errors	3	Error message
warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
informational	6	Descriptive information
Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level.

When the level of log information to be displayed on specified device, the log information is at or below the set level will not be displayed.

Examples

The configuration example below allows logs at and below severity 6 to be recorded in the memory buffer sized 10,000 bytes.

```
DES-7210(config)# logging buffered 10000 6
```

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs in the buffer.
clear logging	Clear the logs in the log buffer.

66.1.4 Logging server

Use this command to record the logs in the specified Syslog Sever. The **no** form of the command disables the function.

logging server {*ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address*}

no logging server {*ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address*}

Parameter description

Parameter	Description
ip-address	Receive IP address of the log server.
vrf vrf-name	Specify VRF (VPN device forwarding list) connecting to the log server.
ipv6 ipv6-address	Specify IPV6 address of the log server.

Default configuration

By default, it does not send the logs to any syslog server.

Command mode

Global configuration mode.

Usage guidelines

This command specifies a Syslog server to receive the logs of the device. The DES-7200 allows the configuration of up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time.

Examples

The example below specifies a syslog server at address 202.101.11.1:

```
DES-7210(config)# logging server 202.101.11.1
```

The example below specifies an ipv6 address as AAAA:BBBB:FFFF:

```
DES-7210(config)# logging server ipv6 AAAA:BBBB:FFFF
```

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs in the buffer.
logging trap	Set the level of logs to be sent to Syslog server.

66.1.5 logging file flash

Use this command to record logs in the flash. The **no** format of the command disables the function.

logging file flash:*filename* [*max-file-size*] [*level*]

no logging file

Parameter description

Parameter	Description
filename	Name of the log file of txt type
max-file-size	Maximal size of the log file in the range 128K to 6M bytes, 128K bytes by default
level	The severity of logs recorded in the log files. The name of the severity or the numeral can be used. By default, the severity of logs recorded in the FLASH is 6. For the details of log severity, please see Table-1.

Default configuration

Logs are not recorded in the FLASH.

Command mode

Global configuration mode.

Usage guidelines

If no **Syslog Server** is specified or it is not desired to transfer logs in the network due to the consideration of security purpose, it is possible to save the logs directly in flash.

The extension of the log file is fixed as txt. Any configuration of extension for the filename will be refused.

Caution

Each syslog file has the limitation of the maximum length. Before writing a new syslog to a file, the followings help determine whether the maximum length of the file has been exceeded:

A new syslog file will be created if the maximum length has been exceeded;

Add a number to the name of the new file based on the original filename, in the format of filename_number with the suffix txt.

The maximum number is 15. The first file will be overwritten if the number reaches 15. Therefore, up to 16 files will be generated in the FLASH when configuring the command to write one syslog to the FLASH.

Examples

The example below records the logs in flash, with the name trace.txt, file size 64K and log severity 6.

```
DES-7210(config)# logging file flash:trace
```

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.
more flash	View the logs in the flash.

66.1.6 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console. The **no** format of the command restores it to the default value.

logging console *level*

no logging console

Parameter description

Parameter	Description
level	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 60-1.

Default configuration

Debugging (7).

Command mode

Global configuration mode.

Usage guidelines

When a log severity is set here, the log messages at or below that severity will be displayed on the console.

The **show logging** command displays the related setting parameters and statistics of the log.

Examples

The example below sets the severity of log that is allowed to be displayed on the console as 6:

```
DES-7210(config)# logging console informational
```

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.

66.1.7 logging monitor

Use this command to set the severity of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.). The **no** format of the command restores it to the default value.

logging monitor *level*

no logging monitor

Parameter description

Parameter	Description
level	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 60- 1.

Default configuration	Debugging (7).
Command mode	Global configuration mode.
Usage guidelines	To print log messages on the VTY window, execute first the privileged user command **terminal monitor**. The level of logs to be displayed is defined with **logging monitor**. The log level defined with "Logging monitor" is for all VTY windows.
Examples	The example below sets the severity of log that is allowed to be printed on the VTY window as 6: `DES-7210(config)# logging monitor informational`

Related commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.

