



ICS5530 Series Layer 3 Industrial Ethernet Switch CLI User Manual

Version 01

Issue Date: 10/22/2020

Copyright © 2020 3onedata Co., Ltd. All rights reserved.

For this manual, all rights reserved by 3onedata Co., Ltd. No company or individual is allowed to duplicate or translate this manual in any forms without written permission issued by 3onedata Co., Ltd.

Trademark statement

3onedata, **3onedata** and  are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Notes

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.



Please scan our QR code
for more details

3onedata
Make network communication more reliable



BlueEyes pro



Embedded Industrial
Ethernet Switch Modules

Embedded Serial
Device Server Modules



Industry-specialized
Products
(Rail Transit, Power,
Smart City, Pipe Gallery...)

Honor · Quality · Service



Layer 2 (Unmanaged)
Managed Industrial
Ethernet Switch

Layer 3 Managed
Industrial Ethernet Switch
Industrial PoE Switch



BlueEyes Pro
Management Software

VSP Virtual Serial Port
Management Software

SNMP Management
Software



Modbus Gateway

Serial Device Server

Media Converter

CAN Device Server

Interface Converter



Industrial Wireless
Products

3onedata Co., Ltd.

Headquart 3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District,

Technolog tech-support@3onedata.com

Service +86-400-880-4496

E-mail: sales@3onedata.com

Fax: +86-0755-26703485

Website: <http://www.3onedata.com>

<http://www.3onedata.com>

Preface

Switch CLI user manual has introduced:

- CLI configuration interface login
- CLI configuration rule and method
- Network management functions related CLI introduction

Readers

This manual mainly suits for engineers as follows:

- Network administrator responsible for network configuration and maintenance
- On-site technical support and maintenance staff
- Network Engineer

Text Format Convention

Format	Description
“”	Words with “” represent the interface words. e.g.: "The port number".
>	Multi-level paths are separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: 'Light Blue'.
About this chapter	The section 'about this chapter' provides links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

Icon Convention

Format	Description
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.

Format	Description
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Notes	Make a necessary supplementary instruction for operation description.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

Revision Record

Version NO.	Revision Date	Revision Description
01	10/22/2020	Product release

Content

Preface	1
Content	1
1 Login the Switch Configuration	1
1.1 Login the Switch Function Overview	1
1.2 Login the Switch	1
1.2.1 Login the Switch via Serial Port	1
1.2.2 Login the Switch via Telnet.....	3
1.2.3 Login the Switch via SSH.....	5
1.2.4 Login the Switch via WEB:.....	7
1.2.5 Manage the switch via Network Management Software	8
1.3 Command Line	8
1.3.1 Command Analysis	8
1.3.2 Command Line Mode.....	8
1.3.3 Shortcut Key.....	9
1.4 Common Command.....	10
1.4.1 Password Verification	10
1.4.2 Customization display	11
1.4.3 Configuration Management.....	14
1.4.4 System Upgrade.....	14
1.4.5 Debug Mode.....	15
2 User Configuration	16
2.1 Add user.....	16
2.2 Delete User.....	17
2.3 View current online users	18
2.4 Console Login Management	18
2.5 Virtual Terminal Login Management.....	19
2.6 Timeout Logout.....	20
3 Port Configuration.....	21
3.1 Enter port configuration mode.....	21
3.2 Port Rate Limit	22
3.3 Port Settings	23

3.3.1	Combo PortTransmission Media.....	23
3.3.2	Duplex Mode	24
3.3.3	Flow Control.....	25
3.3.4	Max-Frame	25
3.3.5	Interface Switch	26
3.3.6	Rate	27
3.4	Port Isolation	28
3.5	Storm Suppression.....	29
3.6	MAC Address	30
3.6.1	Clear Dynamic MAC address	30
3.6.2	MAC address learning	30
3.6.3	MAC address aging-time	31
3.6.4	Static MAC Address Filtering	32
3.6.5	Multicast MAC Address Filtering.....	33
3.6.6	Display MAC Address Table	34
3.7	Mirror Command	35
3.7.1	Port Mirror Configuration.....	35
3.7.2	Delete Port Mirror	36
3.8	Link Aggregation Configuration.....	36
3.8.1	Dynamic Aggregation System Priority	36
3.8.2	Dynamic Aggregation Port Priority.....	37
3.8.3	Dynamic Aggregation Port Timeout.....	38
3.8.4	Add Dynamic Aggregation Group	38
3.8.5	Add static LACP	39
3.8.6	Link Aggregation Load Balance Mode.....	40
3.8.7	Displays Dynamic Aggregation Group.....	41
3.8.8	Displays Static Aggregation Group.....	41
3.9	Port Statistics	42
3.9.1	Display Port.....	42
4	VLAN Configuration	44
4.1	Enter VLAN Configuration Mode	44
4.2	Add VLAN ID	44
4.3	Port Type.....	45
4.4	Port Default VLAN	46
4.5	Classify VLAN Based on Port.....	47
4.6	Display VLAN Information	48
4.7	Port receive frame type	48
4.8	Port Entry Filtering.....	49
4.9	VLAN Classifier Function.....	50
4.9.1	VLAN Classifier Function Introduction	50
4.9.2	Rule configuration.....	50

4.9.3	Group Configuration	53
4.9.4	Interface Configuration Command.....	54
5	Ring Configuration	55
5.1	Globle Ring Enablement	55
5.2	Create Ring NetworkGroup	56
5.3	Display Ring Network Information.....	57
6	MSTP Configuration.....	59
6.1	Globle Spanning-tree Enablement	59
6.2	Enter MSTP Instance Configuration View	59
6.3	Create MSTP Instance.....	60
6.4	MSTP Revision Level.....	61
6.5	MST Domain Name.....	61
6.6	Device Priority.....	62
6.7	Spanning-tree Protocol Version	63
6.8	Spanning Tree Timer Parameter	64
6.9	The Maximum Hop of Spanning-tree.....	65
6.10	The Rate that the Spanning Tree Sends a BPDU.....	66
6.11	Compatible with Cisco MSTP Mode.....	66
6.12	Global Edge Port BPDU Filtering.....	67
6.13	Global Edge Port BPDU Protection	69
6.14	Port error-disable Timeout Recovery.....	70
6.15	Port error-disable Recovery Interval	71
6.16	Edge	71
6.17	BPDU Filter of Edge Port.....	72
6.18	BPDU Filter of Edge Port.....	73
6.19	Automatical Switching Edge Port.....	74
6.20	Root Port Protection	75
6.21	Port Spanning-tree Enablement	76
6.22	Port Hello-time	76
6.23	Port Connection Type.....	77
6.24	Port Priority	78
6.25	Cost.....	78
6.26	Port Restricted Election.....	79
6.27	Port Restriction TC.....	80
6.28	Display Spanning-tree Detail Information.....	80
6.29	Display the Basic Information of the Spanning Tree	82
7	ERPS Configuration	83
7.1	Enter ERPS Instance Configuration View.....	83
7.2	Create ERPS Instance Name	83
7.3	ConfigureERPS Instance ID	84
7.4	Specify the Ring Instance Corresponding to the ERPS Instance.....	85

7.5	Specify the Timer Instance Corresponding to the ERPS Instance	85
7.6	ERPS Instance Device Role	86
7.7	ERPS Instance Ring Role	87
7.8	Major Instance Name of ERPS Instance	87
7.9	ERPS Instance Protocol Message Management VLAN	88
7.10	ERPS Instance Virtual Channel	89
7.11	ERPS Instance Reverse Mode	89
7.12	ERPS Instance Force-switch or Manual-switch	90
7.13	ERPS Instance Clear Command	91
7.14	ERPS Instance Enablement	91
7.15	Enter Ring Instance Configuration View	92
7.16	Create Ring Instance Name	92
7.17	Ring Instance Interface	93
7.18	Ring Instance Network Level	94
7.19	Enter Timer Instance Configuration View	94
7.20	Create Timer Instance Name	95
7.21	WTB Timer	95
7.22	WTR Timer	96
7.23	GuardTimer	97
7.24	HoldTimer	97
7.25	Display ERPS Instance Information	98
7.26	Display Ring Instance Information	99
7.27	Display Timer Instance Information	100
8	Remote Loop Detection Configuration	101
8.1	Enable configuration	101
8.2	Port Loopback Detection	102
9	IGMP Configuration	103
9.1	IGMP Enablement	103
9.2	IGMP Version	104
9.3	The Times the IGMP Query Started	104
9.4	Start Query Interval of IGMP Querier	105
9.5	The Robustness Factor of IGMP Querier	106
9.6	IGMP Universal Group Query Message Time Interval	106
9.7	IGMP Lifetime of Other Queries	107
9.8	Maximum Response Time of IGMP Universal Group Query Message	108
9.9	The Number of IGMP Query Packets in a Particular Group	109
9.10	Time Interval of IGMP Group Query Message	109
9.11	IGMP Message with RA Option	110
9.12	Fast Aging ACL Group	111
9.13	Illegal Multicast Group	112
9.14	Multicast Group Number Limit	112

9.15	IGMP Message Source Address and Receive Interface Subnet Restrictions.....	114
9.16	Static Multicast	114
9.17	Global IGMP SSM Mapping Enablement	115
9.18	IGMP SSM-Map Static Multicast	116
9.19	Display IGMP Multicast Information.....	117
9.20	Display IGMP Interface Information.....	117
10	IGMP Snooping Configuration	119
10.1	IGMP SnoopingEnablement	119
10.2	IGMP SnoopingQuerier Enablement.....	120
10.3	IGMP Snooping Port Fast-leave Enablement	120
10.4	IGMP SnoopingPort Suppression Enablement.....	121
10.5	Display the IGMP Snooping Multicast Group Routing Interface.....	122
10.6	Display IGMP SnoopingMulticast Statistics.....	122
11	GMRP and MMRP Configuration	124
11.1	GlobalGMRP or MMRP Enablement.....	124
11.2	Port GMRP or MMRP Enablement.....	125
11.3	GMRP or MMRP Registration Mode	126
11.4	GMRP or MMRP Timer	126
11.5	Display GMRP or MMRP Configuration Information	127
11.6	Display GMRP or MMRP State Machine Information.....	128
11.7	Display GMRP or MMRP Message Statistics.....	128
11.8	Display GMRP or MMRP Timer Information	129
12	GVRP and MVRP Configuration	130
12.1	Globe GVRP or MVRP Enablement	130
12.2	GVRP or MVRP Dynamic VLAN Enablement	131
12.3	Port GVRP or MVRP Enablement	132
12.4	GVRP or MVRP Registration Mode	132
12.5	GVRP or MVRP Timer	133
12.6	Display Dynamic VLAN Information	134
12.7	Display GVRP or MVRP Configuration Information	134
12.8	Display GVRP or MVRP State Machine Information.....	135
12.9	Display GVRP or MVRP Message Statistics.....	136
12.10	Display GVRP or MVRP Timer Information.....	136
13	PIM-DM Configuration	137
13.1	PIM-DM Enablement.....	137
13.2	PIM-DM DR Priority.....	138
13.3	PIM-DM GenID Information	138
13.4	PIM-DM Neighbor Reachable State Time	139
13.5	Time Interval of PIM-DM Hello Message	140
13.6	PIM-DM Neighbor Filter.....	140
13.7	IPM-DM SRM Message Enablement.....	141

13.8	Time Interval of Sending PIM-DM SRM Message	142
13.9	Time Interval for PIM-DM to Receive SRM message	143
13.10	Display PIM-DM Interface Information	143
13.11	View the Local Multicast Group Members of PIM-DM	145
13.12	Displays the PIM-DM Multicast Routing Table Entry	145
13.13	Display PIM-DM Neighbor Information	146
13.14	Displays PIM-DM Next Hop Information	146
14	PIM-SM Configuration	148
14.1	PIM-SM Enablement	148
14.2	PIM-SM DR Priority	149
14.3	PIM-SM GenID Information	149
14.4	PIM-SM Neighbor Reachable State Time	150
14.5	Time Interval of PIM-SM Hello Message	151
14.6	PIM-SM Neighbor Filter	151
14.7	PIM-SM Illegal Registration Message Restriction	152
14.8	PIM C-BSR	153
14.9	PIM Registered Message Validation and Compatibility with Cisco Standard	154
14.10	PIM C-RP Compatibility with Cisco Standard	155
14.11	PIM BSR C-RP Priority Ignorance	155
14.12	Time Interval for PIM to Send Joined/Pruned Message	156
14.13	The Rate for the PIM Receive and Process Multicast Service Message	157
14.14	The PIM Checks the Accessibility of the RP	157
14.15	The VLAN Interface or Source IP Address of a PIM that Sends a Registered Message 158	
14.16	PIM Registration Suppression Time	159
14.17	PIM Static PR	160
14.18	PIM C-RP	161
14.19	PIM KAT Timer Aging Time	162
14.20	PIM SPT Switch	162
14.21	Display BRS Running Information of PIM-SM	163
14.22	Display PIM-SM Interface Information	164
14.23	View the local multicast group members of PIM-SM	165
14.24	Displays the PIM-SM Multicast Routing Table Entry	166
14.25	Display PIM-SM Neighbor Information	167
14.26	Display PIM-SM Next Hop Information	168
14.27	Display PIM-SM Information	169
14.28	Display the RP Address of the PIM-SM Multicast Group	169
15	VRRP Configuration	171
15.1	Create VRRP Group and Enter VRRP Configuration View	171
15.2	VRRP Interface Enablement	171
15.3	VRRP virtual IP address	172

15.4	Preemption Mode Enablement	173
15.5	Preemption Delay Time.....	173
15.6	Priority of VRRP Device	174
15.7	VRRP Notification Message Interval	175
15.8	VRRP Message Authentication Mode	176
15.9	Authentication Word of VRRP Message	176
15.10	Configure the Monitoring Specified Interface.....	177
15.11	Track ipdt Session	178
15.12	Enable VRRP Backup Group	179
15.13	Disable VRRP Backup Group	180
15.14	Display VRRP Backup Group Information	180
16	RIP Configuration.....	182
16.1	Enter RIP View	182
16.2	RIP Interface Enablement	182
16.3	Configure IP Address of RIP Neighbor in NBMA Network.....	183
16.4	Add Static RIP Route	184
16.5	Add default Routing to RIP Routing Database.....	185
16.6	Default Route Metric	185
16.7	RIP Route Management Distance	186
16.8	Access List Route Filtering.....	187
16.9	Other Routing Protocols Route Import	187
16.10	Block RIP Broadcast.....	188
16.11	Time of RIP Timer.....	189
16.12	RIP version.....	190
16.13	Maximum number of RIP route	190
16.14	RIP Routing Measures Offset	191
16.15	RIP Route UDP to Receive Cache Size.....	192
16.16	RIP Message Authentication Mode	193
16.17	RIP Message Authentication Key Chain	193
16.18	RIP Message Authentication Password.....	194
16.19	Receive RIP Message enablement.....	195
16.20	Accept Message of Specified RIP Version.....	196
16.21	Send RIP Message Enablement	196
16.22	Send the Message of the Specified RIP Version	197
16.23	RIP Horizontal Split Enablement.....	198
16.24	Display Routing Information learned by RIP.....	198
16.25	Display the Routing Information in the RIP Routing information Base	200
16.26	Display RIP Interface Information	201
17	OSPF Configuration	203
17.1	Enter OSPF Router Configuration View	203
17.2	OSPF Route ID	203

17.3	OSPF Area and Enablement	204
17.4	Configure and Publish a Host Route	205
17.5	Configure Neighbor Interface Address in the NBMA Network	206
17.6	Create Virtual Connection	206
17.7	Routing Within the Aggregation Area.....	207
17.8	Type-3 LSA Filter.....	208
17.9	Stub Area	209
17.10	NSSA Area	210
17.11	Area Shortcut Mode.....	211
17.12	Default Costs for Introduced Default Routes	212
17.13	Configure Aggregation of External Routes and Notify or Suppress	213
17.14	Link Cost Bandwidth Reference Value	214
17.15	Opaque LSA Publishing and Receiving Capabilities	214
17.16	Compatibility with RFC1583	215
17.17	Introduce Default Route	216
17.18	OSPF Routing Default Metric	217
17.19	OSPF Route Management Distance	218
17.20	Ingress Route Information Filter.....	218
17.21	Egress Route Information Filter.....	219
17.22	Introduce Additional Routing Information	220
17.23	Interface Hello Message Control	221
17.24	SPF Timer	221
17.25	The Maximum Number of LSA.....	222
17.26	Maximum Concurrent Number of Current DD Packet.....	223
17.27	Regional OSPF Message Validation	223
17.28	OSPF ABR Type	224
17.29	Interface OSPF Message Validation	225
17.30	Interface OSPF Message Authentication Key	226
17.31	Interface OSPF Cost	227
17.32	Interface LSA Database Filter	228
17.33	Interface OSPF Neighbor Failure Time.....	228
17.34	Time Interval of Sending Hello Message	229
17.35	Interface Retransmission LSA Interval	230
17.36	Interface to LSA Transmission Delay Time	230
17.37	Disable the OSPF Function of the Interface	231
17.38	Interface OSPF MTU Value	232
17.39	Interface DD Exchanges Ignore MTU	232
17.40	Interface OSPF Network Type.....	233
17.41	The DR Priority of the Interface	234
17.42	Display OSPF Route Information	234
17.43	Display OSPF Database Information.....	236

17.44	Display OSPF Neighbor Information	237
18	BGP Configuration	239
18.1	Enter BGP Route Configuration View	239
18.2	Enter the IPv4 or IPv6 Address Family.....	239
18.3	BGP Route Aggregation Address.....	240
18.4	BGP Always Comparison MED Value.....	241
18.5	The BGP optimal Path Ignore the AS-Path Length.....	241
18.6	Comparison of AS-Path Length of BGP Optimum Path	242
18.7	BGP Optimum Path Routing ID Comparison	243
18.8	MED Property of BGP Optimum Path.....	243
18.9	BGP Route Reflection.....	244
18.10	Configure the Group Identifier for the Routing Reflector.....	245
18.11	Configure the Identifier for the AS Alliance	245
18.12	Configure the Member AS for the AS Alliance	246
18.13	EBGP Route Suppression	247
18.14	Set the BGP Address Family to IPv4 Unicast by Default	249
18.15	The Default Local Priority Value for BGP	250
18.16	Compare MED Values of the Same AS Counterparts.....	250
18.17	Force the AS-Path of the First Location to be the EBGp Route.....	251
18.18	Reset the Direct Connection EBGp Fault Interface	252
18.19	Record BGP Status Change Information	252
18.20	BGP Route ID.....	253
18.21	BGP Next Hop Detection Interval.....	253
18.22	Specifies the Management Distance for the Routing Prefix	254
18.23	Managed Distances for Internal/External/Local BGP Routes.....	255
18.24	Exit the BGP IPv4 or IPv6 Address Family	255
18.25	Network Segment Routing Notification BGP Routing Table	256
18.26	Route Synchronization Notify Network Information	257
18.27	Configure BGP Peers/Peer Groups.....	258
18.28	Activate the Specified Peer/Peer Group	258
18.29	The Time Interval between Sending BGP Routing Update Packets	259
18.30	The Number of Occurrences of the Same AS in the Neighbor Route AS List.....	260
18.31	The Time Interval Between Sending the Local Originating BGP Route	261
18.32	The Routing Properties Associated with the Transport Neighbors Remain Unchanged.....	262
18.33	Dynamic Updates and Routing Refreshes with Neighbors	263
18.34	Egress route filter with Neighbor	264
18.35	TCP Connection Collision Detection with Neighbor	265
18.36	Send a Default Route to a Peer/Peer Group.....	265
18.37	Peer/Peer Group Description Information	266
18.38	Filtering Strategy Based on ACL	267
18.39	No Capacity Negotiation when Establishing a Connection	268

18.40	Allows Non-directly Connected Neighbors to Establish EBGp Sessions	269
18.41	Force Direct Contact with Neighbors for Multiple Hop	270
18.42	AS-Path Access List Filtering.....	270
18.43	Configure the Interface to the BGP Peer/Peer Group	271
18.44	Number of Received Peer Prefixes.....	272
18.45	Force Next-hop Addresses as Neighbors	273
18.46	Ignore the Results of Peer Capacity Negotiation	274
18.47	The Peer Connection is Passive	275
18.48	Create a BGP Peer Group	275
18.49	Add a Peer Group Member	276
18.50	TCP Port Number for Communicating with Neighbors.....	277
18.51	Routing Filtering Strategy based on IP Prefix List	277
18.52	BGP Update Message Removes Private AS	278
18.53	Route Mapping Strategy	279
18.54	Route Reflection.....	280
18.55	Router Server	281
18.56	Community Property Transfer	281
18.57	Disable BGP Connection	282
18.58	Store BGP Original Routing Information	283
18.59	Strict Ability Matching Connection.....	284
18.60	BGP Session Timer with the Specified Peer	285
18.61	Unsuppress the Routing Map	286
18.62	Specify the BGP Connection Interface	286
18.63	Configure the BGP Version of the Peer.....	287
18.64	Configure the Weight Value of the Peer	288
18.65	Introduce Additional Routing Information to the BGP	289
18.66	BGP Connection Survival Interval and Holdtime	289
18.67	Display BGP Route Information	290
18.68	Display BGP IPv4 Unicast Route Information.....	293
18.69	Display BGP Summary Information.....	295
19	IPv6 Configuration	299
19.1	Create Layer 3 Interface	299
19.2	IPv6 address:.....	299
19.3	Static IPv6Route	300
19.4	Configure RA message related parameters	300
19.5	Enable IPv6Multicast Function	303
19.6	Static IPv6Multicast Route	303
19.7	The Maximum Transmission Unit	304
19.8	Ping IPv6Address.....	305
20	DHCP Configuration.....	306
20.1	Global DHCP Service Enablement	306

20.2	Enable Interface DHCP Relay	306
20.3	InterfaceDHCP Relay Address	307
20.4	DHCP Option82 Enablement	308
20.5	Treatment Strategy of DHCP Option82	309
20.6	Relay Identity of DHCP Option82	310
20.7	Remote Identity of DHCP Option82	311
20.8	Create DHCP Address Pool	312
20.9	DHCP Address Pool Subnet Segment.....	312
20.10	Default Route of DHCP Address Pool	313
20.11	DHCP Address Pool.....	314
20.12	The Lease Time of DHCP Address Pool	315
20.13	The Threshold of DHCP Address Pool	316
20.14	DNS Server Address	317
20.15	Log Server Address.....	318
20.16	WINS Server Address	318
20.17	Display DHCP Information.....	319
21	SNMP Configuration.....	321
21.1	SNMP Enablement	321
21.2	SNMP View.....	321
21.3	SNMP Community Name	322
21.4	SNMP Group	323
21.5	SNMP User	324
21.6	SNMP Trap Destination	326
22	LLDP Configuration	328
22.1	LLDP enablement.....	328
22.2	LLDP Port Operating Mode	328
22.3	Time Interval of Sending LLDP Message	329
22.4	LLDP Interface Management Address.....	330
22.5	Encapsulation Format of LLDP Message.....	331
22.6	Display LLDP neighbor information.....	331
22.7	Display LLDP Statistics Information.....	333
22.8	Display LLDP Local Information	334
22.9	Display LLDP Status Information.....	335
23	QOS Configuration	337
23.1	Configure Global QOS Enable/Disable	337
23.2	Configure the queue bitmap	337
23.3	Configure queue mode	338
23.4	Configure DSCP -COS bitmap	339
23.5	Configure DSCP -DSCP bitmap	340
23.6	Create a CLASS-MAP	341
23.7	Create a POLICY-MAP.....	342

23.8	Configure the CLASS-MAP Property	342
23.9	Configure the POLICY-MAP property	344
23.10	Configure the POLICY-MAP-C Property.....	344
23.11	Configure QOS Interface Mode.....	345
24	ACL Configuration	348
24.1	Configure IPV4 standard ACL based on IP addresses.....	348
24.2	Configure IPV4 Extended ACL based on IP addresses	349
24.3	Configure other IPV4 protocols based on IP addresses to extend ACL	351
24.4	Configure IPV4 ICMP Extend ACL Based on IP Addresses	352
24.5	Configure IPV4 ICMP Extend ACL Based on IP Addresses	353
24.6	Configure IPV4 based on IP addresses TCP extend ACL	354
24.7	Configure IPV4 based on IP addresses UDP extend ACL	357
24.8	Configure character type ACL based on IPV4 addresses.....	360
24.9	Configure character type ACL based on IPV6 addresses.....	362
24.10	View all configured ACL	364
24.11	Configure time-range	365
24.12	Time-range binds to the ACL	366
24.13	Activate ACL	367
24.14	Configure ACL based on MAC address	367
24.15	View all configured MAC ACL	369
24.16	Time-range and MAC ACL binding	369
24.17	Activate MAC ACL	370
24.18	View all Activated ACL.....	371
25	802.1X Authentication Configuration.....	372
25.1	Global802.1X Authentication Enablement	372
25.2	802.1X authentication port authorization mode	373
25.3	802.1X Authentication Port Controlled Direction	373
25.4	802.1X Authentication EAPOL Protocol Version.....	374
25.5	802.1X Authentication Port Silent Time	375
25.6	802.1x Authorization Port Reauthentication Interval	375
25.7	802.1X Authorization Server Timeout Time	376
25.8	802.1X Authorization Client Timeout Time	377
25.9	802.1X Authorization Message Retransmission Interval	377
25.10	802.1X Authorization Message Retransmission Interval	378
25.11	802.1x authorization port reauthentication mode.....	379
25.12	802.1X Authentication Port Initialization.....	380
25.13	802.1X Authorization Key Encryption Function	380
25.14	Display 802.1X Authentication Global Information	381
25.15	Display 802.1X Authentication Detailed Information	381
25.16	Display 802.1X Authentication Port Information	382
25.17	Display 802.1X Authentication Port Diagnosis Information	383

25.18	Display 802.1X Authentication Port Session Information	384
25.19	Display 802.1X Authentication Port Message Statistics	385
25.20	RADIUS Server Regeneration Interval	386
25.21	RADIUS Server	386
26	Alarm Configuration	388
26.1	Enable Port Alarm	388
26.2	Disable Port Alarm	389
26.3	Enable Power Alarm	389
26.4	Power off Warning	390
27	RMON Configuration	391
27.1	RMON Alarm Group	391
27.2	RMON Statistical Group	393
27.3	RMON History Group	393
27.4	RMON Event Group	394
27.5	Display RMON Alarm Group Information	395
27.6	Display RMON Statistics Information	396
27.7	Display RMON History Group Information	396
27.8	Display RMON Event Group Information	397
28	Log Configuration	398
28.1	Log File Size Limit	398
28.2	Log stdout Display	399
28.3	LogInformation Highest Display Level	399
28.4	Log Level Record Display	400
28.5	Syslog Server Download Log	401
29	NTP Configuration	403
29.1	NTP server	403
30	Network Diagnose Configuration	405
30.1	Ping Test	405
30.2	TracerouteTest	406
30.3	Port Loopback	407
31	System Management	408
31.1	Device Information Display	408
31.1.1	Display System Version	408
31.1.2	Display Product Information	408
31.2	System Software Upgrade	409
31.3	Configuration File Import and Export	410
31.3.1	Import Configuration File	410
31.3.2	Configure File Export	410
31.4	Log File Export	411
31.5	Save Configuration	412
31.6	Reboot the device	413

31.7	Restore factory settings	413

1 Login the Switch Configuration

1.1 Login the Switch Function Overview

There are two ways for users to manage devices: CLI and WEB.

- CLI
After logging into the device through the Console port, Telnet, or SSH, use the command line provided by the device to manage and configure the device. This approach requires configuring the user interface for the corresponding login mode.
- WEB
When the device acts as a server, users can log in to the device through the WEB administration. The device provides a graphical interface with the built-in WEB server to facilitate users to manage and maintain the device intuitively and conveniently. This method can only realize the management and maintenance part of functions of the device. If more complex or fine management of the device is needed, the CLI method is still needed.

1.2 Login the Switch

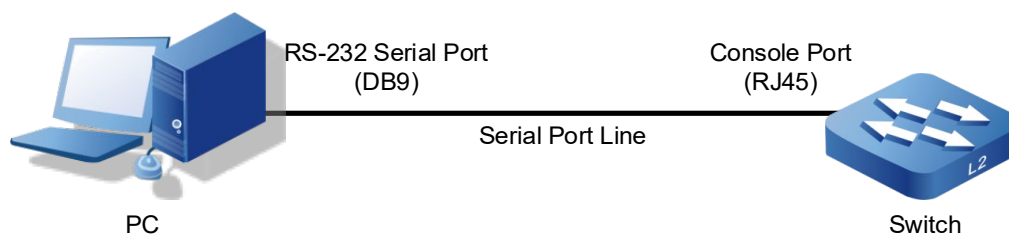
1.2.1 Login the Switch via Serial Port

Logging in through the Console port is the basic way to log in a device, and is the basis for configuring a device logged in through other means. By default, users can log into the device directly through the serial port, and the switch baud rate is

115200bit/s. The PC can log into the command line interface of the device by connecting to its Console port.

Operation Steps

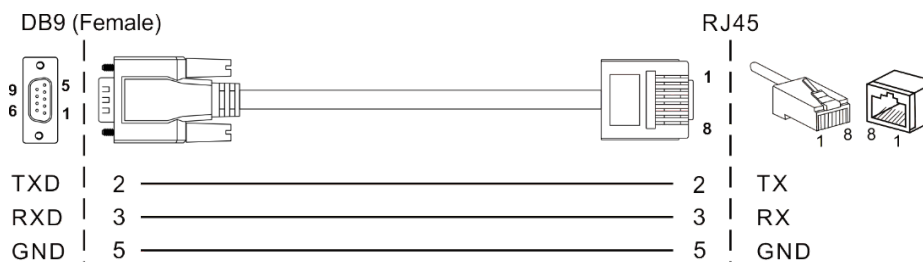
Step 1 Connect the serial port of the computer to the Console port of the device through the serial port line to establish a local configuration environment, as shown in the topology diagram below.



1. Connect DB9 at one end of serial port line to RS-232 serial port of PC.
2. Connect the RJ45 on the other end of the serial line to the Console port of the device.

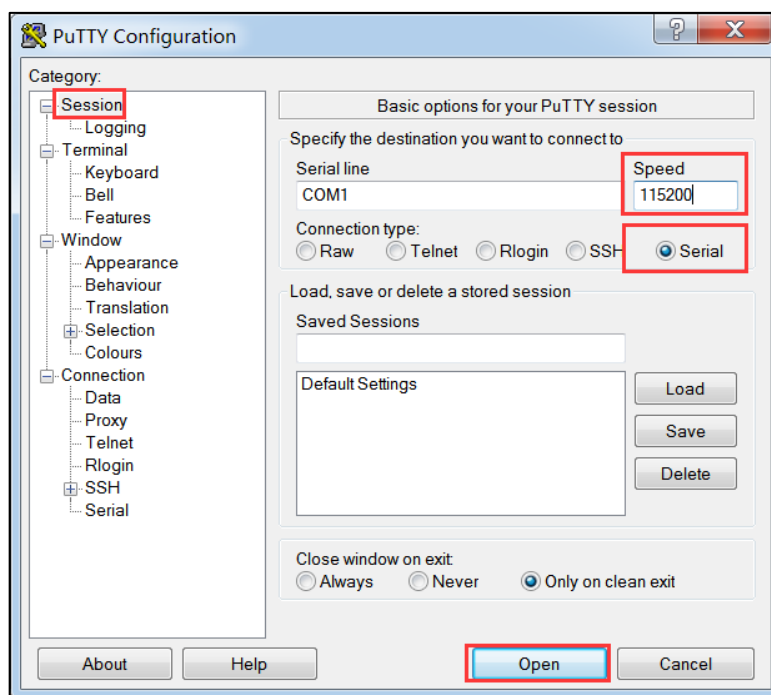
Notes:

Diagram of internal connection line of serial port line/communication cable is shown below.

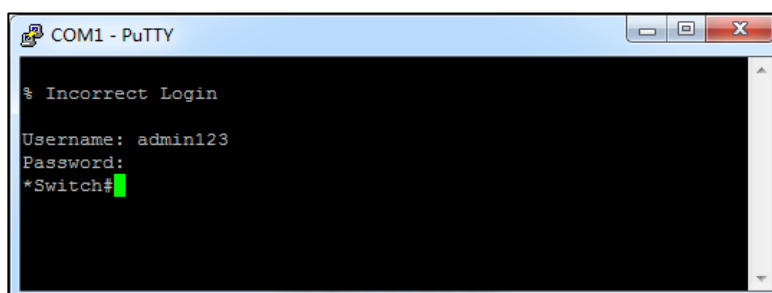


Step 2 Open the terminal simulation software on the PC, create a new connection, and set the interface and communication parameters of the connection. (Using PuTTY as an example here.)

1. Open PuTTY and click "Session" on the menu bar.
2. In the "Basic options for your PuTTY session" input box on the right, do the following:
 - Select "Connection type" to "Serial".
 - Enter "115200" in the "Speed" text box;
 - Click "Open".



3. The "COM1-PuTTY" command line edit dialog box pops up. Press enter key to enter user name and password. The user name and password are both "admin123" by default, as shown below.



Step 3 End.

1.2.2 Login the Switch via Telnet

Log into the switch by Telnet, and the device acts as Telnet-Server By default, the Telnet-Server function is enabled. Therefore, before using Telnet to log into the switch, it is necessary to configure the IP of the switch through serial port to ensure the normal communication between PC and DUT.

Telnet-Server Configuration

Operation	Command	Remark
Enter Configure Mode	configure terminal	-
Enable Telnet Server	telnet-server enable	Optional

Disable Telnet Server	<code>no telnet-server enable</code>	Optional



Notes

DUT acts as a Telnet server, if the logged client does not do any operation for a long time, it will automatically disconnect, i.e. timeout exit, and the function is enabled by default with 30m.

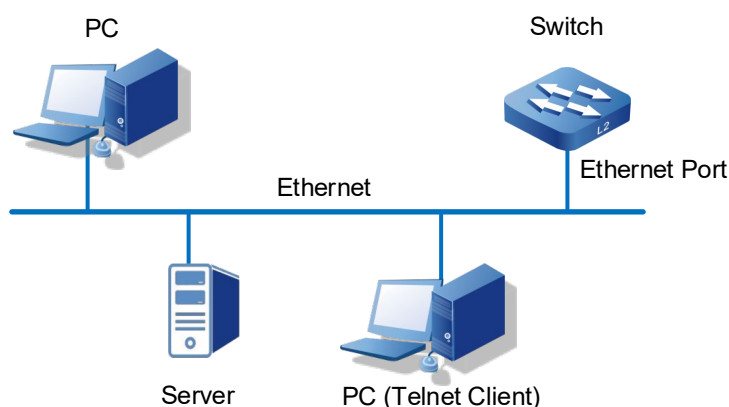
Through Telnet client login to the command line interface of the device, the client and the device should meet the following requires:

1. Configure the IP address of the switch correctly.
2. If the Telnet client and the device are in the same LAN, the IP address of the device and the client must be configured in the same network segment. Otherwise, the route between Telnet client and device must be accessible.

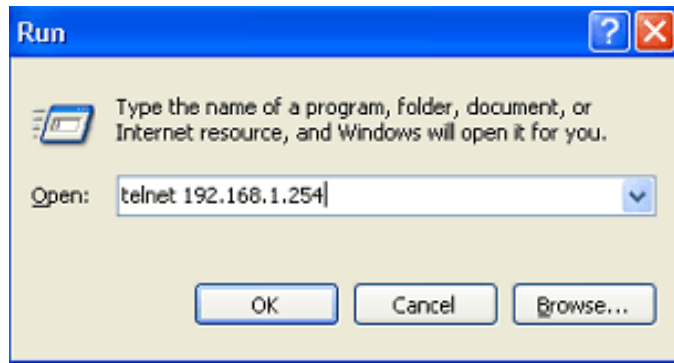
User can log in to the switch device through the Telnet client and configure the device if the two requires above are met.

Operation Steps

Step 1 As shown in the figure below, set up the configuration environment to connect the Ethernet port of the computer to the Ethernet port of the device through the LAN.



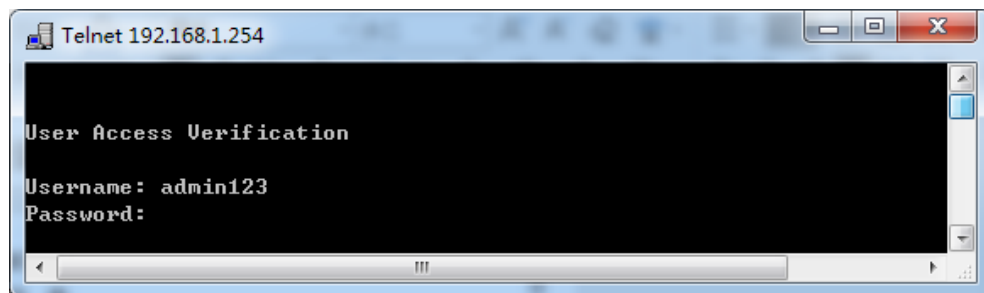
1. Run the Telnet client on the computer and input the administrative IP address of the Ethernet port connected the computer to the switch, as shown in the figure below.
2. Press "Win+R" to pop up the running window;
3. Enter "Telnet+ space + device IP address" in the "Open (O)" input box.
4. Click "OK" button.



Notes:

- Using the command line prompt interface of Win7/Win8/Win10 and other operating systems to configure the device needs to enable Telnet client in advance, user can check and enable Telnet client in the Windows function window under the path of "Control Panel > Program and Function > Enable or Disable Windows function", if Telnet client has been enabled, user can ignore this instruction.
- If the computer operating system does not support Telnet clients, a third party software PuTTY can be used as a Telnet client.
- The default IP address of the device is "192.168.1.254".

Step 2 The "Telnet" dialog box pops up and user can enter user name and password according to the hint. The default user name and password of the device is "admin123". Shown as below figure.



Step 3 End.

1.2.3 Login the Switch via SSH

The switch can be used as an SSH server, but can not used as an SSH client.

By default, the SSH server function of the device is disabled. When SSH is used to log in to the device, first of all, user needs to log in to the device through the Console port to enable the SSH server function and configure other properties correspondingly, to ensure normal login to the device through SSH.

SSH Configuration

Operation	Command	Remark
Enter Configure Mode	configure terminal	-

Operation		Command	Remark
Enable server	SSH	ssh-server enable	Optional
Disable server	SSH	no ssh-server enable	Optional



Notes

If SSH login to DUT is needed, the simplest operations are:

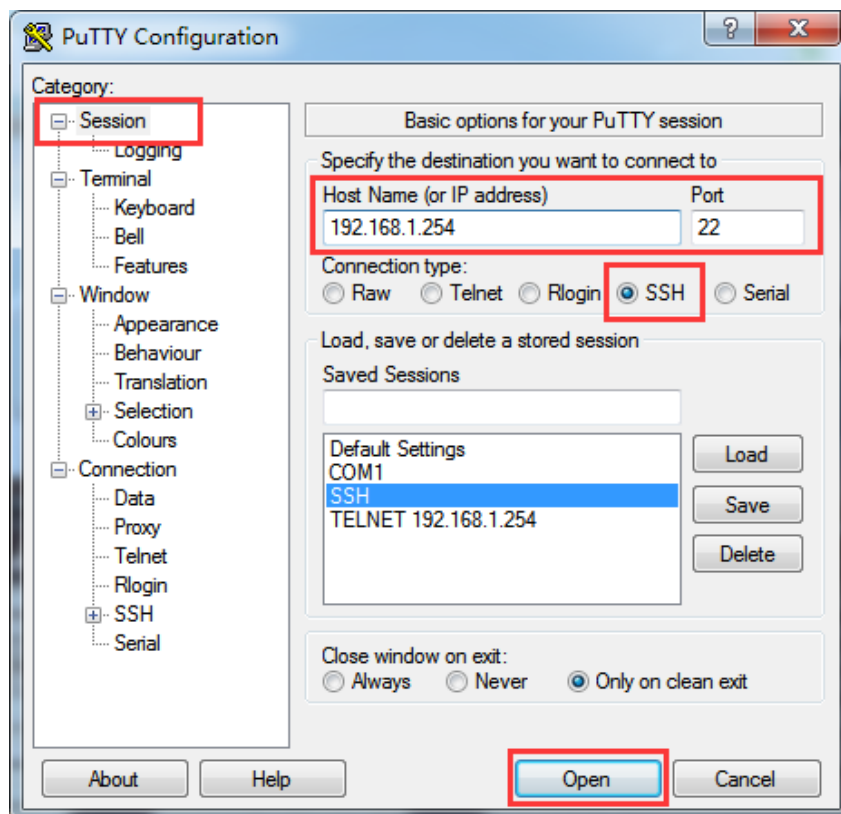
- Enable SSH;
- Configure SSH users, that is device users;
- Login the device

Operation Steps

Step 1 Using the Console port, enable SSH service using the "ssh-server enable" command.