66.1.8 logging trap

Use this command to set the severity of logs that are allowed to be sent to the syslog server. The **no** format of the command restores it to the default value.

logging trap *level*

no logging trap

Parameter description

Parameter	Description
level	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 60-1.

Default configuration	Informational(6).
Command mode	Global configuration mode.

Usage guidelines

To send logs to the Syslog Server, execute first the global configuration command **logging** to configure the **Syslog Server**. Then, execute **logging trap** to specify the severity of logs to be sent.

The **show logging** command displays the related setting parameters and statistics of the log.

Examples

The example below enables logs at severity 6 to be sent to the Syslog Server at address 202.101.11.22:

```
DES-7210(config)# logging 202.101.11.22
DES-7210(config)# logging trap informational
```

Related commands

Command	Description
logging on	Reocrd logs on different devicds.
logging	Record logs to the Syslog server.
show logging	Show the logs and related log configuration parameters in the buffer.

66.1.9 logging source interface

Use this command to configure the source interface of logs. The **no** format of the command restores it to the default value.

logging source interface *interface-type interface-number*

no logging source interface

Parameter description

Parameter	Description
interface-type	The type of interface
interface-number	The number of interface

Default configuration

N/A.

Command mode

Global configuration mode.

Usage guidelines	By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique addresses.
Examples	The example below specifies loopback 0 as the source address of the syslog messages: `DES-7210(config)# logging source interface loopback 0`

Related commands

Command	Description
logging	Record logs to the Syslog server.

66.1.10 logging source ip| ipv6

Use this command to configure the source IP address of logs. The **no** format of the command restores it to the default value.

logging source {**ip** *ip-address* **| ipv6** *ipv6-address*}

no logging source {**ip | ipv6**}

Parameter description

Parameter	Description
ip-address	Specify the source IPV4 address sending the logs to IPV4 log server.
ipv6-address	Specify the source IPV6 address sending the logs to IPV6 log server.

Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique addresses.

Examples

The example below specifies loopback 0 as the source address of the syslog messages:

```
DES-7210(config)# logging source ip 192.168.1.1
```

Related commands

Command	Description
logging	Record logs to the Syslog server.

66.1.11 logging facility

Use this command to configure the log device. The **no** format of the command restores it to the default device value (23).

logging facility *facility-type*

no logging facility

Parameter description

Parameter	Description
facility-type	Syslog device value

Default configuration

Local7(23).

Command mode

Global configuration mode.

Usage guidelines

The following table (Table 56-2) is the possible device value of Syslog:

Numerical Code	Facility
0	**kernel messages**
1	**user-level messages**
2	**mail system**
3	**system daemons**
4	**security/authorization messages**
5	**messages generated internally by syslogd**
6	**line printer subsystem**
7	**network news subsystem**

8	**UUCP subsystem**
9	**clock daemon**
10	**security/authorization messages**
11	**FTP daemon**
12	**NTP subsystem**
13	**log audit**
14	**log alert**
15	**clock daemon**
16	**local use 0 (local0)**
17	**local use 1 (local1)**
18	**local use 2 (local2)**
19	**local use 3 (local3)**
20	**local use 4 (local4)**
21	**local use 5 (local5)**
22	**local use 6 (local6)**
23	**local use 7 (local7)**

The default device value of DES-7200 is 23 (local 7).

Examples

Following is to set the device value of **Syslog** as **kernel**:

```
DES-7210(config)# logging facility kern
```

Related commands

Command	Description
logging console	Set the severity of logs that are allowed to be displayed on the console.

66.1.12 logging count

Use this command to enable the log statistics function. The **no** format of the command deletes the log statistics and disables the statistics function.

logging count

no logging count

Parameter description

N/A.

Default configuration

Disabled.