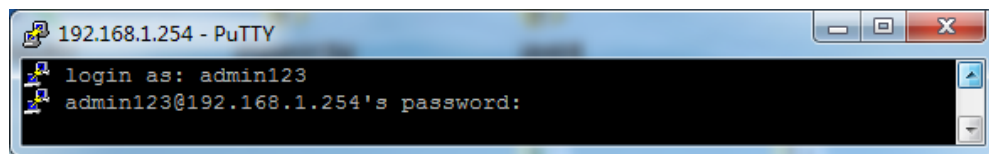
```
switch> enable
switch# configure terminal
switch(config)# ssh-server enable
```

Step 2 Run the third-party PuTTY software on the PC host as an SSH client to establish a secure connection with the device, and fill in the following parameters:



1. Click "Session" in the "Category" column.

2. Select "SSH" in "Connection type";
3. Enter the IP address "192.168.1.254" of the device in the "Host Name (or IP address)" text box.
4. The default port number is 22.
5. (Optional) enter the session name in the "Saved Sessions", such as SSH; click "Save" to save the session;
6. Click "Open" button to enter SSH configuration interface;
7. Enter the user account name of this device in the SSH client, such as the default user name and password is "admin123";



Notes:

With SSH enabled, all users on the device support SSH encrypted login.

8. SSH access to device succeed.

Step 3 End.

1.2.4 Login the Switch via WEB:

User can log into the switch through the WEB.

By default, the switch acts as an HTTP server function is enabled. Before logging into the WEB, user needs to ensure that the client has a browser and corresponding IP address to ensure normal communication between the client and the HTTP server.

WEB Log in Configuration

Operation	Command	Remark
Enter global mode	<code>configure terminal</code>	Required
Enable HTTP server	<code>http-server enable</code>	Optional
Disable HTTP server	<code>no http-server enable</code>	Optional

Configuration Environment Requirements

Client requirements: IE browser 8.0 above, some versions of 360 browser may have problems, other browsers have not found any problem at present.

Login WEB Management Platform

The user enter `http://X.X.X.X` directly in the browser (default switch management IP is 192.168.1.254), press Enter key to enter the switch login interface, enter user name

and password and click login to enter the main interface.
name and password of the device is "admin123".

The default user

1.2.5 Manage the switch via Network Management Software

The switch supports login management via network management software. By default, SNMP function is enabled, and can use the default community name. This only shows that the switch can be managed by SNMP. Please refer to the SNMP user manual for more detailed configuration.

SNMP login configuration

Operation	Command	Remark
Enter global mode	<code>configure terminal</code>	Required
Enable SNMP server	<code>snmp-server</code>	Required
Disable SNMP server	<code>no snmp-server</code>	Optional

1.3 Command Line

1.3.1 Command Analysis

Command consists of two parts: command word and command parameter.

Commands are all lowercase, input is case-insensitive; command words come in many forms, including: capital letters, (), <>, *, etc.

For example: IP address A.B.C.D/M (secondary|), IP and address are command words, and A.B.C.D/M and (secondary|) are command parameters.

1.3.2 Command Line Mode

Here are four major command-line patterns:

- Exec Mode: also called "View Mode", the basic mode of entering CLI. The prompt is ">", and user can only execute some simple commands, such as: show, enable, logout, etc. Login with priority of 0 (visiting user) is the Exec Mode. Other users log in in Privileged Exec Mode, and only the console login can upgrade the permissions through "enable". telnet, ssh and other login methods need to be configured with enable password to upgrade the permissions.

- Privileged Exec Mode: also known as "Enable Mode" with the prompt of "#", in Exec Mode, entered by executing enable command, or switched from other modes. Basic commands such as: debug, show, reboot, copy can be executed.
- Configure Mode: also known as "Configure Terminal", the prompt is "(config)#". User can execute the configure terminal to enter this mode in Privileged Exec mode, or switch to this mode from another mode, and all Configure Mode commands can be executed.
- Interface Mode: prompt is "(config-IFNAME)#". User can enter "Interface IFNAME" in ConfigurE Mode or switch to this Mode from another mode. Configuration command for the specified Interface can be executed.

1.3.3 Shortcut Key

Only the commonly used command parameters are covered here.

Shortcut Key	Description
?	Help command, enter"?" Command help is displayed.
Tab	Command completion, "Tab" can prompt or complete the remaining characters to be input when typing part of the command word.
Ctrl+D	To exit the current mode, can exit to the upper level mode in any mode, such as Interface Mode to Configure Mode.
Ctrl+C	End up command input or execution. Or directly return to "Enable Mode".
Ctrl+W	Delete an input command word or delete an input command parameter.
Ctrl+U	Deletes all characters from the current input command line.

Instance

"?" Help command. When using the command line, type"?" command help is displayed. Cases are as follows:

1. Type only "?" in a configuration mode, a list of all commands in the current mode is displayed.

```
Switch#?
```

```
Exec commands:
```

```
clear      Reset functions
clock      Config clock time
configure  Enter configuration mode
copy       Copy file
debug      Debugging functions (see also 'undebug')
```


disable	Turn off privileged mode command
enable	Turn on privileged mode command
erase	erase file
exit	End current mode and down to previous mode
faults	Fault management command
help	Description of the interactive help system
logout	Exit from the EXEC
loopback	config l2 interface loopback
mstat	Show statistics after multiple multicast traceroutes
mtrace	Trace multicast path from source to destination
no	Negate a command or set its defaults
ping	Send echo messages
quit	Exit current mode and down to previous mode
reboot	Halt and perform a cold restart
rm	erase file
show	Show running system information
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
undebug	Disable debugging functions (see also 'debug')
write	Write running configuration to memory, file or terminal

2. All commands matching the current command word are displayed when partial command words are entered.

Switch#**c?**

clear	Reset functions
clock	Config clock time
configure	Enter configuration mode
copy	Copy file

1.4 Common Command

1.4.1 Password Verification

The configuration process for enabling password verification:

Switch>**enable**

Switch#**configure terminal**

Switch(config)#**username admin password admin**

Switch(config)#**line vty 0**

Switch(config-line 0)#**login local**

Disable password verification:

```
Switch(config-line_0)#no login local
```

1.4.2 Customization display

Currently, there are four ways: exclude, include, grep and redirect:

- Exclude: only shows rows that do not contain the current string;
- Include: only displays the line that contains the current string;
- Grep: displays only the rows that conform to the current rule;
- Redirect: Redirect input to a system file.

Instance 1: show interface brief all

```
Switch#show interface brief all
```

Interface	IP-Address	Link	Protocol
lo	127.0.0.1	up	up
vlanif1	192.168.1.254	up	up

Interface	Link	Speed	Duplex	Type	PVID	Description
ge1	down	auto	auto	access	1	
ge2	down	auto	auto	access	1	
ge3	down	auto	auto	access	1	
ge4	down	auto	auto	access	1	
ge5	down	auto	auto	access	1	
ge6	down	auto	auto	access	1	
ge7	down	auto	auto	access	1	
ge8	down	auto	auto	access	1	
ge9	down	auto	auto	access	1	
ge10	down	auto	auto	access	1	
ge11	down	auto	auto	access	1	
ge12	down	auto	auto	access	1	
ge13	down	auto	auto	access	1	
ge14	down	auto	auto	access	1	
ge15	down	auto	auto	access	1	
ge16	down	auto	auto	access	1	
ge17	down	auto	auto	access	1	
ge18	down	auto	auto	access	1	
ge19	down	auto	auto	access	1	
ge20	down	auto	auto	access	1	
ge21	down	auto	auto	access	1	
ge22	up	100m(a)	full(a)	access	1	
ge23	down	auto	auto	access	1	
ge24	down	auto	auto	access	1	

```

xe1          down    10g(a)  full(a)  access  1
xe2          down    10g(a)  full(a)  access  1
xe3          down    10g(a)  full(a)  access  1
xe4          down    10g(a)  full(a)  access  1

```

Instance 2: show interface brief all | exclude ge Does not show interfaces containing ge

```

Switch#show interface brief all | exclude ge
Interface      IP-Address      Link      Protocol
lo             127.0.0.1       up        up
vlanif1        192.168.1.254   up        up

```

```

Interface      Link      Speed      Duplex      Type      PVID      Description
xe1            down      10g(a)     full(a)     access    1
xe2            down      10g(a)     full(a)     access    1
xe3            down      10g(a)     full(a)     access    1
xe4            down      10g(a)     full(a)     access    1

```

Instance 3: show interface brief all | include ge Only show interfaces containing ge

```

Switch#show interface brief all | include ge
ge1            down      auto       auto        access    1
ge2            down      auto       auto        access    1
ge3            down      auto       auto        access    1
ge4            down      auto       auto        access    1
ge5            down      auto       auto        access    1
ge6            down      auto       auto        access    1
ge7            down      auto       auto        access    1
ge8            down      auto       auto        access    1
ge9            down      auto       auto        access    1
ge10           down      auto       auto        access    1
ge11           down      auto       auto        access    1
ge12           down      auto       auto        access    1
ge13           down      auto       auto        access    1
ge14           down      auto       auto        access    1
ge15           down      auto       auto        access    1
ge16           down      auto       auto        access    1
ge17           down      auto       auto        access    1
ge18           down      auto       auto        access    1
ge19           down      auto       auto        access    1
ge20           down      auto       auto        access    1
ge21           down      auto       auto        access    1
ge22           up        100m(a)    full(a)     access    1
ge23           down      auto       auto        access    1
ge24           down      auto       auto        access    1

```

Instance 4: show interface brief all | grep ge*1 Show interfaces containing ge*1

```
Switch#show interface brief all | grep ge*1
ge1          down    auto    auto    access  1
ge10         down    auto    auto    access  1
ge11         down    auto    auto    access  1
ge12         down    auto    auto    access  1
ge13         down    auto    auto    access  1
ge14         down    auto    auto    access  1
ge15         down    auto    auto    access  1
ge16         down    auto    auto    access  1
ge17         down    auto    auto    access  1
ge18         down    auto    auto    access  1
ge19         down    auto    auto    access  1
```

Instance 5: show interface brief all | grep down Only show down interfaces

```
Switch#show interface brief all | grep down
ge1          down    auto    auto    access  1
ge2          down    auto    auto    access  1
ge3          down    auto    auto    access  1
ge4          down    auto    auto    access  1
ge5          down    auto    auto    access  1
ge6          down    auto    auto    access  1
ge7          down    auto    auto    access  1
ge8          down    auto    auto    access  1
ge9          down    auto    auto    access  1
ge10         down    auto    auto    access  1
ge11         down    auto    auto    access  1
ge12         down    auto    auto    access  1
ge13         down    auto    auto    access  1
ge14         down    auto    auto    access  1
ge15         down    auto    auto    access  1
ge16         down    auto    auto    access  1
ge17         down    auto    auto    access  1
ge18         down    auto    auto    access  1
ge19         down    auto    auto    access  1
ge20         down    auto    auto    access  1
ge21         down    auto    auto    access  1
ge23         down    auto    auto    access  1
ge24         down    auto    auto    access  1
xe1          down    10g(a)  full(a) access  1
xe2          down    10g(a)  full(a) access  1
xe3          down    10g(a)  full(a) access  1
xe4          down    10g(a)  full(a) access  1
```

1.4.3 Configuration Management

Command	Description
Switch# show running-config	Displays the configuration of the current system running
Switch# show startup-config	Displays the configuration of the system startup profile
Switch# write	Save command
Switch# erase startup-config	Restore factory settings
Switch# copy tftp startup-config 192.168.1.168 Switch.conf	Upload configuration file to switch
Switch# copy flash startup-config 192.168.1.168 Switch.conf	Download Configuration file from switch



Notes

If the configuration of the current system is inconsistent with the configuration of the system startup configuration file:

- After entering Configure Mode, the prompt is `*Switch`;
- Performing a system reboot will prompt whether need to save a disk.

1.4.4 System Upgrade

Suppose the upgrade package is "packetapp.bin", the IP address of the TFTP server is "192.168.1.168", and the command to upgrade the switch system is:

```
Switch#copy tftp package 192.168.1.168 packetapp.bin
```



Notes

The system upgrade must restart the switch to take effect.

The command to restart the system is: Switch#reboot.

After executing the restart, the screen will display as follows:

```
*Switch#reboot
save running config? (y/n): y
Building configuration...
[OK]
reboot system? (y/n): y
```

1.4.5 Debug Mode

1. Enter the debugging state of function module.

```
*Switch#debug ospf packet /*Enable receiving packet debug of ospf*/  
*Switch(config)#log stdout /*Log output to serial port*/
```

2. Print **message** information:

```
Switch # debug PKT-filter tx/rx icmp enable the information  
printing of received icmp messages or sent icmp messages.  
Switch # no debug PKT-filter tx/rx icmp disable the information  
printing of received icmp messages or sent icmp messages.
```

3. Check the detailed information such as the number of sending and receiving packets of various messages:

```
Switch#show pkt-filter
```

2 User Configuration

2.1 Add user

Command

```
username WORD
username WORD password (8|) LINE
username WORD privilege <0-15>
username WORD privilege <0-15> password (8|) LINE
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

WORD: a user name, length limited to 16 characters. And it cannot be numbers, characters other than ,! @ # ¥%.

(8|) : 8 means password encryption. This function will only take effect when global encryption is turned on.

LINE: password, limited to 8 characters. And it cannot be numbers, characters other than ,! @ # ¥%.

<0-15> a total of 16 user privilege priority, divided into four categories:

- 0: visit level; user can only view device version information and some simple configuration information.
- 1: view level; The configuration information of the device can be viewed, but the configuration of the device cannot be modified.
- 2: configuration level; User can view the configuration information of the device and configure some functional parameters of the device, but cannot manage the device.
- 3-15: management level; Have all permissions of the device, can download,

upload, restart, modify the device information and other operations.

Description

username WORD: this command adds a user name that has no password and priority defaults to 1.

Username WORD password (8) LINE: this command can add or change passwords to users that have already been created, or add users with passwords.

username WORD privilege <0-15> : this command has setting permission of the user and the default priority for all new users is 15.

Username WORD privilege <0-15> password (8) LINE: this command can create a new user, specify priority, and specify password.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#username admin123 privilege 15 password admin123
```

2.2 Delete User

Command

no username WORD

View

Configure Mode

Default Level

2: Configuration level

Parameters

WORD: a user name, length limited to 16 characters.

Description

Delete specify user

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#no username admin123
```



Notes

Deleted user names cannot be logged into the device, and when all user names have been deleted, the device only can be logged in through the Console port.

2.3 View Current Online Users

Command

```
show users
show logged users
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

show logged users: view current online users
show users: view current users with lower priority.

Instance

```
Switch> enable
Switch#show Logged users
Line      User      Type      Idle      Host(s)      Uptimes      Location
0         admin123  console   0          01:36:08     console
```

2.4 Console Login Management

The Console user interface is used to manage and monitor users logging in through the Console port. The device provides a RJ45 type Console port of RS-232 serial port. The terminal serial port of the user can connect directly with the device Console port to achieve local access to the device.

Command

```
line console <0-0>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<0-0> : parameter "0", local Console configuration, supporting only one user.

Description

Line console <0-0>: enters the Console user interface configuration view. The Console user interface can configure connection timeout, password validation, priority, and history command buffer sizes.

Instance

```
*Switch#configure terminal
*Switch(config)#line console 0
*Switch(config-console_0)#
```

2.5 Virtual Terminal Login Management

The VTY (Virtual Type Terminal) user interface is used to manage and monitor users logging in through VTY. After the user establishes a Telnet or SSH connection with the device through the terminal, a VTY channel is established. Currently each device supports up to 16 simultaneous VTY users. There is no fixed relationship between user interface and user. The user interface is assigned differently when the same user logs in different ways. Different user interfaces may be assigned for different login times for the same user.

Command

```
line vty <0-15>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<0-15> : VTY user channel 0-15, supports 16 VTY users to access the device simultaneously.

Description

Line vty <0-15> : enters the VTY user interface configuration view. The VTY user interface can configure connection timeout, password validation, priority, and history command buffer sizes.

Instance

```
*Switch#configure terminal
```

```
*Switch(config)#line vty 0  
*Switch(config-vty_0)#
```

2.6 Timeout Logout

Command

```
exec-timeout <0-35791> <10-2147483>
```

View

Console/ VTY user interface configuration mode

Default Level

2: Configuration level

Parameters

<0-35791> : timeout minutes range.

<10-2147483> : timeout seconds range.

Description

`exec-timeout <0-35791> <10-2147483>` : this command disconnects idle connections within a set time. If the connection is always idle during the set time, the system will automatically disconnect the connection. By default, the timeout of user interface disconnection is 10 minutes.

Instance

The system is configured with a 10-minute timeout by default. If the user is configured with password authentication, the user needs to enter the username and password again after the timeout to enter the system.

Configuration process for modifying the timeout logout:

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#line vty 0
```

```
Switch(config-vty_0)#exec-timeout 0 600
```

3 Port Configuration

3.1 Enter Port Configuration Mode

Command

```
interface IFNAME
interface ge <1-24>
interface loopback <0-1>
interface po <1-12>
interface range (ge | xe)
interface sa <1-12>
interface vlanif <1-4094>
interface xe <1-4>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

IFNAME: port name

Ge: Gigabit port name.

loopback: loopback port name

po: dynamic aggregation group name.

Range: supports range type port input. For example, interface range ge 1-10 is denoted as going into Gigabit port 1-10. Only Gigabit ports and 10 Gigabit ports are currently supported.

sa: static aggregation group name

vlanif : layer 3 interface

xe: 10 Gigabit port.

Description

This command is the mode navigation command that goes from Configure Mode to interface configuration mode. The next step is to modify the configuration of the corresponding interface.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface range ge 1-10
Switch(config-ge1-10)#
Enter 10 ports from ge1 to ge10.
```

3.2 Port Rate Limit

Command

```
bandwidth <64-10000000>
no bandwidth
```

View

fe (100M Ethernet) port view
ge (Gigabit Ethernet) port view
xe (10 Gigabit Ethernet) port view
sa (static aggregation group) port view
po (dynamic aggregation group) port view

Default Level

2: Configuration level

Parameters

<64-10000000> : the unit is kbps. For different ports, there are some restrictions on the parameters. The allowed input range of normal Gigabit ports is 64-1000000, and the allowed input range of 10 Gigabit ports is 64-10000000. If the input parameter is not in the specified range, the setting will not be successful and an error will be returned.

Description

bandwidth: this command does not actually affect the bandwidth of an interface, but simply allows the user to inform the system the bandwidth standard of that interface. By default, the bandwidth of an Ethernet interface is determined by the rate of the actual port connection, and can be manually configured if necessary. The bandwidth

is only a routing parameter and does not affect the real bandwidth of the interface of the physical link.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#bandwidth 128
```

3.3 Port Settings

3.3.1 Combo PortTransmission Media

Command

```
combo-port ( auto | copper | fiber )
```

View

fe (100M Ethernet) port view
ge (Gigabit Ethernet) port view

Default Level

2: Configuration level

Parameters

auto: Automatically select media types
Copper: forced to select copper port.
fiber: forced to select fiber port.

Description

combo-port: used to select the media type of the port.



Note

Change the media type of the port, the properties of the port will be updated to the default values.

By default, the first eight ports (ge1-ge8) default to "auto" mode, and the fiber transmission medium is preferred. That is, if a port is connected to both fiber port and copper port, then the port type is fiber port. If a port is only connected a copper port, the port type is copper port.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#combo-port copper
```

3.3.2 Duplex Mode

Command

```
duplex ( auto | full | half )
no duplex
```

View

```
fe (100M Ethernet) port view
ge (Gigabit Ethernet) port view
xe (10 Gigabit Ethernet) port view
```

Default Level

2: Configuration level

Parameters

Auto: full duplex and half duplex self-adaption.
Full: represents full duplex.
Half: represents half duplex.

Description

duplex (auto | full | half) : this command is used to set the duplex mode of the port.
By default, duplex mode of all ports is auto.
When setting the normal port rate to Gigabit, the duplex mode of the port cannot be set to half-duplex. When setting 10 Gigabit fiber ports, the duplex mode of the port cannot be set to half duplex. Otherwise the setting will not take effect and an error will be returned.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#duplex full
```

3.3.3 Flow Control

Command

```
flowcontrol (both| receive | send)
flowcontrol send (on | off)
flowcontrol receive (on | off)
no flowcontrol
```

View

```
fe (100M Ethernet) port view
ge (Gigabit Ethernet) port view
xe (10 Gigabit Ethernet) port view
sa (static aggregation group) port view
po (dynamic aggregation group) port view
```

Default Level

2: Configuration level

Parameters

both: Data transmit and receive of the port are set to self-negotiate flow control.

receive (on | off) : only enable or disable flow control on data receiving of the ports.

send (on | off) : only enable or disable flow control on data transmission of the ports.

Description

flowcontrol: this command is used to enable or disable flow control of the ports.

By default, flow control on all ports default to disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#flowcontrol both
```

3.3.4 Max-Frame

Command

```
mtu <64-16360>
no mtu
```

View

```
fe (100M Ethernet) port view
```


ge (Gigabit Ethernet) port view
xe (10 Gigabit Ethernet) port view
sa (static aggregation group) port view
po (dynamic aggregation group) port view
vlanif (layer 3) port view

Default Level

2: Configuration level

Parameters

<64-16360> : the allowed setting range of mtu is 64-16360.

<128-1500> : the allowed setting range of mtu in a layer 3 interface is 128-1500.

Description

mtu: this command is used to set the maximum data frame length supported by the interface, that is, the maximum length of the data portion of the link.

By default, the maximum data frame length for all physical ports is set to 1518. The MTU for the virtual port, such as vlanif1, is set to 1500.



Notes

when setting up virtual ports (such as vlanif1), the allowed maximum MTU value is 1500.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#mtu 1800
```

3.3.5 Interface Switch

Command

shutdown
no shutdown

View

fe (100M Ethernet) port view
ge (Gigabit Ethernet) port view
xe (10 Gigabit Ethernet) port view
sa (static aggregation group) port view

po (dynamic aggregation group) port view
vlanif (layer 3) port view

Default Level

2: Configuration level

Parameters

-

Description

shutdown: for interfaces (Ethernet ports, converged ports, and switched virtual interfaces), the command is primarily to close the corresponding interface, but other configurations of the interface still exist, just do not work. no shutdown is to open the port.

By default, the administrative state of the interface is UP.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface sa1
Switch(config-sa1)#shutdown
```

3.3.6 Rate

Command

```
speed (auto | 10m | 100m | 1g | 10g)
speed (auto | 1g | 10g)
speed (auto | 10m | 100m | 1g )
no speed
```

View

ge (Gigabit Ethernet) port view
xe (10 Gigabit Ethernet) port view
sa (static aggregation group) port view
po (dynamic aggregation group) port view

Default Level

2: Configuration level

Parameters

auto: Indicates that the rate of the interface is self-adaptive.
10M: set the interface rate to 10Mbps.
100M: set the interface rate to 100Mbps.

1G: set the interface rate to 1Gbps.

10G: set the interface rate to 10Gbps.

(auto|10m|100m|1g|10g): port rate configuration of dynamic and static aggregation groups.

(auto|1g|10g): 10 Gigabit port speed configuration

(Auto|10m|100m|1g): Gigabit port speed configuration.

Description

speed: this command is used to set the rate of the port.

By default, the rate of the interface is self-adaptive (auto). The port rate cannot be set to 1g or above when setting the normal port duplex mode to half. The port rate is set to a minimum of 1g, when setting a 10 Gigabit fiber port.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#speed 100m
```

3.4 Port Isolation

Command

```
port-isolate enable group <1-8>
no port-isolate enable
```

View

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

sa (static aggregation group) port view

po (dynamic aggregation group) port view

Default Level

2: Configuration level

Parameters

<1-8> : isolation group ID

Description

port-isolate: this command is used to add the current Ethernet ports to the isolation group.

no port-isolated: this command is used to remove the current Ethernet ports from the isolation group.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#port-isolate enable group 1
Switch(config-ge8)#no port-isolate enable
```

3.5 Storm Suppression

Command

```
storm-control ( broadcast | dlf | multicast ) level LEVEL
no storm-control ( broadcast | dlf | multicast ) level
```

View

ge (Gigabit Ethernet) port view
xe (10 Gigabit Ethernet) port view
sa (static aggregation group) port view
po (dynamic aggregation group) port view

Default Level

2: Configuration level

Parameters

broadcast: sets the limit of broadcast message traffic of the port
dlf: Destination look-up fail, which is to set unicast storm suppression.
multicast: sets the limit of multicast message traffic of the port
LEVEL: the percentage of restricted storm suppression, ranging from 0.00 to 100.00 to two decimal places.

Description

storm-control: this command is used to set the limit on unicast/multicast/broadcast messages traffic of the port.
no storm-control: this command is used to unconfigure restricted port messages.
After setting the upper limit of port message traffic, the port regularly detects the received unicast/multicast/broadcast message flow. Once the data flow of a certain type of message is detected to reach the storm control of the port, it would be considered as storm, then the port can block the forwarding of such message.
By default, the percentage of storm suppression is 100.00%.

Instance

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#storm-control broadcast level 20.02
Switch(config-ge8)#no storm-control broadcast level
```

3.6 MAC Address

3.6.1 Clear Dynamic MAC address

Command

```
clear mac-address-table dynamic (MAC | address MACADDR | interface  
IFNAME | vlan VID)
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

MAC: means clear of the specified dynamic MAC address, in the format HHHH.HHHH.HHHH.

address: means clear the specified dynamic MAC address.

interface: means to clear all dynamic addresses of a specified interface.

vlan: means to clear all dynamic addresses of the specified vlan, ranging from 1-4094;

Description

clear mac-address-table dynamic: this command is used to clear the specified dynamic MAC address, or to clear all dynamic MAC addresses on the specified interface or VLAN.

Instance

```
Switch> enable
*Switch#clear mac-address-table dynamic interface ge1
```

3.6.2 MAC address learning

Command

```
mac-address-learning ( disable | enable )
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

disable: disable global MAC learning.

enable: enable global MAC learning.

Description

mac-address-learning: The function of this command is to disable the global MAC address learning ability, so that the global MAC address learning can not be carried out; Or enable the global MAC address learning ability, according to the port of the MAC address learning ability to take effect.

By default, the learning capability of the global MAC address is enabled.

When the MAC address learning ability is enabled, the MAC address learned by the port is a dynamic MAC address, and the aging time is determined by the user settings.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mac-address-learning disable
```

3.6.3MAC address ageing-time

Command

```
mac-address-ageingtime ( 0 | <10-1000000> )
no mac-address-ageingtime
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

ageing-time: set the aging time of the global MAC. The value range of dynamic address aging time is <10-1000000>, in seconds. 0 means to disable aging function.

Description

mac-address-table ageingtime: command is to set the dynamic aging time of the MAC address table. When the user enters the 0 parameter, it means to disable the aging time of MAC.

no mac-address-ageingtime: MAC address aging time is restored to the default value. By default, the aging time is set to 300 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mac-address-ageingtime 500
```

3.6.4 Static MAC Address Filtering

Command

```
mac-address-table static MAC ( discard | forward ) IFNAME vlan VLAN
no mac-address-table static address MAC ( vlan VLAN | )
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

Discard: set a MAC address for the port .Discard the packet if the packet's source MAC address is the same as the set MAC address.

Forward: sets a MAC address of the port. Forward the packet if the source MAC address is consistent with the set MAC address.

Vlan: specifies the vlan corresponding to the table entry, with a range of <2-4094>. If there is no input, the default is vlan 1.

Description

mac-address-table static MAC forward IFNAME: this command is to set a static MAC address to the MAC table entry on the specified port. Static addresses, as opposed to dynamic ones, never aging and can only be manually configured and deleted. Static addresses will not lost even if the device is reset.

No static address is set by default.

Static addresses cannot be set to multicast addresses.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mac-address-table static 0.8.4 forward ge10 vlan
3
```

3.6.5 Multicast MAC Address Filtering

Command

```
mac-address-table multicast MAC ( discard | forward) IFNAMELIST
vlan <2-4094>
no mac-address-table multicast address MAC interface IFNAME vlan
<2-4094>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

IFNAMELIST: multiple ports can be entered simultaneously. For example: ge1, ge2

Vlan: specifies the vlan corresponding to the table entry, with a range of <2-4094>. If there is no input, the default is vlan 1.

Description

mac-address-table static MAC forward IFNAMELIST: this command is to set a static Multicast MAC address to the MAC table entry on the specified port. Static addresses, as opposed to dynamic protocol learned, never aging and can only be manually configured and deleted. Static addresses will not lost even if the device is reset.

no mac-address-table multicast: is used to remove static multicast table entries configured with command. The three commands of interface, mac and vlan can be randomly combined. That is, through the port to batch delete, can also delete a specific MAC specific VLAN under the specific port.

No static address is set by default.



Notes

Currently only single port deletions are allowed when deleting configuration. Multiple port combination deletion is not allowed.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mac-address-table multicast 0100.5e00.0001
forward ge10,ge11,ge12 vlan 3
```

3.6.6 Display MAC Address Table

Command

```
show mac-address-table
show mac-address-table ( multicast | dynamic | static | )
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

multicast: displays the table entry of multicast MAC address.

Dynamic: displays dynamic MAC address table entries.

static: displays dynamic MAC address table entries.

Description

show mac-address-table: this command displays the MAC table of the device. Without parameters, all MAC addresses are displayed, including user-configured static MAC addresses, dynamic MAC addresses learned by protocol, and multicast MAC addresses. With the relevant parameters, the corresponding MAC address is displayed, when with multicast, dynamic and static multicast MAC addresses are displayed.

Instance

```
Switch> enable
Switch#show mac-address-table
```

3.7 Mirror Command

3.7.1 Port Mirror Configuration

Command

```
mirror session <1-4> (both | receive | transmit ) destination IFNAME  
source IFNAMELIST
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

session: mirror group number, value range: <1-4>.

TRAFFIC: messages direction of monitored port. That is to monitor the messages received or transmit.

- both: means both receiving and sending packets are monitored.
- transmit: stands for direction of transmit package.
- receive: stands for direction of receive package.

directions: means the destination port.

source: means the source port. Multiple ports can be input at the same time, separated by commas.

Description

Mirrors a message in the specified direction of the source port to the destination port.



Notes

- There is and can only be one destination port for mirroring, but multiple source ports can be configured simultaneously. And the destination port of one mirror group cannot be the source port for other mirror groups.
 - The direction of the port mirroring cannot be covered, but only superimposed. When a certain direction is not needed, the group needs to be deleted and reconfigured.
-

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#mirror session 1 both destination ge1 source ge2,ge3
```

3.7.2 Delete Port Mirror

Command

```
no mirror session <1-4> direction (both | receive | transmit ) source  
IFNAME
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

session: mirror group number, value range: <1-4>.

TRAFFIC: messages direction of monitored port. That is to monitor the messages received or transmit.

- both: means both receiving and sending packets are monitored.
- transmit: stands for direction of transmit package.
- receive: stands for direction of receive package.

source: means the source port. Multiple ports can be input at the same time, separated by commas.

Description

Delete Mirror Configuration The three parameters in this instruction are optional, that is, user can only type session, or session and direction when deleting, or directly type no mirror without any parameters. And parameter position arbitrary swap, will not affect the execution of instructions.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#no mirror session 1 source ge2
```

3.8 Link Aggregation Configuration

3.8.1 Dynamic Aggregation System Priority

Command

```
lacp system-priority <priority>  
no lacp system-priority
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<priority> : dynamic aggregation system priority, range is 1-65535

Description

lacp system-priority: this command is used for dynamical aggregate system priorities.
By default, the system priority is 32768.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#lacp system-priority 1
```

3.8.2 Dynamic Aggregation Port Priority

Command

```
lacp prot-priority <priority>
no lacp prot-priority
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<priority> : dynamic aggregation port priority, range is 1-65535.

Description

lacp port-priority: this command is used for dynamic aggregation port priorities.
By default, the port priority is 32768.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#lacp port-priority 1
```

3.8.3 Dynamic Aggregation Port Timeout

Command

```
lacp timeout (short | long)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

Short: short timeout 3 seconds, the time threshold of neighborhood information aging.

Long: long timeout 90 seconds, the time threshold of neighborhood information aging.

Description

lacp timeout: this command is used for dynamic aggregate port timeout.

By default, it is long timeout.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#lacp timeout short
```

3.8.4 Add Dynamic Aggregation Group

Command

```
channel-group <id> mode (active | passive)
no channel-group
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

< id > : aggregation group number, the range is <1-12>.

Active: active mode, in which the switch actively initiates the aggregation negotiation process.

Passive: the mode in which the switch passively receives the aggregate negotiation process.

Description

channel-group: this command is used to add dynamic aggregation port members and configure the LACP mode for the ports.

When the first aggregation group member port is added, the corresponding aggregation group interface will be created. The interface name is Po + aggregation group number (the static aggregation group is sa+ aggregation group number). For example, a dynamic aggregation group interface named po100 with aggregation group number 100 is created by command channel-group 100 mode active.

When the last aggregation group member port is deleted, the corresponding aggregation group interface will be deleted.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#channel-group 1 mode active
```

3.8.5 Add static LACP

Command

```
static-channel-group <id>
no static-channel-group
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

< id> : aggregation group number, the range is <1-12>.

Description

static-channel-group: this command is used to add static aggregate port members.

When the first aggregation group member port is added, the corresponding aggregation group interface will be created. The interface name is sa + aggregation group number (the dynamic aggregation group is po+ aggregation group number). For example, a static aggregation group interface named sa9 with aggregation group number 9 is created by command static-channel-group 9.

When the last aggregation group member port is deleted, the corresponding aggregation group interface will be deleted.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#static-channel-group 2
```

3.8.6 Link Aggregation Load Balance Mode

Command

```
port-channel load-balance (dst-ip | dst-mac | dst-port | src-dst-ip
| src-dst-mac | src-dst-port | src-ip | src-mac | src-port)
no port-channel load-balance
```

View

Aggregation group interface view

Default Level

2: Configuration level

Parameters

dst-ip: the load balance mode is based on destination IP.

src-ip: the load balance mode is based on source IP.

src-dst-ip: the load balance mode is based on source and destination IP.

dst- MAC: the load balance mode is based on destination MAC.

src- MAC: the load balance mode is based on source MAC.

src- dst- MAC: the load balance mode is based on source and destination IP.

dst- port: the load balance mode is based on destination port, do not support currently.

src- MAC: the load balance mode is based on source port, do not support currently.

src- dst- port: the load balance mode is based on source and destination port, do not support currently.

Description

port-channel load-balance: this command is used to configure the load balance mode of the aggregate group.

Instance

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#interface ge8
Switch(config-ge8)#static-channel-group 2
Switch(config)#interface sa2
Switch(config-sa2)#port-channel load-balance dst-port
Switch(config-sa2)#exit
Switch(config)#interface ge7
Switch(config-ge7)#channel-group 1 mode active
Switch(config)#interface po1
Switch(config-po1)#port-channel load-balance src-mac
```

3.8.7 Displays Dynamic Aggregation Group

Command

```
show etherchannel {[<id>] | [detail] | [load-balance] | [summary]}
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

<id>: LACP aggregation group number

Description

show etherchannel: this command is used for LACP aggregation group related information.

Instance

```
Switch#show etherchannel
% LACP Aggregator: po1
% Member:
    ge7
```

3.8.8 Displays Static Aggregation Group

Command

```
show static-channel-group
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show static-channel-group: this command is used for static aggregation group information.

Instance

```
Switch#show static-channel-group
% Static Aggregator: sa1
% Member:           state
                    ge8          unbndl
```

3.9 Port Statistics

Port message statistics can be seen through the show interface IFNAME command. The following is the analysis of this instruction.

3.9.1 Display Port

Command

```
show interface IFNAME
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

IFNAME: port name

Description

The display mainly includes port name, port number, port medium, port property, port MAC address, MTU, bandwidth, configuration rate, duplex mode, running time and port message statistics. Here is an explanation of the key words that appear in the statistics:

- "Input" refers to the message statistics received by the port, i.e., "receive". "output" means the number of packets transmitted by the port, i.e., "transmit".

- "TYPE" refer to the classification of statistical message types.
 - "Total" represents the statistics of all types of messages in the corresponding direction (i.e. input or output), and the unit is bit.
 - "Unicast" represents the statistics of the packets of Unicast in the corresponding direction, and the unit is packets.
 - "Multicast" represents the statistics of the packets of packets in the corresponding direction, and the unit is packets.
 - "Broadcast" represents the statistics of the number of packets Broadcast in the corresponding direction, and the unit is packets.
 - "Dropped" represents the statistics of the packets lost in the corresponding direction, and the unit is packets.
 - "Error" represents the statistics of the number of packets of errors in the corresponding direction, with the unit of packets.
- "RATE" refers to the rate in the corresponding direction (it should be noted that this rate refers to the average rate in the corresponding type and direction in a specific period of time. Port statistics cannot be updated in real time, with an interval of about 24 seconds). In the "Total" type, the rate is expressed in parentheses as the ratio of message bytes to the "defined bandwidth" of the port, not the set bandwidth. The "defined bandwidth" here refers to the maximum bandwidth corresponding to the port, that is, the bandwidth ratio of the Gigabit port is calculated by Gigabit, and the 10 Gigabit port is calculated by 10 Gigabit, having nothing to do with the actual bandwidth set by the user.
- "PEAK" refers to the PEAK value, which is the maximum speed from the start to the execution of the command. The following brackets represent the time point at which the peak occurs.
- "TOTAL" refers to the total number of corresponding "TYPE". That is to say, the number (or digits) of corresponding type and direction messages obtained from startup to execution of command are counted. The following brackets represent the unit conversion result of the corresponding TOTAL (that is, when the TOTAL is 1024, the brackets show 1K).

In addition, all unit conversion in the command is carried out in the form of 1K = 1024.

Instance

```
Switch> enable
Switch#show interface gel
```

4 VLAN Configuration

4.1 Enter VLAN Configuration Mode

Command

```
vlan database
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

The vlan database command is used to enter VLAN configuration mode.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#vlan database
```

4.2 Add VLAN ID

Command

```
vlan <vlan-id> (name WORD | )  
vlan range VLANLIST  
no vlan <vlan-id>
```

View

VLAN configuration view

Default Level

2: Configuration level

Parameters

<vlan-id> : vlan id value, range is 2-4094.

WORD: VLAN name.

range: set the static VLAN in batch.

VLANLIST: VLAN range to be set, user can input a single number, continuous range

vlan or a combination of single and range, separated by commas, eg: 4, 10-20.

Description

vlan: this command is used to create a static VLAN and configure the VLAN name.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
```

4.3 Port Type

Command

```
switchport mode (access| hybrid | trunk)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

Access: set the link type of the port to access type.

Hybrid: set the link type of the port to hybrid type.

trunk: set the link type of the port to trunk type.

Description

switchport mode: this command is used to configure the link type of the port.

By default, the link type of all ports are access.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
```

```
Switch(config-ge8) #switchport mode trunk
```

4.4 Port Default VLAN

Command

```
switchport (access| hybrid ) vlan <vlan-id>  
no switchport (access| hybrid ) vlan  
switchport trunk native vlan <vlan-id>  
no switchport trunk native vlan
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

access vlan: set the default vlan for a port in access mode to <2-4094>.

hybrid vlan: sets the default vlan for a port in hybrid mode to <2-4094>.

<2-4094> : VID allowed setting range is 2-4094.

Native vlan: set the local VLAN and classify the unmarked traffic through the Layer 2 interface, that is, set the PVID of the port.

Description

switchport (access | hybrid) vlan: this command is to reset the default VLAN of the port. For example, enter the configuration mode of port ge1, the port ge1 is in hybrid mode, and enter "switchport hybrid vlan 3". The default VLAN ID for port ge1 becomes 3.

switchport trunk native vlan: this command specifies a native VLAN for a trunk port. As a Trunk port, it must belong to a native VLAN. The native VLAN refers to UNTAG messages sent and received on the interface, which are all considered to belong to the VLAN. Obviously, the default VLAN ID of the interface (i.e., PVID in IEEE 802.1Q) is the VLAN ID of the native VLAN. At the same time, if native VLAN frames are sent in Trunk port, UNTAG must be adopted.

By default, the default VLAN ID of the port is 1.



Notes

When setting the VLAN ID, the port mode parameter of the command must be consistent with the current mode of the setting port to ensure the setting takes effect, otherwise an error

will be returned.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#switchport access vlan 2
```

4.5 Classify VLAN Based on Port

Command

```
switchport hybrid allowed vlan add (tag| untag )<vlan-id>
switchport hybrid allowed vlan remove <vlan-id>
switchport hybrid allowed vlan (all | none)
switchport trunk allowed vlan (add |except | remove) <vlan-id>
switchport trunk allowed vlan (all | none)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<vlan-id> : VLAN ID, range is 1-4094.

Add: add the port to the VLAN.

All: add ports to all VLANS.

Except: adds a port to all VLANS except the one specified.

None: delete the port from all VLANS except PVID.

Remove: delete the port from the specified VLAN.

Tag: the port will add a VLAN tag when forwarding a VLAN message.

Untag: the port will remove the VLAN Tag when forwarding a VLAN message.

Description

switchport (hybrid | trunk) allowed vlan: this command is used to configure the port to be added to or removed from a specified VLAN.



Notes

- When adding hybrid or trunk ports to a VLAN, the port should be set to the appropriate type.

- Hybrid or trunk ports are untag in the VLAN to which PVID belongs, and trunk ports are tag in VLAN except PVID.
-

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#switchport hybrid allowed vlan add tag 2
```

4.6 Display VLAN Information

Command

```
show vlan all
show vlan brief
show vlan <2-4094>
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

<2-4094>: VLAN ID range is 2-4094.