Command mode	Global configuration mode.
Usage guidelines	This command enables the log statistics function. The statistics begins when the function is enabled. If you run **no logging count**, the statistics function is disabled and the statistics data is deleted.
Examples	Enable the log statistics function: `DES-7210(config)# logging count`

Related commands

Command	Description
show logging count	Show the log statistics.
show logging	Show the logs in the buffer.

66.1.13 logging rate-limit

Use this command to enable log rate limit function to limit the output logs in a second in the global configuration mode. The **no** form of this command disables log rate limit function.

logging rate-limit {*number* | *all number* | *console* {*number* | **all** *number*}} [*except severity*]

no logging rate-limit

Parameter description

Parameter	Description
number	The number of logs processed in a second with the range from 1 to 10000.
all	Set rate limit to all the logs with severity level 0-7.
console	Set the amount of logs shown in the console in a second.
except	By default, the severity level is error(3). The rate of the log whose severity level is less than or equal to error(3) is not controlled.
severity	Log severity level with the range from 0 to 7. The lower the level is, the higher the severity is.

Default configuration	Disabled.

Command mode	Global configuration mode.
Usage guidelines	Use this command to control the syslog outpt to prevent the massive log output.
Examples	The example below sets the number of the logs (including debug) processed in a second as 10. However, the logs with warning or higher severity level are not controlled: `DES-7210(config)#logging rate-limit all 10 except warnings`

Related commands

Command	Description
show logging count	Show the log statistics.
show logging	Show the logs in the buffer.

66.1.14 logging synchronous

Use this command to enable synchronization function of user input and log output in the line configuration mode to prevent the user from interrupting when keying in the characters. The **no** form of this command disables this function.

logging synchronous

no logging synchronous

Parameter description	N/A.
Default configuration	Disabled.
Command mode	Line configuration mode.
Usage guidelines	This command enables synchronization function of user input and log output, preventing the user from interrupting when keying in the characters.

Examples	DES-7210(config)# DES-7210(config)#**line console** *0* DES-7210(config-line)#logging synchronous Print UP-DOWN logs on the port when keying in the command, the input command will be output again: DES-7210#configure terminal Oct 9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to down Oct 9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to DOWN DES-7210#configue terminal ----the input command by the user is output again rather than being intererupted.

Related commands	**Command**	**Description**
	show running-config	View the configuration.

66.1.15 service sequence-numbers

Use this command to attach sequential numbers into the logs. The **no** format of the command removes the sequential numbers in the logs.

service sequence-numbers

no service sequence-numbers

Parameter description	N/A.
Default configuration	N/A.
Command mode	Global configuration mode.
Usage guidelines	In addition to the timestamp, it is possible to add sequential numbers to the logs, numbering from 1. Then, it is clearly known whether the logs are lost or not and their sequence.

Examples

The example below adds sequential numbers to the logs.

```
DES-7210(config)#  service sequence-numbers
```

Related commands

Command	Description
logging on	Record logs on different devices.
service timestamps	Attach the timestamp to the logs

66.1.16 service timestamps

Use this command to attach timestamp into logs. The **no** format of the command removes the timestamp from the logs.

service timestamps *message-type* [*uptime* | *datetime* | *msec* | *year*]

no service timestamps *message-type*

default service timestamps *message-type*

Parameter description

Parameter	Description
message-type	The type of log, including **Log** and **Debug**. The **log** type means the log information with severity levels of 0 to 6. The **debug** type means that with severity level 7.
uptime	Device start time in the format of *Day*Hour*Minute*Second, for example, 07:00:10:41
datetime	Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07
msec	Current time of the device in the format of Month*Date*Hour*Minute*Second*milisecond, for example, Jul 27 16:53:07.299
year	Current time of the device in the format of Year*Month*Date*Hour*Minute*Second, for example, 2007 Jul 27 16:53:07

Default configuration

The time stamp in the log information is the current time of the device. If the device has no RTC, the time stamp is automatically set to the device start time.