Description

```
show vlan all: displays all vlan information.
show vlan brief: displays vlan information of all Bridges.
show vlan <2-4094> : displays the specified vlan information.
```

Instance

```
Switch> enable
Switch# show vlan 2
```

4.7 Port Receive Frame Type

Command

```
switchport acceptable-frame-type (all | tagged | untagged)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

All: there is no restriction on whether the received message with tag.

Tagged: only allow the port to receive tagged message, that is, stop the port to receive untagged message.

Untagged: only allow the port to receive untagged message, stop the port to receive tagged message.

Description

switchport accept-frame-type: this command is used to restrict whether the port is allowed to accept message with tags.

By default, the accepted frame type of the port is set to all, which means that the port does not by default restrict whether or not it can receive packets with tags. However, if the accepted frame type of the port is set to tagged, the port can only allow tagged message to pass, and other packets will be discarded.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#switchport acceptable-frame-type tagged
```

4.8 Port Entry Filtering

Command

```
switchport ingress-filter ( enable | disable )
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

Enable: only messages from the VLAN to which the port belongs are allowed to be received.

Disable: allows to receive messages from VLANs that do not belong to the port.

Description

The ingress filter function of the device defaults to enable, that is, any port only allows packets belonging to its VLAN to pass through. Other message will be discarded.

However, when the ingress filter function of the port is set to disable, the port will allow to receive messages not belonging to the VLAN of the port and forward the message to the specified VLAN.

For example, set port entry filtering on port ge1 to disable. Port ge1 belongs to vlan10. The message is sent to ge2 belonging to vlan20. After ge1 receives the message, the port will receive the message and forward the message to the specified vlan. In other words, the message will be forwarded to ge2 belonging to vlan20 instead of discarding the message.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#switchport ingress-filter disable
```

VLAN Classifier Function

VLAN Classifier Function Introduction

The VLAN classifier is similar to PVID in that it assigns a default VLAN ID to packets entering the switch port. It provides MAC based, subnet based and protocol based allocation. If a packet matches all of the three, only one rule will take effect. The priority of the rules is: MAC-based, subnet-based, and protocol-based. For example, if MAC-based rules are matched first, neither subnet-based nor protocol-based VLAN allocation rules will take effect. If none of the three rules match, VLAN ID are assigned according to PVID rule.

Rule configuration.

Classify VLAN Based on Sub-network

Command

```
vlan classifier rule <1-256> ipv4 A.B.C.D/M vlan <1-4094>
```

View

Global Configuration

Default Level

2: Configuration level

Parameters

<1-256>: group number.

A.B.C.D/M: sub-network segment.

<1-4094>: represents the VLAN ID assigned by the matching rule.

Description

Configure subnet-based VLAN rules.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#vlan classifier rule 1 ipv4 192.168.2.0/24 vlan 2
```

4.9.2.2 Classify VLAN Based on MAC Address

Command

```
vlan classifier rule <1-256> mac WORD vlan <1-4094>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<1-256>: group number.

MAC: MAC address.

<1-4094>: represents the VLAN ID assigned by the matching rule.

Description

Configure MAC-based VLAN rules.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#vlan classifier rule 1 mac 0.0.2 vlan 3
```

4.9.2.3 Classify VLAN Based on Protocol

Command

```
vlan classifier rule <1-256> proto  
(ip|ipv6|ipx|x25|arp|rarp|atalkddp|atalkaarp|atmmulti|atmtrans  
port|pppdiscovery|pppsession|xeroxppp|xeroxaddrtrans|g8bpqx25|  
ieeepup|ieeeaddrtrans|dec|decnadamload|decnaremotconsole|d  
ecdnarouting|declat|decagnostics|deccustom|decsyscomm|<0-655  
35>) encap (ethv2|snapllc|nosnapll) vlan <1-4094>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<1-256>: group number.

proto: Ethernet protocol type; enter ip, ipv6, ipx, x25, arp, rarp, atalkddp, atalkaarp, atmmulti, atmtransport, pppdiscovery, pppsession, xeroxppp, xeroxaddrtrans, g8bpqx25, ieeepup, ieeeaddrtrans, dec, decnadamload, decnaremotconsole, decdnarouting, declat, decagnostics, deccustom, decsyscomm or enter protocol number <0-65535>

encap: Ethernet Encapsulation Type; ethv2, snapllc, nosnapll.

<1-4094> : represents the VLAN ID assigned by the matching rule.

Description

Configure protocol-based VLAN rules.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#vlan classifier rule 1 proto ip encap ethv2 vlan  
3
```

4.9.2.4 Delete VLAN Rule

Command

```
no vlan classifier rule <1-256>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<1-256> : group number.

Description

Delete a rule.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#no vlan classifier rule 1
```

4.9.3 Group Configuration

Command

```
vlan classifier group <1-16> (add | delete) rule <1-256>
no vlan classifier group <1-16>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<1-16> : group number.
add: add a rule to a group.
delete: delete a rule from a group.
<1-256> : rule number;

Description

vlan classifier group: group configuration.
no vlan classifier group: delete group.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan classifier group 1 add rule 2
Switch(config)#no vlan classifier group 2
```

4.9.4 Interface Configuration Command

Command

```
vlan classifier activate <1-16>  
no vlan classifier activate <1-16>
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<1-16> : reference group number;

Description

vlan classifier activate: interface reference group.

no vlan classifier activate: delete interface reference group.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#interface ge1  
Switch(config-ge1)#vlan classifier activate 1  
Switch(config-ge1)#no vlan classifier activate 2
```

5 Ring Configuration

Ring is made up of the company independent research and development, professional link redundancy backup for the needs of high reliability of industrial control network application and development of the design of Ethernet rapid spanning tree algorithm, its design concept is completely in accordance with international standards (STP and RSTP) implementation, and do the necessary for industrial control application optimization, with Ethernet link redundancy, fault fast automatic recovery ability, when a network interruption or network failure, Ring can ensure that the user network automatic recovery link communication within 20 ms.

5.1 Globe Ring Enablement

Command

```
[no ] ring
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

ring: this command is used to enable the global Ring function.

no ring: this command is used to disable the global Ring function and delete all Ring groups.

By default, the global Ring function is disabled.

Instance

```
Switch> enable
Switch# configure terminal
Switch(config)# ring
```

5.2 Create Ring NetworkGroup

Command

```
ring <group-id> id <ring-id> port1 <ifname> port2 <ifname> type
0 hello <hello-time> (master | slave)
ring <group-id> id <ring-id> port1 <ifname> port2 <ifname> type
<type-id> hello <hello-time>
no ring <group-id>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

group-id : ring group ID, range is 1-4.

ring-id : ring loop ID, range is 0-255.

ifname: ring port name, the port can be a physical port or a static aggregation group, and the port cannot enable spanning tree or ERPS.

type-id: ring loop type, range 0-3, corresponding to Single Ring, Coupling Ring, Chain, Dual Homing.

hello-time: hello request packet sending period, range 0-300(*100ms), 0 means to do not send.

Master | slave: ring network master device selection, no master station if all are masters, only ring type is Single ring can be configured.

Description

ring <group-id> : this command is used to configure the ring group.

no ring <group-id> : this command is used to delete the ring group.

By default, no ring group is configured.

Ring Type Description

A Single ring is a basic ring networking structure in which all devices are connected in a ring. When the network is working normally, the algorithm running on the device will automatically block a link as a backup link to ensure the normal operation of the

network. When the network link failure occurs, the algorithm will automatically start the backup link and restore the data communication within 20ms.

Coupling Ring is a redundant structure introduced to connect two separate networks. The Coupling Ring provides additional security by enabling the coupling of two ports on different switches. For some systems, users can also create single rings for devices from different regions and also integrate multiple single rings through the Coupling Ring to create a larger redundant network.

Chain refers to connecting multiple switch devices in series and connecting both ends of the Chain to Ethernet network. Chain has strong channel selection ability. When the network is working properly, the algorithm automatically blocks one link in the Chain as a backup link, forcing all devices to access the Ethernet network from the unblocked end of the link. When Chain link failure occurs, the algorithm will automatically start the backup link within 20ms and quickly guide the device access the Ethernet network through the side that do not has a link failure.

Dual Homing is a special case of the Chain, in which users can host the same switch on two different networks or two different switching devices on the same network. The algorithm will automatically select one link for data communication according to the link condition. When the link in the communication state fails, the other link will start to work within 20ms.

Note:

1. RING loop ports can be normal physical ports or static aggregation groups.
2. The RING loop port cannot enable other layer 2 protocols (MSTP, ERPS, etc.) at the same time.

Instance

```
Switch> enable
Switch# configure terminal
Switch(config)# ring 1 id 1 port1 ge1 port2 ge3 type 1 hello 1
```

5.3 Display Ring Network Information

Command

```
show ring [<group-id>]
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

group-id : ring group ID, range is 1-4

Description

show ring: this command is used to show Ring information.

Instance

```
Switch(config)#interface ge3
Switch(config-ge3)#spanning-tree disable
*Switch(config-ge3)# exit
*Switch(config)#interface ge4
*Switch(config-ge4)#spanning-tree disable
*Switch(config-ge4)#exit
*Switch(config)#ring 1 id 1 port1 ge3 port2 ge4 type 0 hello 0 master
*Switch#show ring
ring global : Enable
ring list:
ring GROUP: 1
ring ID: 1
ring PORT1: ge3
ring PORT1 state: block
ring PORT2: ge4
ring PORT2 state: block
ring TYPE: Single
ring HELLOTIME: 0
ring : master
```

6 MSTP Configuration

6.1 Globle Spanning-tree Enablement

Command

```
spanning-tree (enable | disable)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree enable: this command is used to enable the globle spanning tree protocol.

spanning-tree disable: this command is used to disable the spanning tree protocol.

By default, the global spanning tree protocol is enabled.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#spanning-tree disable
```

6.2 Enter MSTP Instance Configuration View

Command

```
spanning-tree mst configuration
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree mst configuration: this command is used to enter the MSTP instance configuration view.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
```

6.3 Create MSTP Instance

Command

```
instance < instance -id> vlan <vlan-id>
no instance < instance -id> [vlan <vlan-id>]
```

View

MST configuration view

Default Level

2: Configuration level

Parameters

<instance-id> : represents the number of MSTI in the range 0-16.

<vlan-id> : VLAN ID value, range is 1-4094.

Description

instance: This command is used to create MSTP instance.

no instance: this command is used to delete the MSTP instance.

instance instance_id vlan vlan_id: this command is used to configure the mapping between vlan and MSTP instances. If the Instance does not exist, it will be created first.

By default, all VLANs map to CIST (that is, MSTI 0).

**Notes**

- Different MSTI cannot be mapped to the same VLAN. If a VLAN that has been mapped to one MSTI is remapped to another MSTI, the original mapping relationship will be canceled.
 - When adding a VLAN mapping, it is recommended to configure the VLAN first.
-

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 1 vlan 2
```

6.4 MSTP Revision Level

Command

```
revision <level>
```

View

MST configuration view

Default Level

2: Configuration level

Parameters

<level> : revision level, range 0-255.

Description

revision: this command is used to configure the MSTP revision level for the MST domain.

By default, the MSTP revision level for the MSTP domain is 0.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#revision 1
```

6.5 MST Domain Name

Command

```
region <name>
```

```
no region <name>
```

View

MST configuration view

Default Level

2: Configuration level

Parameters

<name> : the domain name of the MST domain.

Description

region <name>: this command is used to configure the domain name for the MST domain.

By Default, the MST domain name is Default.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#region test
```

6.6 Device Priority

Command

```
spanning-tree [instance <instance_id>] priority <priority>
no spanning-tree [instance <instance_id>] priority
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<priority> : device priority (multiple of 4096), <0-61440>

Description

spanning-tree priority: this command is used to configure the device priority of CIST.

no spanning-tree priority: this command is used to restore the device priority of CIST to the default value.

spanning-tree instance priority: this command is used to configure the device priority of the MSTI.

no spanning-tree instance priority: this command is used to restore the device priority of MSTI to the default value.

By default, the device priority is 32768.

CIST refers to spanning tree instance 0, and MSTI refers to creating spanning tree instance, with instance range 1-16.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree priority 4096
```

6.7 Spanning-tree Protocol Version

Command

```
spanning-tree force-version <version>
no spanning-tree force-version
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<version> : spanning tree protocol version number, range is 0-3, 0 is STP compatibility mode, 2 is RSTP mode, 3 is MSTP mode, 1 is unsupported.

Description

spanning-tree force-version: this command is used to configure the version of the spanning tree protocol.

no spanning-tree force-version: this command restores the version of the spanning tree protocol to the MSTP protocol.

By default, the working mode of MSTP is MSTP mode.

MSTP and RSTP can recognize each other's protocol messages and are compatible with each other. STP cannot recognize MSTP messages, in order to realize mixed networking with STP equipment and complete compatibility with RSTP, there are three operating modes have been set: STP compatibility mode, RSTP mode and MSTP mode.

- In STP compatibility mode, each port of the device will send out STP BPDU messages.
- In the RSTP mode, each port of the device will send out RSTP BPDU messages.

When it is found to be connected with the device running STP, the port will automatically switch to the STP compatibility mode.

- In MSTP mode, each port of the device will send out MSTP BPDU messages. When it is found that it is connected with the device running STP, the port will automatically switch to STP compatibility mode.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree force-version 2
```

6.8 Spanning Tree Timer Parameter

Command

```
spanning-tree (hello-time | forward-time | max-age) <seconds>
no spanning-tree hello-time
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<seconds> : hello-time range <1-10>, forward-time range <4-30>, max-age range <6-40>, all in seconds

Description

spanning-tree hello-time: the command is used to configure the hello-time.

no spanning-tree hello-time: this command is used to restore the hello-time to default value.

By default, hello-time is 2 seconds, forward-time is 15 seconds, and max-age is 20 seconds.

The values of the three time parameters of the root bridge hello-time, forward-time and max-age should meet the following formula, otherwise will cause the network oscillation frequently:

$$2 \times (\text{forward-time} - 1) \geq \text{max-age}$$
$$\text{max-age} \geq 2 \times (\text{hello-time} + 1)$$

Instance

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#spanning-tree hello-time 3
```

6.9 The Maximum Hop of Spanning-tree

Command

```
spanning-tree max-hops <hops>  
no spanning-tree max-hops
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<hops> : the maximum hops of MST domain are in the range <1-40>.

Description

spanning-tree max-hops: this command is used to configure the maximum number of hops of the MST domain.

no-spanning -tree max-hops: this command restores max-hops as the default.

By default, the max-hops is 20.

Starting from the root bridge of spanning tree in MST domain, every time configuration message in domain (namely BPDU message) is forwarded by a device, the hop number is reduced by 1; Devices discard configuration messages with 0 hops received, preventing devices outside the maximum hops from participating in the spanning tree calculation, limiting the size of the MST domain.

If the current device becomes the root bridge of CIST in MST domain or the root bridge of MSTI, the maximum hop number of this device configuration will become the network diameter of this spanning tree, limiting the scale of this spanning tree in the current MST domain. Devices that do not generate root Bridges in the MST domain will use the maximum number of hops set by the root bridge.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#spanning-tree max-hops 24
```


6.10 The Rate that the Spanning Tree Sends a BPDU

Command

```
spanning-tree transmit-holdcount <count>
no spanning-tree transmit-holdcount
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<count> : maximum number of message sent per second, range is <1-10>.

Description

spanning-tree transmit-holdcount: this command is used to configure the maximum rate of sending the BPDU of the port.

no spanning-tree transmit-holdcount: this command is used to restore the maximum rate of sending the BPDU of the port to default value.

By default, transmit-holdcount is 3.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree transmit-holdcount 10
```

6.11 Compatible with Cisco MSTP Mode

Command

```
spanning-tree cisco-interoperability (enable | disable)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree cisco-interoperability enable: this command is used to enable compatibility with the cisco MSTP pattern.

By default, cisco MSTP mode is not compatible.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#spanning-tree cisco-interoperability enable
```

6.12 Global Edge Port BPDU Filtering

Command

```
spanning-tree portfast bpdu-filter
```

```
no spanning-tree portfast bpdu-filter
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree portfast bpdu-filter: this command is used to enable the global portfast bpdu-filter function.

no-spanning -tree portfast bpdu-filter: this command disables the global portfast bpdu-filter function.

By default, global portfast bpdu-filter is disabled.

The portfast features (bpdu-filter and bpdu-guard) both need to be valid on the portfast port (see related command spanning-tree portfast). The portfast feature can be enabled in configure mode or under the port (see the relative commands under the port). There are only enable and disable two state in configure mode, while there are enable, disable and default three states under the port. When the portfast feature configured under the port is default, the actual running portfast feature under the port will be the same as the global portfast feature. When the portfast feature configured of the port is enable or disable, the actual running portfast feature of the port will be

consistent with the portfast feature configured on the port. Use the show spanning-tree interface command to view relative details.

By default, the global portfast bpdu-filter function is disabled.

The portfast function is mainly used to connect devices such as terminals or servers, which needs fast convergence ports, similar to edgeport. Portfast must be enabled if the port needs to use the portfast feature.

Bpdu-filter function is used for portfast port, after enabling it, the port will not send and receive bpdu messages.

bpdu-guard function is used for portfast port. Once enabled, when the port receives bpdu message, the port will change into error-disable state (shutdown), which can be restored by errdisable-timeout function.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree portfast bpdu-filter

*Switch#show spanning-tree interface ge6
% Default: Bridge up - Spanning Tree Enabled - topology change
detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit
Hold Count 6 - Max-hops 20
% Default: CIST Root Id 800000b25f5f0003
% Default: CIST Reg Root Id 800000b25f5f0003
% Default: CIST Bridge Id 800000b25f5f0003
% 0: 1 topology change(s) - last topology change Thu Jan 1 08:00:29
1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard enabled
% Default: portfast errdisable timeout enabled
% Default: portfast errdisable timeout interval 300 sec
% ge6: Port Number 910 - Ifindex 5006 - Port Id 838e - Role Disabled
- State Discarding
% ge6: Designated External Path Cost 0 -Internal Path Cost 0
% ge6: Configured Path Cost 20000 - Add type Explicit ref count
1
% ge6: Designated Port Id 0 - CIST Priority 128 -
% ge6: Message Age 0 - Max Age 0
```

```
% ge6: CIST Hello Time 0 - Forward Delay 0
% ge6: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 -
topo change timer 0
% ge6: forward-transitions 0
% ge6: Version Multiple Spanning Tree Protocol - Received None
- Send MSTP
% ge6: No portfast configured - Current portfast off
% ge6: portfast bpdu-guard default - Current portfast
bpdu-guard on
% ge6: portfast bpdu-filter default - Current portfast
bpdu-filter off
% ge6: no root guard configured - Current root guard off
% ge6: Configured Link Type point-to-point - Current
point-to-point
% ge6: No auto-edge configured - Current port Auto Edge off
```

6.13 Global Edge Port BPDU Protection

Command

```
spanning-tree portfast bpdu-guard
no spanning-tree portfast bpdu-guard
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree portfast bpdu-guard: this command is used to enable the global portfast bpdu-guard function.

no spanning-tree portfast bpdu-guard: this command is used to disable the global portfast bpdu-guard function.

By default, global portfast bpdu-guard is disabled.

The portfast features (bpdu-filter and bpdu-guard) both need to be valid on the portfast port (see related command spanning-tree portfast). The portfast feature can be enabled in configure mode or under the port (see the relative commands under the port). There are only enable and disable two state in configure mode, while there are

enable, disable and default three states under the port. When the portfast feature configured under the port is default, the actual running portfast feature under the port will be the same as the global portfast feature. When the portfast feature configured of the port is enable or disable, the actual running portfast feature of the port will be consistent with the portfast feature configured on the port. Use the show spanning-tree interface command to view relative details.

By default, the global portfast bpdu-filter function is disabled.

The portfast function is mainly used to connect devices such as terminals or servers, which needs fast convergence ports, similar to edgeport. Portfast must be enabled if the port needs to use the portfast feature.

Bpdu-filter function is used for portfast port, after enabling it, the port will not send and receive bpdu messages.

Bpdu-guard function is used for portfast port. Once enabled, when the port receives bpdu message, the port will change into error-disable state (shutdown), which can be restored by errdisable-timeout function.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree portfast bpdu-guard
```

6.14 Port error-disable Timeout Recovery

Command

```
spanning-tree errdisable-timeout (enable | disable)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree errdisable-timeout enable: this command is used to configure the error-disable timeout recovery function of the port.

spanning-tree errdisable-timeout disable: this command is used to disable the error-disable timeout recovery function of the port.

By default, the port error-disable timeout recovery function is enabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree errdisable-timeout enable
```

6.15 Port error-disable Recovery Interval

Command

```
spanning-tree errdisable-timeout interval <seconds>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<seconds>: the recover interval of error-disable, in the range <10-1000000>.