Command mode	Global configuration mode.
Usage guidelines	When the uptime option is used, the time format is the running period from the last start of the device to the present time, in seconds. When the datetime option is used, the time format is the date of the current device, in the format of YY-MM-DD, HH:MM:SS.

Examples	The example below enables the timestamp for **log** and **debug** information, in format of Datetime, supporting milisecond display.
	`DES-7210(config)# service timestamps debug datetime msec`
	`DES-7210(config)# service timestamps log datetime msec`
	`DES-7210(config)# end`
	`DES-7210(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I: configured from console by console`

Related commands

Command	Description
logging on	Record logs on different devices.
service sequence-numbers	Attach sequential number to logs.

66.1.17 service sysname

Use this command to attach system name to logs. The **no** format of the command removes the system name from the logs.

service sysname

no service sysname

Parameter description	N/A.
Default configuration	N/A.
Command mode	Global configuration mode.
Usage	This command allows you to decide whether to add system name in

guidelines	the log information.

Examples

Add system name in the log information:

```
Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console
DES-7210 #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210 (config)#service sysname
DES-7210 (config)#end
DES-7210 #
```

Mar 22 15:35:57 S3250 %SYS-5-CONFIG: Configured from console by console

Related commands

Command	Function
show logging	Show the logs in the buffer.

66.1.18 more flash

Use this command to show the contents of the logs stored in the FLASH.

more flash:*filename*

Parameter description

Parameter	Description
filename	Log file name

Command mode	Privileged EXEC mode.
Usage guidelines	In the FLASH, the log file means the files with the prefix "//f2/", "//f3/'. This command only allows you to view the log files. You cannot use this command to view other non-log files.

Examples

The following example shows the results of the log files in the FLASH as you can see:

```
DES-7210# more  flash://f2/log.txt
look up  file in the extended flash://f2/log.txt
```

00004 2004-11-17 4:1:32 DES-7210: %5:Reload requested by Administrator. Reload Reason :Reload command

Related commands	**Command**	**Function**
	logging file flash	Record the logs to the FLASH.

66.1.19 clear logging

Use this command to clear the logs from the buffer.

clear logging

Command mode	Privileged EXEC mode.
Usage guidelines	This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.
Examples	The following example clears the log packets from the memory buffer. `DES-7210# clear logging`

Related commands	**Command**	**Function**
	logging on	Record logs on different devices.
	show logging	Show the logs in the buffer.
	logging buffered	Record the logs to the memory buffer.

66.2 Showing Related Command

66.2.1 show logging

Use this command to show the logs in the buffer.

show logging

Parameter description	N/A.
Command mode	Privileged EXEC mode.

Usage guidelines

In the extended FLASH, the log file means the files with the prefix "//f2/", "//f3/'. This command only allows you to view the log files. You cannot use this command to view other non-log files.

Examples

The following command shows the result of the show logging command:

```
DES-7210# show logging
Syslog logging: enabled
Console logging: level debugging, 4 messages logged
Monitor logging: level informational, 0 messages logged
Buffer logging: level debugging, 6 messages logged
Timestamp debug messages: datetime
Timestamp log messages: disabled
Sequence log messages: enable
Trap logging: level debugging, 2 message lines logged,0 reserved,0 fail
logging to  202.101.11.22
logging to  192.168.200.112
Log Buffer (Total 4096 Bytes) : have written 680
00001  2004-11-17  10:20:59   DES-7210:  %7:%LINK  CHANGED:  Interface
FastEthernet 0/0, changed state to up
00002 2004-11-17 10:20:59  DES-7210: %7:%LINE PROTOCOL CHANGE: Interface
FastEthernet 0/0, changed state to UP
00003  2004-11-17  10:57:18   DES-7210:  %7:%LINK  CHANGED:  Interface
FastEthernet 0/1, changed state to administratively down
00004  2004-11-17  10:57:21   DES-7210:  %7:%LINK  CHANGED:  Interface
FastEthernet 0/1, changed state to down
00005  2004-11-17  10:57:41   DES-7210:  %7:%LINK  CHANGED:  Interface
FastEthernet 0/1, changed state to administratively down
00006  2004-11-17  10:57:43   DES-7210:  %7:%LINK  CHANGED:  Interface
FastEthernet 0/1, changed state to down
```

The log messages are described as below:

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics
Timestamp debug messages	Timestamp format of the Debug

	messages
Timestamp log messages	Timestamp format of the Log messages
Sequence log messages	Sequence flag
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

Related commands	Command	Function
	logging on	Record logs on different devices.
	clear logging	Clear the logs in the buffer.

66.2.2 show logging count

Use this command to show the log statistics.

show logging count

Parameter description

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

To use the log packet statistics function, run **logging count** in the global configuration mode. The **show logging count** can show the information of a log, occurrence times, and the last occurrence time.

You can use **show logging** to check whether the log statistics function is enable.

Examples

The following is the execution result of **show logging count**:

```
DES-7210# show logging count
Module Name   Message Name Sev Occur     Last Time
-------------------------------------------------------------
SYS          CONFIG_I        5   1        Jul 6 10:29:57
-------------------------------------------------------------
SYS TOTAL                        1
```

Related commands

Command	Function
logging count	Enable the log statistics function.
show logging	Show the logs in the buffer.
clear logging	Clear the logs in the buffer.

67 Module Hot-plugging/ unplugging Configuration Commands

67.1 Related Configuration Commands

The module hot-plugging/unplugging involves the following Related Commands:

- **install** *slot-num moduletype*
- **no install** *slot-num*
- **remove configure module** *slot-num*
- **show version module detail**
- **show version slots**
- **reset module** *slot-num*

67.1.1 install slot-num moduletype

Use this command to install the module manually.

install *slot-num moduletype*

Parameter description

Parameter	Description
slot-num	Slot number.
moduletype	Module type

Command mode

Global configuration mode.

Usage guidelines

This command is used to install the module driver manually. After the installation, all configurations for the slot will be done for the type of the installed module. Even if the module is unplugged, you can still configure it without loss of the configuration.

Examples

Install module 24SFP/12GT in slot 2

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# install 2 24SFP/12GT
2006-04-22 09:26:00  @5-CONFIG:Configured from outband
DES-7210(config)# end
DES-7210# show version module detail 2
Device  : 1
Slot    : 2
User Status  : installed
Software Status: none
Online Module :
Type  :
Ports   : 0
Version :
Configured Module :
Type  : M8606-24SFP/12GT
Ports   : 24
Version :
DES-7210#
```

Related commands

Command	Description
no install slot-num	Uninstall the module in the slot.
show version module detail	Show the detailed information of a module.
show version slots	Show slot details

67.1.2 no install slot-num

Use this command to unistall the module manually.

no install *slot-num*

Parameter description

Parameter	Description
slot-num	Slot number.

Command mode

Global configuration mode.

Usage guidelines

Use this command to uninstall a module. Once uninstalled, all configurations for that module will be lost and the module will be deactivated, unless you manually install the driver for the module.

Examples

Uninstall module 24SFP/12GT in slot 2

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# no install 2
2006-04-22 09:26:00  @5-CONFIG:Configured from outband
DES-7210(config)#end
DES-7210# show version module detail 2
Device  : 1
Slot    : 2
User Status  : none
Software Status: none
Online Module :
Type  :
Ports   : 0
Version :
Configured Module :
Type  :
Ports   :
Version :
DES-7210#
```

Related commands

Command	Description
install slot-num *moduletype*	Install a module in the slot.
show version slots	Show slot details.

67.1.3 remove configuration module slot-num

Use this command to remove the module configurations.

remove configuration module *slot-num*

Parameter description

Parameter	Description
slot-num	Slot number.

Command mode

Global configuration mode.

Usage guidelines

Use this command to remove the module configurations.

Examples

```
DES-7210(config)# remove configure module 4
```

67.1.4 reset module slot-num

Use this command to reset a module.

reset module *slot-num*

Parameter description

Parameter	Description
slot-num	Slot number.