Description

spanning-tree errdisable-timeout interval: this command is used to configure the time interval for recovery after error-disable of the port .

no spanning-tree errdisable-timeout interval: The command to restore the port after error-disable is restored at the default interval. errdisable-timeout interval is 300 seconds by default.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree errdisable-timeout interval 400
```

6.16 Edge

Command

```
spanning-tree portfast
no spanning-tree portfast
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree portfast: this command is used to enable the portfast function of the port.

no spanning-tree portfast: this command is used to disable the portfast function.

By default, port portfast is disabled.

The portfast function is mainly used to connect terminals or servers and other devices, requiring fast convergence of the port. Portfast must be enabled if the port needs to use the portfast feature.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree portfast
```

6.17 BPDU Filter of Edge Port

Command

```
spanning-tree portfast bpdu-filter (enable | disable | default)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree portfast bpdu-filter: this command is used to configure the mode of the portfast bpdu-filter feature under the port, enable, disable, default respectively.

By default, the port portfast bpdu-filter is in default.

The portfast features (bpdu-filter and bpdu-guard) both need to be valid on the portfast port (see related command spanning-tree portfast). The portfast feature can be enabled in configure mode or under the port (see the relative commands under the port). There are only enable and disable two state in configure mode, while there are

enable, disable and default three states under the port. When the portfast feature configured under the port is default, the actual running portfast feature under the port will be the same as the global portfast feature. When the portfast feature configured of the port is enable or disable, the actual running portfast feature of the port will be consistent with the portfast feature configured on the port. Use the show spanning-tree interface command to view relative details.

By default, the global portfast bpdu-filter function is disabled.

The portfast function is mainly used to connect devices such as terminals or servers, which needs fast convergence ports, similar to edgeport. Portfast must be enabled if the port needs to use the portfast feature.

Bpdu-filter function is used for portfast port, after enabling it, the port will not send and receive bpdu messages.

bpdu-guard function is used for portfast port. Once enabled, when the port receives bpdu message, the port will change into error-disable state (shutdown), which can be restored by errdisable-timeout function.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree portfast bpdu-filter enable
```

6.18 BPDU Filter of Edge Port

Command

spanning-tree portfast bpdu-guard (enable | disable | default)

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree portfast bpdu-guard: this command is used to configure the modes of the portfast bpdu-guard feature of the port, they are enable, disable, default.

By default, the port portfast bpdu-guard is in default.

The portfast features (bpdu-filter and bpdu-guard) both need to be valid on the portfast port (see related command spanning-tree portfast). The portfast feature can be enabled in configure mode or under the port (see the relative commands under the port). There are only enable and disable two state in configure mode, while there are enable, disable and default three states under the port. When the portfast feature configured under the port is default, the actual running portfast feature under the port will be the same as the global portfast feature. When the portfast feature configured of the port is enable or disable, the actual running portfast feature of the port will be consistent with the portfast feature configured on the port. Use the show spanning-tree interface command to view relative details.

By default, the global portfast bpdu-filter function is disabled.

The portfast function is mainly used to connect devices such as terminals or servers, which needs fast convergence ports, similar to edgeport. Portfast must be enabled if the port needs to use the portfast feature.

Bpdu-filter function is used for portfast port, after enabling it, the port will not send and receive bpdu messages.

bpdu-guard function is used for portfast port. Once enabled, when the port receives bpdu message, the port will change into error-disable state (shutdown), which can be restored by errdisable-timeout function.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree portfast bpdu-guard enable
```

6.19 Automatical Switching Edge Port

Command

```
spanning-tree autoedge
no spanning-tree autoedge
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree autoedge: this command is used to configure ports to automatically switch to edge ports.

no spanning-tree autoedge: this command configures ports that cannot be automatically switched to non-edge ports.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree autoedge
```

6.20 Root Port Protection

Command

```
spanning-tree guard root
no spanning-tree guard root
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree guard root: this command is used to configure the root port protection function.

no spanning-tree guard root: this command configures the port to not enable root port protection.

By default, root port guard is not enabled.

guard root is a mandatory root protection that stops accidental (or illegal) switches becoming root Bridges in the network. When the guard root port (designated ports) is opened and receives better BPDU packets, the port will enter a Listening (STP) or discarding state (RSTP, MSTP).

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
```

```
Switch(config-ge8) #spanning-tree guard root
```

6.21 Port Spanning-tree Enablement

Command

```
spanning-tree (enable | disable)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

spanning-tree enable: this command is used to enable the spanning tree function of the port.

spanning-tree disable: this command is used to disable the spanning tree function of the port.

By default, the port spanning tree function is enabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config) #interface ge8
Switch(config-ge8) #spanning-tree enable
```

6.22 Port Hello-time

Command

```
spanning-tree hello-time <seconds>
no spanning-tree hello-time <seconds>
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<seconds> : hello-time, range is 1-10.

Description

spanning-tree hello-time: this command is used to configure the hello-time of the port.
no spanning-tree hello-time: this command is used to restore the hello-time of the port to its default value.

By default, the hello-time of the port is 2.

It is better to use global configuration commands for hello-time.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree hello-time 3
```

6.23 Port Connection Type

Command

```
spanning-tree link-type (auto | point-to-point | shared)
no spanning-tree link-type
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

Auto: automatically determines the connection type, point-to-point or shared, based on duplex mode.

Point-to-point: specifies the port type as point-to-point.

Shared: specifies the port type as shared.

Description

spanning-tree link-type: this command is used to modify the link type of the port.

no spanning-tree link-type: this command is used to restore the link type of the port to the default value.

By default, the link type of the port is auto.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree link-type point-to-point
```

6.24 Port Priority

Command

```
spanning-tree [instance <instance_id>] priority <priority>
no spanning-tree instance <instance_id> priority
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<instance-id> : represents the number of MSTI in the range 0-16.

<priority> : port priority, the range is 0-240.

Description

spanning-tree priority: this command is used to configure the port priority.

no spanning-tree priority: this command is used to restore the port priority to the default.

By default, the port priority is 128.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree priority 32
```

6.25 Cost

Command

```
spanning-tree [instance <instance_id>] path-cost <cost>
no spanning-tree instance <instance_id> path-cost
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<instance-id> : represents the number of MSTI in the range 0-16.

<cost> : means the cost value of the port, ranging from 1-200000000.

Description

spanning-tree path-cost: this command is used to configure the port cost.

no spanning-tree path-cost: this command is used to restore the port cost as the default.

By default, the port cost is 20000000.

When the port cost is the default value, the actual cost of link up port is converted according to the port rate, the rate of 10M corresponds to the cost of 2000000, and 100M corresponds to the cost of 200000.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree path-cost 1000
```

6.26 Port Restricted Election

Command

```
spanning-tree [instance <instance_id>] restricted-role
no spanning-tree instance <instance_id> restricted-role
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<instance-id> : the number of MSTI in the range 0-16.

Description

spanning-tree restricted-role: the command is used to configure ports to restrict elections so that ports cannot be elected as root ports.

no spanning-tree restricted-role: the command is used to cancel port restricted elections.

By default, the port does not restrict elections.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
```

```
Switch(config-ge8)#spanning-tree restricted-role
```

6.27 Port Restriction TC

Command

```
spanning-tree [instance <instance_id>] restricted-tcn  
no spanning-tree instance <instance_id> restricted-tcn
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<instance-id> : the number of MSTI in the range 0-16.

Description

spanning-tree restricted-tcn: the command is used to configure port restriction processing for receiving TC bits in BPDU message.

no spanning-tree restricted-tcn: the command is used to cancel the port restriction processing of the TC bit in the received BPDU message.

By default, no restriction on the port.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#interface ge8  
Switch(config-ge8)#spanning-tree restricted-tcn
```

6.28 Display Spanning-tree Detail Information

Command

```
show spanning-tree (interface IFNAME |)
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Interface IFNAME: displays state information of the specified port.

Description

show spanning-tree: this command is used to display the details of spanning-tree.

Instance

```
Switch#show spanning-tree
% Default: Bridge up - Spanning Tree Disabled
% Default: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit
Hold Count 6 - Max-hops 20
% Default: CIST Root Id 800000226f0100a3
% Default: CIST Reg Root Id 800000226f0100a3
% Default: CIST Bridge Id 800000226f0100a3
% 0: 0 topology change(s) - last topology change Thu Jan 1 08:00:00
1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
% gel: Port Number 1 - Ifindex 5001 - Port Id 8001 - Role Disabled
- State Discarding
% gel: Link down - Spanning Tree Disabled
% gel: Designated External Path Cost 0 -Internal Path Cost 0
% gel: Configured Path Cost 20000000 - Add type Explicit ref count
1
% gel: Designated Port Id 0 - CIST Priority 128 -
% gel: Message Age 0 - Max Age 0
% gel: CIST Hello Time 0 - Forward Delay 0
% gel: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 -
topo change timer 0
% gel: forward-transitions 0
% gel: Version MSTP - Received None - Send MSTP
% gel: Auto edge - On
% gel: Portfast - Off
% gel: Edge port - False
% gel: Bpdu Guard - Disabled (Config - default)
% gel: Bpdu filter - Disabled (Config - default)
% gel: Link Type - point-to-point (Config - auto)
% gel: Root Guard - Off
```


6.29 Display the Basic Information of the Spanning Tree

Command

```
show spanning-tree (instance <instance-id>|) brief
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

<*instance-id*> : the number of MSTI in the range 0-16.

Description

The show spanning-treebrief command is used to show information for spanning-tree.

Instance

```
Switch#show spanning-tree brief
MST  Port          Role          State
0    ge10          Designated   Forwarding
```

7 ERPS Configuration

7.1 Enter ERPS Instance Configuration View

Command

```
erps instance config
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

erps instance config: this command is used to enter the ERPS instance configuration view.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#erps instance config
```

7.2 Create ERPS Instance Name

Command

```
erps creat erps-name <NAME>  
no erps creat erps-name <NAME>
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name

Description

erps creat erps-name: the command is used to create an ERPS instance and specify the instance name.

By default, no configuration.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
```

7.3 ConfigureERPS Instance ID

Command

```
erps <NAME> set instanceID <instance>
no erps <NAME> set instanceID
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name

< instance > : MSTP instance number, the range is 0-16

Description

erps set instanceID: the command is used to configure the ERPS protection instance (configured by the spanning tree).

By default, no configuration.

Instance

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set instanceID 1
```

7.4 Specify the Ring Instance Corresponding to the ERPS Instance

Command

```
erps <NAME> set ring <NAME>
no erps <NAME> set ring
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name
< NAME > : ring instance name of ERPS

Description

erps set ring: this command is used to specify the ring instance corresponding to the ERPS instance (the ring instance is created and configured by the command in ring mode).

By default, no configuration.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set ring 1
```

7.5 Specify the Timer Instance Corresponding to the ERPS Instance

Command

```
erps <NAME> set timer <NAME>
no erps <NAME> set timer
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

< NAME > : timer instance name of ERPS.

Description

erps set ring: this command is used to specify the timer instance corresponding to the ERPS instance (the timer instance is created and configured by the command in ring mode).

By default, no configuration.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set timer 1
```

7.6 ERPS Instance Device Role

Command

```
erps <NAME> set role {rpl-owner|neighbor|interconnection|other}
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

Description

erps set role: this command is used to specify the role of the ERPS instance in the ring network.

By default, it is other.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set role rpl-owner
```

7.7 ERPS Instance Ring Role

Command

```
erps <NAME> set ring-role { major-ring| sub-ring}
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

Description

erps set ring-role: this command is used to specify the role of the ERPS instance in the ring network.

By default, it is a major-ring role.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set role-ring major-ring
```

7.8 Major Instance Name of ERPS Instance

Command

```
erps <NAME> set major-instance-name <NAME>
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS subinstance name.

< NAME >: ERPS major instance name.

Description

erps set majority-instance-name: this command is used to set the major instance of ERPS for the specified subinstance of ERPS, and is executed only if the specified instance of ERPS is a subring.

By default, no configuration.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set role-ring sub-ring
Switch(config-erps-instance)#erps 1 set major-instance-name 2
```

7.9 ERPS Instance Protocol Message Management VLAN

Command

```
erps <NAME> set raps-channel <vlan>
no erps <NAME> set raps-channel
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

< vlan > : VLAN of raps protocol message, the range is 1-4094.

Description

erps set raps-channel: this command is used to set the raps protocol message channel for the erps instance.

By default, it is 0 and invalid VLAN.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set raps-channel 10
```

7.10 ERPS InstanceVirtual Channel

Command

```
erps <NAME> set virtual-channel {enable|disable}
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

Description

erps set ring-role: this command is used to set whether raps protocol message are going through virtual channels (note: virtual channels are not currently supported). By default, it is default.

Instance

-

7.11 ERPS Instance Reverse Mode

Command

```
erps <NAME> set revertive {enable|disable}
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

Description

erps set revertive: command is used to configure the work mode of ERPS instance, enable is revertive mode and disable is irreversible mode.

By default, it is enable, that is reversible mode.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set revertive disable
```

7.12 ERPS Instance Force-switch or Manual-switch

Command

```
erps <NAME> command { force-Switch| manual-Switch}
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

Description

erps command: this command is used to perform forced or manual switch commands of ERPS instance.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 command force-Switch
```

7.13 ERPS Instance Clear Command

Command

```
erps <NAME> command clear
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

Description

erps command clear: this command is used to configure the ERPS instance to perform the clear command.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 command clear
```

7.14 ERPS Instance Enablement

Command

```
erps <NAME> {start|stop}
```

View

ERPS instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

Description

erps start|stop: this command is used to start or stop an ERPS instance.
By default, the ERPS instance is in the stop state.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 start
```

7.15 Enter Ring Instance Configuration View

Command

```
erps ring config
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

erps ring config: this command is used to enter the ERPS ring configuration view.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps ring config
```

7.16 Create Ring Instance Name

Command

```
ring creat ring-name <NAME> ring-id <ring-id>
no ring creat ring-name <NAME>
```

View

ERPS ring instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS ring name.

< ring-id > : ERPS ring ID, the range is 1-239.

Description

erps creat ring-name: this command is used to create the RING instance and specify the RING name and RING ID.

By default, no configuration.

RING ID will be the last byte of the MAC destination of the raps message.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps ring config
Switch(config-erps-ring)#ring creat ring-name 1 ring-id 1
```

7.17 Ring Instance Interface

Command

```
ring <NAME> set east-ifname <if-name> west-ifname <if-name>
```

View

ERPS ring instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

<if-name>: port name.

Description

ring set east-ifname: this command is used to configure the ring port for the specified ring instance.

By default, no configuration.

Note:

1. ERPS ring ports can be normal physical ports or static aggregation groups.
2. ERPS ring port cannot be opened at the same time with other layer 2 protocols (MSTP, SWRING, etc., when ERPS protection is not 0, it can be opened at the same time with MSTP).

Instance

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#erps ring config  
Switch(config-erps-instance)#ring creat ring-name 1  
Switch(config-erps-instance)#ring 1 set east-ifname ge1  
west-ifname ge2
```

7.18 Ring Instance Network Level

Command

```
ring <NAME> set ring-level <level>
```

View

ERPS ring instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name.

<level> : ring grade, the range is 1-7.

Description

erps set ring-level: this command is used to configure the RING level for the specified RING instance.

By default, the RING level is 1.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#erps ring config  
Switch(config-erps-ring)#ring creat ring-name 1  
Switch(config-erps-ring)#ring 1 set ring-level 2
```

7.19 Enter Timer Instance Configuration View

Command

```
erps timer config
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

erps timer config: this command is used to enter the ERPS timer configuration view.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
```

7.20 Create Timer Instance Name

Command

```
timer creat timer-name <NAME>
no timer creat timer-name <NAME>
```

View

ERPS Timer Instance Configuration View

Default Level

2: Configuration level

Parameters

< NAME >: ERPS timer instance name.

Description

timer creat timer-name: this command is used to create a timer instance and specify the timer instance name.

By default, no configuration.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps-time)#timer creat timer-name 1
```

7.21 WTB Timer

Command

```
timer <NAME> set wtb <interval>
```

View

ERPS timer instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS timer instance name.

<interval> : WTB timer value, the range is 1-12min.

Description

timer set wtb: this command is used to create the timing cycle of the TIMER instance WTB timer.

By default, it is 5min.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps- time)#timer 1 set wtb 1
```

7.22 WTR Timer

Command

```
timer <NAME> set wtr <interval>
```

View

ERPS timer instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS timer instance name.

<interval> : WTR timer value, the range is 1-12min.

Description

timer set wtr: this command is used to create the timing cycle of the timer instance WTR timer.

By default, it is 5min.

Instance

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps- time)#timer 1 set wtr 1
```

7.23 GuardTimer

Command

```
timer <NAME> set guard <interval>
```

View

ERPS timer instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS timer instance name.

<interval> : guard timer value, the range is 10-2000ms.

Description

timer set guard: this command is used to create the timing cycle of TIMER instance guard timer.

By default, it is 500ms.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps- time)#timer 1 set guard 1000
```

7.24 HoldTimer

Command

```
timer <NAME> set hold <interval>
```

View

ERPS timer instance configuration view

Default Level

2: Configuration level

Parameters

< NAME >: ERPS timer instance name.

<interval> : hold timer value, the range is 0-10s.

Description

timer set hold: this command is used to create the timing cycle of TIMER instance

hold timer.

By default, it is 0.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps- time)#timer 1 set hold 1
```

7.25 Display ERPS Instance Information

Command

```
show {erps <NAME>| erps-all}
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

< NAME >: ERPS instance name

Description

show erps: this command is used to display the ERPS instance information.

Instance

```
Switch#show erps 1

-----ERPS INSTANCE INFORMATION START-----
ERPS  Name:1                               ERPS Version:1
ERPS-STATE:ERPS_PROTECTION                 Device  Role:NEIGHBOR
InstanceID:0                               Channel Mode:NON-VRITUAL
ERPS  revert  mode:REVERTIVE
Major InstanceName:NULL
R-APS Vlan Channel:10
Data  Vlan Channel:NULL
WTR   Timer State:Stop
WTB   Timer State:Stop
Guard Timer State:Stop
```

```

Hold   Timer State:Stop
Hello  Timer State:Running
Instance Run State:Running
-----RING INSTANCE INFORMATION START-----
Ring Name:1
East Port:ge2      Port Role:OTHER-PORT      Port State:BLOCK
West Port:ge1      Port Role:RPL-NEIGHBOR-PORT  Port State:BLOCK
Ring   ID:1        Ring Level:1              Ring Role:Major Ring
-----RING INSTANCE INFORMATION END-----
-----TIMER INSTANCE INFORMATION START-----
Timer      Name:1
WTR   Timer Value:1 min
WTB   Timer Value:5 min
Guard  Timer Value:10 ms
Hold   Timer value:0 ms
Hello  Timer value:5 s
-----TIMER INSTANCE INFORMATION END-----
-----ERPS INSTANCE INFORMATION END-----

```

7.26 Display Ring Instance Information

Command

```
show erps {ring <NAME>| ring-all}
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

< NAME >: ERPS ring instance name.

Description

show erps ring: this command is used to display the ERPS ring instance information.