Command mode

Privileged EXEC mode

Examples

```
DES-7210# reset module 4
```

67.2 Showing Related Command

67.2.1 show version module detail [module-num]

Use this command to show the details of the module.

show version module detail [*module-num*]

Parameter description

Parameter	Description
module-num	(Optional) Module number.

Command mode

Privileged EXEC mode.

Examples

```
DES-7210# show version module detail 2
Device  : 1
Slot    : 2
User Status :    none
Software Status: none
Online Module :
Type  :
Ports   : 0
Version :
Configured Module :
Type  :
Ports   :
Version :
```

```
DES-7210#
```

Related commands

Command	Description
show version slots	Show slot details.

67.2.2 show version slots [slot-num]

Use this command to view the details of the slot.

show version slots [*slot-num*]

Parameter description

Parameter	Description
num	(Optional) Slot number.

Command mode

Privileged EXEC mode.

Examples

```
DES-7210# show version slots
Dev Slot  Configured Module Online Module  User Status   Software
Status
--- ----  -----------------   -----  --------------
1 1    none         none
1 2 M8606-24SFP/12GT M8606-24SFP/12GT installed none
1 3 M8606-2XFP M8606-2XFP uninstalled  cannot startup
1 4 M8606-24GT/12SFP M8606-24GT/12SFP installed ok
1 M1 M8606-CM   M8606-CM              master
1   M2                                 none
```

Related commands

Command	Description
show version moduel detail	Show the details of the module.

68 LCD Configuration Commands

68.1 Related Configuration Commands

The LCD configuration commands include:

- **lcd trap-number** *num*
- **memory-rate rising-threshold** *num*

68.1.1 lcd trap-number num

Use this command to configure the length of alarm messages. Use the **no** form of this command to restore the default value.

lcd trap-number *num*

no lcd rap-number

Parameter description

Parameter	Description
num	An integer in the range of 1 to1000.

Default configuration

The default value is 100.

Command mode

Global configuration mode

Usage guidelines

Use this command to view the recently generated alarms. By default, 100 latest alarms are displayed. You can use this command to change the number of the latest alarms displayed.

Examples

The following example shows 200 latest alarms.

```
lcd trap-num 200
```

68.1.2 memory-rate rising-threshold num

Use this command to set the value of memory-rate rising-threshold.

memory-rate rising-threshold *num*

Parameter description

Parameter	Description
num	An integer in the range of 1 to 100.

Default configuration

The default value is 80.

Command mode

Global configuration mode.

Usage guidelines

If the num is 80, the result of show running-config does not show the memory-rate rising-threshold *80.*

Examples

```
DES-7210(config)# memory-rate rising-threshold 60
```

69 USB configuration Commands

69.1 Related Configuration Commands

The commands described here are used to query and remove USB devices in the CLI environment in the main program.

- View USB device information: **show usb** command
- Remove a USB device: **usb remove** command

69.1.1 show usb

Use this command to show the information about the inserted USB device in the system.

show usb

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	Device information is displayed if there is a USB device. Otherwise, there is no output.

Examples	The following example shows the information about the USB device:
	`DES-7210# sh usb`
	`Device: USB Mass Storage Device :`
	`ID : 778`
	`Lun 0:`
	`ID : 0`
	`Disk Partitions:`
	`1: /dev/uba/disc0/part1 --> /mnt/uba`
	`size : 131072000B(125MB)`
	The meaning of the information is as below:

USB Mass Storage Device: Name of the device

ID: The ID number of the device. (Useful when removing it)

Lun: A logical unit number of the device, and the following ID is the ID of the logical unit.

Disk Partitions: the partition information of the device. As shown in the above output, this device has one partition, and the partition file is **/dev/uba/disc0/part1**, which is mounted to the directory **/mnt/uba**. You can use the file system command **cd /mnt/uba** to go to this directory and perform operations on the contents in this partition.

69.1.2 usb remove

usb remove *device_ID*

Parameter description

Parameter	Description
device_ID	Device ID of USB to be removed.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Before pulling out the USB device, you need to remove the device using a command, so as to prevent errors that may occur because the system is using the device. If the device is removed successfully, the system will show a prompt, when you can pull out the device. If the device cannot be pulled out, it indicates that the system is using this USB device, so you have to wait a moment before removing it again.

Examples

The following example demonstrates how to remove the USB device mentioned in the example in the previous section.

```
DES-7210# usb remove 778
OK, now you can pull out the device 778.
0:1:1:38 DES-7210: USB-5-USB_DISK_REMOVED: USB Device <USB Mass Storage Device> Removed!
```

At this moment, the usb device can be plugged out.

70 POE Management Configuration Commands

70.1 Configurtion Related Command

POE configuration management includes the following related commands:

- **poe enable**
- **poe-power lower lower**
- **poe-power upeer upeer**
- **poe disconnect-mode mode**

70.1.1 poe enable

Use this command to enable the POE(Power-over-Ethernet) function on the interface. Use the **no** form of this command to disable this function.

poe enable

no poe enable

Command mode	Interface configuration mode.
Examples	`DES-7210(config-if)# poe enable` `DES-7210(config-if)# no poe enable`

70.1.2 poe-power lower lower

Use this command to the minimum allowed voltage. Use the **no** form of this command to restore to the default value.

poe-power lower *lower*

no poe-power lower

Parameter description

Parameter	Description
lower	Minimum allowed voltage, within the range [45000 to 47000] mv.

Command mode

Global configuration mode.

Examples

The following example sets the minimum allowed voltage of the current POE system as 46000 mv.

```
DES-7210# configure
DES-7210(config)# poe-power lower 46000
DES-7210(config)# end
```

70.1.3 poe-power upeer upper

Use this command to the maximum allowed voltage. Use the **no** form of this command to restore to the default value.

poe-power upper *upper*

no poe-power upper

Parameter description

Parameter	Description
upper	Maximum allowed voltage, within the range [55000 to 57000] mv.

Command mode

Global configuration mode。

Examples

The following example sets the maximum allowed voltage of the current POE system as 56000 mv.

```
DES-7210# configure
DES-7210(config)# poe-power upeer 56000
DES-7210(config)# end
```

70.1.4 poe disconnect-mode mode

Use this command to set the disconnection detection mode. Use the **no** form of this command to restore to the default value.

poe disconnect-mode *mode*

no poe disconnect-mode

Parameter description

Parameter	Description
mode	Disconnection detection mode, within the range of [ac/dc]

Command mode

Global configuration mode.

Examples

Set the disconnect detection mode of the current POE system as **dc**:

```
DES-7210# configure
DES-7210(config)# poe disconnect-mode dc
DES-7210(config)# end
```

70.2 Show Related Command

There are the following POE showing commands:

- **show poe interfaces**
- **show poe powersupply**

70.2.1 show poe interfaces

Use this command to view the POE status on the interface.

show poe interfaces *interface-id*

Command mode

Privileged EXEC mode.

Examples

```
DES-7210# show poe interface gigabitethernet 0/2
Interface : Gi0/2
Port power enabled : ENABLE
Port connect status : OFF
```

```
Port PD Class : no PD devices
Port max power : 15400 mW
Port current power : 0 mW
Port peak power : 0 mW
Port current : 0 mA
Port voltage : 48082 mV
Port trouble cause : normal
```

70.2.2 show poe powersupply

Use this command to view the POE power supply status.

show poe powersupply

Command mode	Privileged EXEC mode.

Examples

```
DES-7210# show poe powersupply
PSE Total Power : 379971 mW
PSE Total Power Consumption : 0 mW
PSE Available Power : 379971 mW
PSE Peak Value : 0 mW
PSE Min Allow Voltage : 45000 mV
PSE Max Allow Voltage : 57000 mV
PSE Disconnect Sense Mode : ac
```