Instance

```

Switch#show erps ring 1
-----RING INSTANCE INFORMATION START-----
Ring Name:1
East Port:ge2      Port Role:OTHER-PORT      Port State:BLOCK
West Port:ge1      Port Role:RPL-NEIGHBOR-PORT  Port State:BLOCK
Ring   ID:1        Ring Level:1              Ring  Role:Major Ring

```

-----RING INSTANCE INFORMATION END-----

7.27 Display Timer Instance Information

Command

```
show erps {timer <NAME>| timer-all}
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

< NAME >: ERPS timer instance name.

Description

show erps timer: this command is used to display the instance information of the ERPS timer.

Instance

```
Switch#show erps timer 1
-----TIMER INSTANCE INFORMATION START-----
Timer      Name:1
WTR    Timer Value:1 min
WTB    Timer Value:5 min
Guard   Timer Value:10 ms
Hold    Timer value:0 ms
Hello   Timer value:5 s
-----TIMER INSTANCE INFORMATION END-----
```

8 Remote Loop Detection Configuration

GSTP means the remote loop detection function. Switch connect iwth the client, if the client network has a loop, it will affect the entire network. The GSTP is designed to solve this problem. After the switch port enabled the remote loop detection function, it will periodically broadcast and send detection messages. When the switch port enabled the remote loop detection function, it will periodically broadcast the detection message. If the client network has a loop, the switch will receive detection message sent by itself. The switch will regard client network has loop network and set the ports that connect with client port to discarding or shutdown according to processing strategy.

8.1 Enable Configuration

Command

```
loop-detect enable
no loop-detect enable
```

View

Configure Mode

Default Level

2. Configuration level

Parameters

-

Description

loop-detect enable: this command is used to enable loop-detect function.

no loop-detect enable: this command is used to disable loop-detect function.

Instance

```
Switch#configure terminal  
Switch(config)#loop-detect enable
```

8.2 Port Loopback Detection

Command

```
loop-detect force up  
loop-detect protect vlan <1-4094>  
loop-detect resume time <300-600>  
loop-detect tx-interval time <10-300>
```

View

Interface Mode

Default Level

2. Configuration level

Parameters

<1-4094> : VLAN ID and the range is 1-4094.

<300-600>: the recovery time of the port, ranging from 300-600 seconds.

<10-300> : probe packet detection interval, the range is 10-300 seconds.

Description

Loop-detect force up: force open the port closed by the protocol (this command does not save).

Loop-detect protect vlan <1-4094> : specify protection VLAN and enable port check.

loop-detect resume time <300-600>: Recovery port time.

loop-detect tx-interval time <10-300>:The time interval between sending probe packets.

Instance

```
Switch>enable  
Switch#configure terminal  
Switch(config)#interface ge1  
Switch(config-ge1)#loop-detect protect vlan 1
```

9 IGMP Configuration

9.1 IGMP Enablement

Command

```
ip igmp
no ip igmp
```

View

Vlan-if Ethernet port configuration mode

Default Level

2: Configuration level

Parameters

-

Description

Ip igmp: this command is used to enable IGMP on the interface.

no ip igmp: this command is used to disable IGMP on the interface.

By default, IGMP on the interface is disabled.

Only when IGMP is enabled on the interface can the configuration of other IGMP features on that interface take effect.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp
```

9.2 IGMP Version

Command

```
ip igmp version VERSION-NUMBER
no ip igmp version
```

View

Vlan-if Ethernet port configuration mode

Default Level

2: Configuration level

Parameters

version-number: means the version number of IGMP, with a value range of 1-3.

Description

ip igmp version: this command is used to configure the version of IGMP on the interface.

no ip igmp version: this command is used to restore the IGMP to the default value. By default, the version of IGMP is IGMPv3.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp version 2
```

9.3 The Times the IGMP Query Started

Command

```
ip igmp startup-query-count <2-10>
no ip igmp startup-query-count
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

<2-10> : specifies the number of times IGMP queries are started, with a value range of 2-10.

Description

ip igmp startup-query-count: this command is used to configure the times that the IGMP queries is started on the interface.

no ip igmp startup-query-count: this command is used to restore to the default value. By default, the number of starts of an IGMP querier is equal to the robustness of the IGMP querier.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp startup-query-count 5
```

9.4 Start Query Interval of IGMP Querier

Command

```
ip igmp startup-query-interval <1-18000>
no ip igmp startup-query-interval
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

<1-18000> : specifies the start query interval of the IGMP query, ranging from 1-18000 in seconds.

Description

ip igmp startup-query-interval: this command is used to configure the start query interval of the IGMP querier on the interface.

no ip igmp startup-query-interval: this command is used to restore to the default value. By default, the IGMP query starts at a query interval 1/4 of the time it takes to send IGMP universal group query messages. The interval of sending IGMP universal group query packet is 125 seconds, then the interval of launching IGMP querier is $125 \div 4 = 31$ (seconds).

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
```



```
Switch(config-vlanif1)#ip igmp startup-query-interval 20
```

9.5 The Robustness Factor of IGMP Querier

Command

```
ip igmp robustness-variable <2-7>  
no ip igmp robustness-variable
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

<2-7>: specifies the robustness of the IGMP query, ranging from 2 to 7. This coefficient is used to specify the default number of times the IGMP query sends the universal group query message at startup and the number of times the IGMP query sends the specific group query message after receiving the outgoing group message.

Description

ip igmp robustness-variable: this command is used to configure the robustness coefficient of the igmp query on the interface.

no ip igmp robustness-variable: this command is used to restore to the default value. By default, the robustness factor of IGMP querier is 2.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#interface vlanif1  
Switch(config-vlanif1)#ip igmp robustness-variable 3
```

9.6 IGMP Universal Group Query Message Time Interval

Command

```
ip igmp query-interval <1-1800>  
no ip igmp query-interval
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

<1-1800>: specifies the time interval for sending IGMP universal group query packet, ranging from 1 to 18000 in seconds.

Description

ip igmp query-interval: this command is used to configure the interval at which the igmp universal group query message is sent on the interface.

no ip igmp query-interval: this command is used to restore to the default value.

By default, the interval between sending IGMP universal group query packets is 125 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp query-interval 240
```

9.7 IGMP Lifetime of Other Queries

Command

```
ip igmp querier-timeout <60-300>
no ip igmp querier-timeout
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

<60-300>: specifies the duration of IGMP other querier, ranging from 60 to 300 seconds.

Description

ip igmp querier-timeout: this command is used to configure the duration of other igmp queries on the interface.

no ip igmp querier-timeout: this command is used to restore to the default value.

By default, the existence time of IGMP other queries = the interval between sending IGMP universal group query packets × the robustness coefficient of IGMP query + the maximum response time of IGMP universal group query ÷ 2.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp querier-timeout 180
```

9.8 Maximum Response Time of IGMP Universal Group Query Message

Command

```
ip igmp query-max-response-time <1-240>
no ip igmp query-max-response-time
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

<1-240>: specifies the maximum response time of IGMP universal group query message, ranging from 1 to 240 in seconds.

Description

ip igmp query-max-response-time: this command is used to configure the maximum response time for IGMP universal group queries on the interface.

No ip igmp query-max-response-time: this command is used to restore the default.

By default, the maximum response time for IGMP universal group query message is 10 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp query-max-response-time 20
```

9.9 The Number of IGMP Query Packets in a Particular Group

Command

```
ip igmp last-member-query-count <2-7>
no ip igmp last-member-query-count
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

<2-7>: specifies the number of sending query message a particular group of IGMP, with a value range of 2-7.

Description

ip igmp last-member-query-count: this command is used to configure the number of sending query message of IGMP specific groups on the interface.

no ip igmp last-member-query-count: command is used to restore to the default value. By default, the number of sending IGMP specific group query message is 2.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp last-member-query-count 3
```

9.10 Time Interval of IGMP Group Query Message

Command

```
ip igmp last-member-query-interval <1000-25500>
no ip igmp last-member-query-interval
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

<1000-25500>: specifies the time interval for sending IGMP specific group query message, ranging from 1000 to 25500 in milliseconds.

Description

ip igmp last-member-query-interval: the command is used to configure the interval at which the IGMP specific group query message is sent on the interface.

no ip igmp last-member-query-interval: the command is used to restore to the default value.

By default, the interval between sending IGMP specific group query message is 1000 milliseconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp last-member-query-interval 2000
```

9.11 IGMP Message with RA Option

Command

```
ip igmp ra-option
no ip igmp ra-option
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip igmp ra-option: the command is used to configure the dropping of igmp packets on the interface without the Router-Alert option.

no ip igmp ra-option: this command is used to restore the default value.

By default, the device does not check the Router-Alert option, which means that all received IGMP packets are sent to the upper protocol for processing, whether they carry the Router-Alert option.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp ra-option
```

9.12 Fast Aging ACL Group

Command

```
ip igmp immediate-leave group-list <ACL-NUMBER | ACL-NAME>
no ip igmp immediate-leave
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

acl-number: standard acl number, ranging from 1-99 or 1300-1999.

acl-name: extended acl name.

Description

ip igmp immediate-leave group-list: the command is used to configure the acl group address range of fast leave. The acl action must be permit.

no ip igmp immediate-leave: the command is used to restore to the default value.

By default, when the interface is working on version 2 and version 3, upon receiving the igmp leave message, a group-specific query message is sent to determine whether to age the multicast member table entry. Once this capability is configured, the multicast member table entry can be aged immediately if the group address specified by the acl is within the group address specified by the acl.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 1300 permit 225.1.1.0 0.0.0.255
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp immediate-leave group-list 1300
```

9.13 Illegal Multicast Group

Command

```
ip igmp access-group <ACL-NUMBER | ACL-NAME>
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

acl-number: standard acl number, the value range is 1 ~ -99.

acl-name: extended acl name.

Description

ip igmp access-group: this command is used to configure an invalid multicast group range. The action of the acl must be deny, and if the action is permit, mismatched multicast groups are considered legitimate.

no ip igmp access-group: the command is used to remove illegal multicast group range restrictions.

By default, there are no restrictions on the range of multicast groups that an interface can learn from.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 1300 deny 225.1.1.0 0.0.0.255
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp access-group 1300
```

9.14 Multicast Group Number Limit

Command

```
ip igmp limit VALUE [except <ACL-NUMBER | ACL-NAME > ]
no ip igmp limit
```

View

Configure Mode

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

Value: the maximum number of multicast groups allowed to be added by the global or interface, ranging from 1 to 1024.

acl-number: standard acl number, the value range is 1-99.

acl-name: extended acl name.

Description

ip igmp limit: this command is used to configure the maximum number of multicast groups that are allowed to be added to the global or interface.

no ip igmp limit: this command is used to restore to the default value. In the process of working, the device first determines whether it exceeds the global limit, then determines whether it exceeds the interface limit, or ignores the new multicast group learning.

An acl of type permit can be referenced by the except parameter, indicating that there are no restrictions on the number of multicast groups within the range specified by the acl.

By default, there is no limit to the number of multicast groups that can be added to a global or interface.



Notes

When the configured limit value is less than the number of established multicast groups on the global or current interface, the system will not automatically delete the additional multicast groups.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip igmp limit 1000
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp limit 100
```


9.15 IGMP Message Source Address and Receive Interface Subnet Restrictions

Command

```
ip igmp offlink
no ip igmp offlink
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip igmp offlink: this command is used to remove the restriction that the source address of an igmp message must be in the same subnet as the receiving interface, except for querying message and leaving message.

no ip igmp offlink: this command is used to restore to the default value.

By default, the source address of an igmp message must be on the same subnet as the receiving interface. Once the restriction is removed, the source address of the message will be considered valid as long as it passes RPF check.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp offlink
```

9.16 Static Multicast

Command

```
ip igmp static-group <group-address> [ source <source-address> |
ssm-map ]
no ip igmp static-group <group-address> [ source <source-address>
| ssm-map ]
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

Group-address: specify the address of the multicast group, ranging from 224.0.1.0 to 239.255.255.255.

Source-address: specifies the address of the multicast source.

Ssm-map: obtain the address of multicast source by ssm-mapping function

Description

ip igmp static-group: this command is used to configure the interface to statically join a multicast group or multicast source group.

no ip igmp static-group: this command is used to restore to the default value. By default, the interface does not statically add any multicast groups or multicast source groups.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp static 225.1.1.1 source
192.168.1.10
```

9.17 Global IGMP SSM Mapping Enablement

Command

```
ip igmp ssm-map enable
no ip igmp ssm-map enable
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

ip igmp ssm-map enable: this command is used to enable the IGMP SSM Mapping function globally.

no ip igmp ssm-map enable: this command is used to disable the global IGMP SSM Mapping function.

By default, the IGMP SSM Mapping function is disabled.

Because IGMPv1/IGMPv2 cannot specify multicast source in the report message, it is necessary to have compatibility with IGMP SSM Mapping technology. This feature provides SSM services for the interface that receives version1 and version2 igmp report packets, with the source address specified by the `ip igmp ssm-map static` command.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip igmp ssm-map enable
```

9.18 IGMP SSM-Map Static Multicast

Command

```
ip igmp ssm-map static <ACL-NUMBER | ACL-NAME> <SOURCE-ADDRESS>
no ip igmp ssm-map static <ACL-NUMBER | ACL-NAME> <SOURCE-ADDRESS>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

acl-number: standard acl number, ranging from 1 ~ 99 or 1300 ~ 1999.

acl-name: extended acl name.

Source-address: the static mapping source address for SSM mapping.

Description

`ip igmp ssm-map static`: this command is used to configure the IGMP SSM Mapping rule.

`no ip igmp ssm-map`: this command is used to delete the IGMP SSM Mapping rule. IGMP SSM Mapping rules are not configured by default.

Because IGMPv1/IGMPv2 cannot specify multicast source in the report message, it is necessary to have compatibility with IGMP SSM Mapping technology. This feature needs to work with `ip igmp ssm-map enable`.

Instance

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#access-list 1300 deny 225.1.1.0 0.0.0.255
Switch(config)#ip igmp ssm-map enable
Switch(config)#ip igmp ssm-map static 1300 192.168.1.10
```

9.19 Display IGMP Multicast Information

Command

```
show ip igmp groups [<IFNAME> | <GROUP-ADDRESS> | detail ]
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

ifname: vlanif interface.

group-address: ipv4 multicast address.

detail: outputs the details of the multicast group

Description

View the operation of the specified parameter or all the multicast groups.

Instance

```
Switch#show ip igmp groups detail
IGMP Connected Group Membership, Total is 1
Interface:      vlanif1
Group:          255.1.1.1
Uptime:         01:09:31
Group mode:     Exclude (Expires: 00:03:56)
Last reporter:  192.168.1.11
Source list is empty
```

9.20 Display IGMP Interface Information

Command

```
show ip igmp interface <IFNAME>
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Ifname: vlanif interface

Description

View the configuration and operation of the interface with the specified parameters or all igmp enabled.

Instance

```
Switch#show ip igmp interface vlanif1
Interface vlanif1 (Index 3)
  IGMP Enabled, Active, Querier, Configured for version 2
  L3 mcast is not enabled on this interface
  Internet address is 192.168.1.254
  IGMP interface has 1 group-record states
  IGMP activity: 54 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP Startup query interval is 31 seconds
  IGMP Startup query count is 2
  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 Last member query count is 2
  L2 mcast is not enabled on this interface
  IGMP Snooping is globally disabled
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
```

10 IGMP Snooping Configuration

10.1 IGMP Snooping Enablement

Command

```
ip igmp snooping
no ip igmp snooping
```

View

Configure Mode
VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip igmp snooping: this command is used to enable IGMP snooping on global or VLAN interfaces.

no ip igmp snooping: this command is used to disable igmp snooping on the global or VLAN interface.

IGMP snooping is disabled by default on the global or VLAN interfaces.



Notes

Only when IGMP snooping is enabled on the global and VLAN interfaces can the configuration of the other IGMP snooping properties on that interface take effect.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp snooping
```

10.2 IGMP SnoopingQuerier Enablement

Command

```
ip igmp snooping querier
no ip igmp snooping querier
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip igmp snooping querier: this command is used to enable IGMP Snooping querier.
no ip igmp snooping querier: this command is used to disable IGMP Snooping querier.
By default, the IGMP Snooping querier is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp snooping querier
```

10.3 IGMP Snooping Port Fast-leave Enablement

Command

```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip igmp-snooping fast-leave: this command is used to enable the fast leave function on all ports of the VLAN interface. Port fast leave means that when the switch receives the IGMP leaving a multicast group message sent by the host from a port, the port is directly deleted from the list of outgoing ports of the corresponding forwarding item.

no ip igmp-snooping fast-leave: this command is used to disable the fast leave function on all ports of the VLAN interface.

By default, the fast leave function of the port is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp snooping fast-leave
```

10.4 IGMP SnoopingPort Suppression Enablement

Command

```
ip igmp snooping report-suppresstion
no ip igmp snooping report-suppresstion
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip igmp snooping report-suppresstion: this command is used to enable port reporting suppression on all ports of the VLAN interface. When the port is in IGMPv1 or IGMPv2, when receiving the leave message, if the port report suppression function is enabled, the report message will not be sent.

no ip igmp-snooping report-suppression command: this command is used to disable port reporting suppression on all ports of the VLAN interface.

By default, port report suppression is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp snooping report-suppression
```

10.5 Display the IGMP Snooping Multicast Group Routing Interface

Command

```
show ip igmp snooping mrouter interface <IFNAME>
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Ifname: vlanif interface

Description

View the multicast group routing port of the specified interface

Instance

```
Switch#show ip igmp snooping mrouter interface vlanif1
VLAN      interface
1          ge2
```

10.6 Display IGMP Snooping Multicast Statistics

Command

```
show ip igmp snooping statistics interface <IFNAME>
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Ifname: vlanif interface

Description

View the multicast group statistics of the specified interface

Instance

-

11 GMRP and MMRP Configuration

As a carrier of an Attribute Registration Protocol, GARP (Generic Attribute Registration Protocol) can be used to propagate attributes. Application entities that follow the GARP protocol are called GARP applications, GMRP(GARP Multicast Registration Protocol) is one of the applications of the generic property Registration Protocol (GARP) to provide a limited Multicast diffusion capability similar to IGMP probe technology.

As the carrier of an attribute registration protocol, MRP (Multiple Register Protocol) can be used to propagate attribute messages. The application entity following MRP Protocol is called MRP application. MVRP (Multiple VLAN Register Protocol) is one of the applications of MRP. MRP, MVRP and MMRP are the upgraded versions of GARP (Generic Attribute Registration Protocol), GVRP (GARP VLAN Registration Protocol) and GMRP(GARP Multicast Registration Protocol) respectively, which improve the efficiency of Attribute declaration. Used to replace GARP, GVRP, GMRP protocol. MVRP is used to publish and learn VLAN configuration information between devices, so that devices can automatically synchronize VLAN configuration and reduce the configuration work of network administrators. After the network topology changes, MVRP reissues and learns the VLAN according to the new topology, so as to update the network topology synchronously in real time.

11.1 GlobalGMRP or MMRP Enablement

Command

```
(gmrp | mmrp) (enable | disable)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

(gmrp | mmrp) enable: this command is used to enable the global GMRP (MMRP) function.

(gmrp | mmrp) disable: this command is used to disable the global GMRP (MMRP) function.

By default, the global GMRP (MMRP) is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gmrp enable
```

11.2 Port GMRP or MMRP Enablement

Command

(gmrp | mmrp) (enable | disable)

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

port (gmrp | mmrp) enable: this command is used to enable the GMRP (MMRP) function of the port.

port (gmrp | mmrp) disable: this command is used to disable the GMRP (MMRP) function of the port.

By default, the GMRP (MMRP) function of the port is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gmrp enable
```

```
Switch(config)#interface ge5
Switch(config-ge5)#gmrp enable
```

11.3 GMRP or MMRP Registration Mode

Command

```
(gmrp | mmrp) registration (fixed| forbidden | normal | restricted)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

fixed: Fixed mode.

forbidden: Forbidden mode.

normal: Normal mode, allowing registering and deregistering multicast dynamically.

restricted: Restricted mode.

Description

(gmrp | mmrp) registration: this command is used for GMRP port registration mode.

By default, the GMRP port registration mode is normal.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gmrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gmrp registration normal
```

11.4 GMRP or MMRP Timer

Command

```
(gmrp | mmrp) timer (join| leave| leaveall) <TIMER_VALUE>
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

leaveall | join | leave: represent leave All, join and leave three timers respectively.

After GARP is started on each port and LeaveAll timer is started at the same time, the port will send LeaveAll messages to the outer loop to cause the other ports to re-register all their property information. GARP port can send out each Join packet twice to ensure the reliable transmission of message, and the time interval between the two times is controlled by Join timer. The GARP port that receives the Leave packet enable the Leave timer, and if the Join packet is not received before the timer timeout, the corresponding attribute information will be logged out.

<TIMER_VALUE> : timer value, leave All defaults to 1000; The default value for join is 20; The default value for leave is 60. Unit: centiseconds.

Description

(gmrp | mmrp) timer: this command is used to configure leave All, join, and leave timers of the GARP ports.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gmrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gmrp timer leave 100
```

11.5 Display GMRP or MMRP Configuration Information

Command

```
show (gmrp | mmrp) configuration
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show gmrp | mmrp configuration: this command is used to display GMP| MMRP configuration information.

Instance

*Switch#show gmrp configuration

11.6 Display GMRP or MMRP State Machine Information

Command

show (gmrp | mmrp) machine

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show gmrp | mmrp machine command: this command is used to display GMRP|MMRP state machine information.

Instance

Switch> enable

Switch#show gmrp machine

11.7 Display GMRP or MMRP Message Statistics

Command

show (gmrp | mmrp) statistics vlanid [<VLANID>]

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

vlanid: VLAN ID.

Description

show gmrp | mmrp statistics: this command is used to display GMRP| MMRP message statistics.

Instance

```
Switch> enable
Switch#show gmrp statistics vlanid 3
```

11.8 Display GMRP or MMRP Timer Information

Command

```
show (gmrp | mmrp) timer <IFNAME>
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

lname: port name.

Description

show gmrp | mmrp timer: this command is used to display the GMRP| MMRP port timer information.

Instance

```
Switch> enable
Switch#show gmrp timer ge2
```


12 GVRP and MVRP Configuration

As a carrier of an Attribute Registration Protocol, GARP (Generic Attribute Registration Protocol) can be used to propagate attributes. Application entities that follow the GARP protocol are called GARP applications. GVRP (GARP VLAN Registration Protocol) is one of the applications of the common property Registration Protocol (GARP) for VLAN properties login and logout.

As the carrier of an attribute registration protocol, MRP (Multiple Register Protocol) can be used to propagate attribute messages. The application entity following MRP Protocol is called MRP application. MVRP (Multiple VLAN Register Protocol) is one of the applications of MRP. MRP, MVRP and MMRP are the upgraded versions of GARP (Generic Attribute Registration Protocol), GVRP (GARP VLAN Registration Protocol) and GMRP (GARP Multicast Registration Protocol) respectively, which improve the efficiency of Attribute declaration. Used to replace GARP, GVRP, GMRP protocol. MVRP is used to publish and learn VLAN configuration information between devices, so that devices can automatically synchronize VLAN configuration and reduce the configuration work of network administrators. After the network topology changes, MVRP reissues and learns the VLAN according to the new topology, so as to update the network topology synchronously in real time.

12.1 GVRP or MVRP Enablement

Command

```
(gvrp | mvrp) (enable | disable)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

(gvrp | mvrp) enable: this command is used to enable the global GVRP (MVRP) function.

(gvrp | mvrp) disable: this command is used to disable the global GVRP (MVRP) function.

By default, the global GVRP (MVRP) function is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
```

12.2 GVRP or MVRP Dynamic VLAN Enablement

Command

(gvrp | mvrp) dynamic-vlan-creation (enable | disable)

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

(gvrp | mvrp) dynamic-vlan-creation enable: this command is used to enable the dynamic creation of VLAN functions.

(gvrp | mvrp) dynamic-vlan-creation disable: this command is used to disable the dynamic creation of VLAN functions.

By default, the dynamic creation VLAN feature is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
Switch(config)#gvrp dynamic-vlan-creation enable
```

12.3 Port GVRP or MVRP Enablement

Command

(gvrp | mvrp) (enable | disable)

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

port (gvrp | mvrp) enable: this command is used to enable port GVRP (MVRP) function.

port (gvrp | mvrp) disable: this command is used to disable the GVRP (MVRP) function.

By default, the GVRP (MVRP) function of the port is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
Switch(config)#gvrp dynamic-vlan-creation enable
Switch(config)#interface ge5
Switch(config-ge5)#gvrp enable
```

12.4 GVRP or MVRP Registration Mode

Command

(gvrp | mvrp) registration (fixed| forbidden | normal)

View

Interface Mode

Default Level

2: Configuration level

Parameters

fixed: Fixed mode, no dynamic VLAN registration on the port, only static VLAN declaration messages are sent.

forbidden: Forbidden mode, does not allow dynamic VLAN to register on the port, simultaneously deletes all VLANs except VLAN 1 on the port, only sends VLAN 1 declaration message.

Normal: normal mode, which allows dynamic VLANs to be registered on the port and simultaneously sends both static and dynamic VLAN declaration messages.

Description

(gvrp | mvrp) registration: this command is used for the GVRP port registration mode. By default, the GVRP port registration mode is normal.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gvrp registration normal
```

12.5 GVRP or MVRP Timer

Command

```
(gvrp | mvrp) timer (join| leave| leaveall) <TIMER_VALUE>
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

leaveall | join | leave: represent leave All, join and leave three timers respectively.

After GARP is started on each port and LeaveAll timer is started at the same time, the port will send LeaveAll messages to the outer loop to cause the other ports to re-register all their property information. GARP port can send out each Join packet twice to ensure the reliable transmission of message, and the time interval between the two times is controlled by Join timer. The GARP port that receives the Leave packet enable the Leave timer, and if the Join packet is not received before the timer timeout, the corresponding attribute information will be logged out.

<TIMER_VALUE> : timer value, leave All defaults to 1000; The default value for join is 20; The default value for leave is 60. Unit: centiseconds.

Description

(gvrp | mvrp) timer: this command is used to configure leave All, join, and leave timers of the GARP ports.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gvrp timer join 10
```

12.6 Display Dynamic VLAN Information

Command

```
show vlan dynamic
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show vlan dynamic: this command is used to display dynamic vlan information.

Instance

```
Switch> enable
Switch#show vlan dynamic
```

12.7 Display GVRP or MVRP Configuration Information

Command

```
show (gvrp | mvrp) configuration
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show gvrp | mvrp configuration: this command is used to display GVRP| MVRP configuration information.

Instance

Switch> **enable**

Switch#**show gvrp configuration**

12.8 Display GVRP or MVRP State Machine Information

Command

show (gvrp | mvrp) machine

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show gvrp | mvrp machine: this command is used to display GVRP| MVRP state machine information.

Instance

Switch> **enable**

Switch#**show mvrp machine**

12.9 Display GVRP or MVRP Message Statistics

Command

```
show (gvrp | mvrp) statistics [<IFNAME>]
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

lname: port name.

Description

show gvrp | mvrp statistics: this command is used to display GVRP| MVRP message statistics.

Instance

```
Switch> enable
```

```
Switch#show mvrp statistics
```

12.10 Display GVRP or MVRP Timer Information

Command

```
show (gvrp | mvrp) timer <IFNAME>
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

lname: port name.

Description

show gvrp | mvrp timer: this command is used to display timer information of GVRP| MVRP port .

Instance

```
Switch> enable
```

```
Switch#show mvrp time ge1
```

13 PIM-DM Configuration

13.1 PIM-DM Enablement

Command

```
ip pim dense-mode
no ip pim dense-mode
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip pim dense-mode: this command is used to enable the PIM-DM.

no ip pim dense-mode: this command is used to disable the PIM-DM.

By default, the PIM-DM is disabled.



Notes

- this command will only take effect when IP multicast routing is enabled globally.
 - For relative configuration, refer to the command ip multicast-routing.
-

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim dense-mode
```


13.2 PIM-DM DR Priority

Command

```
ip pim dense-mode dr-priority PRIORITY
no ip pim dense-mode dr-priority
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

PRIORITY: specify the priority of the election DR, and the value range is 0 ~ 4294967294. The higher the value, the higher the priority.

Description

ip pim dense-mode dr-priority: this command is used to configure the priority of the election DR on the interface.

no ip pim dense-mode dr-priority: this command is used to restore to the default value. By default, the priority of election DR is 1.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim dense-mode dr-priority 10
```

13.3 PIM-DM GenID Information

Command

```
ip pim dense-mode exclude-genid
no ip pim dense-mode exclude-genid
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip pim dense-mode exclude-genid: this command is used to configure the interface to send hello message without genID information.

The no ip pim dense-mode exclude-genid: this command is used to restore to the default value.

By default, the hello message sent from the interface is with GenID information.

GenID is a random value at the initial creation of the interface to identify unique interface information. With this information, device can detect whether the neighbor device has been restarted.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim dense-mode exclude-genid
```

13.4 PIM-DM Neighbor Reachable State Time

Command

```
ip pim dense-mode hello-holdtime TIME
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

TIME: specifies the time to maintain the reachable state of PIM neighbors, and the value range is 1 ~ 65535, in seconds. If specify 65535 seconds, the PIM neighbors are always reachable.

Description

ip pim dense-mode hello-holdtime: this command is used to configure the time on the interface to maintain the reachable state of the pim neighbors.

no ip pim dense-mode hello-holdtime: this command is used to restore to the default value.

By default, the PIM neighborhood reachable time is 105 seconds.

Instance

```
Switch> enable
```

```
Switch#configure terminal  
Switch(config)#interface vlanif1  
Switch(config-vlanif1)#ip pim dense-mode hello-holdtime 150
```

13.5 Time Interval of PIM-DM Hello Message

Command

```
ip pim dense-mode hello-interval INTERVAL  
no ip pim dense-mode hello-interval
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

INTERVAL: specifies the time interval for sending Hello message, ranging from 1 to 65535 in seconds.

Description

ip pim dense-mode hello-interval: this command is used to configure the time interval between Hello messages on the interface.

no ip pim dense-mode hello-interval: this command is used to restore to the default value.

By default, the interval for sending Hello message is 30 seconds.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#interface vlanif1  
Switch(config-vlanif1)#ip pim dense-mode hello-interval 60
```

13.6 PIM-DM Neighbor Filter

Command

```
ip pim dense-mode neighbor-filter <ACL-NUMBER | ACL-NAME>  
no ip pim dense-mode neighbor-filter
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

ACL-NUMBER: standard acl number, the value range is 1-99.

ACL-NAME: extended acl name.

Description

ip pim dense-mode neighbor-filter: this command is used to configure the illegal neighbor source address range, acl action must be deny, if the action is permit, it will not match even considered to be a legitimate neighbor.

no ip pim dense-mode neighbor-filter: this command used to cancel the configuration of the illegal neighbor source address range.

By default, there are no restrictions on the neighbor source addresses that an interface can learn from.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 20 deny 192.168.1.0 0.0.0.255
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim dense-mode neighbor-filter 20
```

13.7 IPM-DM SRM Message Enablement

Command

```
ip pim dense-mode state-refresh
no ip pim dense-mode state-refresh
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

ip pim dense-mode state-refresh: this command is used for global configuration to enable the sending of SRM messages.

no ip pim dense-mode state-refresh: this command is used to cancel the restore configuration.

By default, enable sending SRM messages globally.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#no ip pim dense-mode state-refresh
```

13.8 Time Interval of Sending PIM-DM SRM Message

Command

```
ip pim dense-mode state-refresh origination-interval < VALUE >
no ip pim dense-mode state-refresh origination-interval
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

VALUE: time interval to send SRM, ranging from 1 to -100, in seconds.

Description

ip pim dense-mode state-refresh origination-interval: this command is used to set the time interval between sending SRM messages globally.

no ip pim dense-mode state-refresh origination-interval: this command is used to restore to the default value.

By default, the interval for sending SRM message is 60 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim dense-mode state-refresh
origination-interval 30
```

13.9 Time Interval for PIM-DM to Receive SRM message

Command

```
ip pim dense-mode state-refresh rate limit-interval < VALUE >  
no ip pim dense-mode state-refresh rate limit-interval
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

VALUE: time interval to receive SRM message, ranging from 1 to 100, the unit is in seconds/piece.

Description

ip pim dense-mode state-refresh rate limit-interval: this command is used to set the time interval for receiving SRM messages globally.

no ip pim dense-mode state-refresh rate limit-interval: this command is used to restore to the default value.

By default, the interval for receiving SRM message is 30 seconds/piece.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#ip pim dense-mode state-refresh rate  
limit-interval 60
```

13.10 Display PIM-DM Interface Information

Command

```
show ip pim dense-mode interface [ <IFNAME> | detail ]
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

ifname: specify vlanif interface.

Detail: specify to view details.

Description

This command is used to view PIM information on the interface.

Instance

```
Switch#show ip pim dense-mode interface
```

Address	Interface	VIFindex	Ver/ Mode	Count	Nbr Prior	DR	DR
10.3.101.252	vlanif10	0	v2/S	1	1		
10.3.101.253							
11.1.1.2	vlanif11	2	v2/S	1	1	11.1.1.3	
172.24.0.2	vlanif50	3	v2/S	1	1	172.24.0.3	

```
Switch#show ip pim dense-mode interface detail
```

```
vlanif10 (vif 0):
```

```
Address 10.3.101.252, DR 10.3.101.253
```

```
Hello period 30 seconds, Next Hello in 2 seconds
```

```
Triggered Hello period 5 seconds
```

```
Neighbors:
```

```
10.3.101.253
```

```
vlanif11 (vif 2):
```

```
Address 11.1.1.2, DR 11.1.1.3
```

```
Hello period 30 seconds, Next Hello in 2 seconds
```

```
Triggered Hello period 5 seconds
```

```
Secondary addresses:
```

```
11.1.1.1
```

```
Neighbors:
```

```
11.1.1.3
```

```
vlanif50 (vif 3):
```

```
Address 172.24.0.2, DR 172.24.0.3
```

```
Hello period 30 seconds, Next Hello in 3 seconds
```

```
Triggered Hello period 5 seconds
```

```
Neighbors:
```

```
172.24.0.3
```

13.11 View the Local Multicast Group Members of PIM-DM

Command

```
show ip pim dense-mode local-members [<IFNAME> ]
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

IFNAME: specify vlanif interface

Description

View the local multicast group members of PIM-DM of the current device.

Instance

```
Switch#show ip pim dense-mode local-members vlanif10
PIM Local membership information
vlanif10:
  (*, 225.2.2.2) : Include
```

13.12 Displays the PIM-DM Multicast Routing Table Entry

Command

```
show ip pim dense-mode mroute [ detail ]
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Detail: specify to view details.

Description

View the current PIM-DM multicast routing table entry.

Instance

-

13.13 Display PIM-DM Neighbor Information

Command

```
show ip pim dense-mode neighbor [ detail ]
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Detail: specify to view details.

Description

View the currently learning PIM-DM neighborhood running status.

Instance

```
Switch#show ip pim dense-mode neighbor
Neighbor      Interface      Uptime/Expires  Ver  DR
Address                               Priority/Mode
10.3.101.253   vlanif10        01:53:56/00:01:17  v2   1 /
DR
11.1.1.3       vlanif11        01:53:57/00:01:18  v2   1 / DR
172.24.0.3     vlanif50        01:53:56/00:01:17  v2   1 / DR
```

13.14 Displays PIM-DM Next Hop Information

Command

```
show ip pim dense-mode nexhop
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

View the next hop information used by the PIM-DM module in the current device.

Instance

```
Switch#show ip pim dense-mode nexthop
```

Flags: N = New, R = RP, S = Source, U = Unreachable

Destination	Type	Nexthop	Nexthop	Nexthop	Nexthop	Metric
Pref	Refcnt					

		Num	Addr	Ifindex	Name	

10.3.101.111	..S.	1	0.0.0.0	4		0
0	2					

14 PIM-SM Configuration

14.1 PIM-SM Enablement

Command

```
ip pim sparse-mode
no ip pim sparse-mode
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip pim sparse-mode: this command is used to enable the PIM-SM.

no ip pim sparse-mode: this command is used to disable the PIM-SM.

By default, the PIM-SM is disabled.



Notes

- This command will only take effect when IP multicast routing is enabled globally.
 - For relative configuration, refer to the command `ip multicast-routing`.
-

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim sparse-mode
```

14.2 PIM-SM DR Priority

Command

```
ip pim sparse-mode dr-priority PRIORITY
no ip pim sparse-mode dr-priority
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

PRIORITY: specify the priority of the election DR, and the value range is 0 ~ 4294967294. The higher the value, the higher the priority.

Description

ip pim sparse-mode dr-priority: this command is used to configure the priority of the election DR on the interface.

no ip pim sparse-mode dr-priority: this command is used to restore to the default value.

By default, the priority of election DR is 1.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim sparse-mode dr-priority 10
```

14.3 PIM-SM GenID Information

Command

```
ip pim sparse-mode exclude-genid
no ip pim sparse-mode exclude-genid
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip pim sparse-mode exclude-genid: this command is used to configure the interface to send hello message without GenID information.

no ip pim sparse-mode dr-priority: this command is used to restore to the default value.

By default, the hello message sent from the interface is with GenID information.

GenID is a random value at the initial creation of the interface to identify unique interface information. With this information, device can detect whether the neighbor device has been restarted.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface vlanif1
```

```
Switch(config-vlanif1)#ip pim sparse-mode exclude-genid
```

14.4 PIM-SM Neighbor Reachable State Time

Command

```
ip pim sparse-mode hello-holdtime TIME
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

TIME: specifies the time to maintain the reachable state of PIM neighbors, and the value range is 1 ~ 65535, in seconds. If specify 65535 seconds, the PIM neighbors are always reachable.

Description

ip pim sparse-mode hello-holdtime: this command is used to configure the time on the interface to maintain the reachable state of the pim neighbors.

no ip pim sparse-mode hello-holdtime: this command is used to restore to the default value.

By default, the PIM neighborhood reachable time is 105 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim sparse-mode hello-holdtime 150
```

14.5 Time Interval of PIM-SM Hello Message

Command

```
ip pim sparse-mode hello-interval INTERVAL
no ip pim sparse-mode hello-interval
```

View

VLAN-IF Interface Configuration View

Default Level

2: Configuration level

Parameters

INTERVAL: specifies the time interval for sending Hello message, ranging from 1 to 65535 in seconds.

Description

ip pim sparse-mode hello-interval: this command is used to configure the time interval between sending hello messages on the interface.

no ip pim sparse-mode hello-interval: this command is used to restore to the default value.

By default, the interval for sending Hello message is 30 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim sparse-mode hello-interval 60
```

14.6 PIM-SM Neighbor Filter

Command

```
ip pim sparse-mode neighbor-filter <ACL-NUMBER | ACL-NAME>
no ip pim sparse-mode neighbor-filter
```

View

Vlan-if Ethernet port configuration mode

Default Level

2: Configuration level

Parameters

ACL-NUMBER: standard acl number, the value range is 1-99.

ACL-NAME: extended acl name.

Description

ip pim sparse-mode neighbor-filter: this command is used to configure the illegal neighbor source address range, acl action must be deny, if the action is permit, it will be considered to be a legitimate neighbor even it doesn't match.

no ip pim sparse-mode neighbor-filter: this command is used to cancel the configuration of the illegal neighbor source address range.

By default, there are no restrictions on the neighbor source addresses that an interface can learn from.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 20 deny 192.168.1.0 0.0.0.255
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim sparse-mode neighbor-filter 20
```

14.7 PIM-SM Illegal Registration Message Restriction

Command

```
ip pim accept-register list <ACL-NUMBER | ACL-NAME>
no ip pim accept-register
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

ACL-NUMBER: standard acl number, ranging from 1 ~ 99 and 2000 ~ 2699.

ACL-NAME: extended acl name.

Description

ip pim accept-register: this command is used to configure the source address range of illegal registration packets. The action of acl must be deny, and the register-stop packet will be sent immediately after matching. If it is any other action type, it is considered to be the legitimate source address.

no IP pim accept-register: this command is used to cancel the configuration of the source address range of an invalid registration message.

By default, there is no restriction on the source address of registered message that the interface can learn from.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 20 deny 192.168.1.0 0.0.0.255
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip pim accept-register 20
```

14.8 PIM C-BSR

Command

```
ip pim bsr-candidate <IFNAME> [ hash-mask-length <HASH-LEN> |
priority <PRI> ]
no ip pim bsr-candidate <IFNAME> [ hash-mask-length <HASH-LEN> |
priority <PRI> ]
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

IFNAME: specify C- BSR vlanif interface.

HASH-LEN: specifies the length of the hash mask, with a value range of 0 ~ 32.

PRI: specifies the priority of C-BSR, with values ranging from 0 to 255. The higher the value, the higher the priority.

Description

ip pim bsr-candiat: this command is used to configure an interface as C-BSR.

no ip pim bsr-candiat: this command is used to cancel the relevant configuration of C-BSR.

By default, C-BSR is not configured.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim bsr-candidate vlanif1 hash-mask-length 20
priority 20
```

14.9 PIM Registered Message Validation and Compatibility with Cisco Standard

Command

```
ip pim cisco-register-checksum [ group-list <ACL-NUMBER |
ACL-NAME> ]
no ip pim cisco-register-checksum [ group-list <ACL-NUMBER |
ACL-NAME> ]
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

ACL-NUMBER: standard acl number, ranging from 1 ~ 99 and 1300 ~ 1999.

ACL-NAME: extended acl name.

Description

ip pim cisco-register-checksum: this command is used to configure and calculate the verification and compatibility of registered packet with CISCO standard, that is, including the whole PIM message, the ACL can be applied to specify the group address range, the action of ACL must be permit, if no ACL is specified, it means that all multicast groups need to be compatible with CISCO standard.

no ip pim cisco-register-checksum: this command is used to cancel the configure the calculation of the check and compatibility of registered packets with the CISCO standard.

By default, calculating the checksum of registered packets only includes 8 bytes of PIM headers.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim cisco-register-checksum
```

14.10 PIM C-RP Compatibility with Cisco Standard

Command

```
ip pim crp-cisco-prefix
no ip pim crp-cisco-prefix
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

ip pim crp-cisco-prefix: this command is used to keep BSR communication with the CISCO device when as C-RP.

no ip pim crp-cisco-prefix: this command is used to restore the default configuration. By default, this function is not enabled.

If the BSR of CISCO equipment is not compatible with Prefix Count when it equals to 0 in some versions, after this feature is enabled, if CRP uses the default Group Range, the Prefix Count in CRP-Adv message should be set to 1, and the Group Range use 224.0.0.0/4.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim crp-cisco-prefix
```

14.11 PIM BSR C-RP Priority Ignorance

Command

```
ip pim ignore-rp-set-priority
no ip pim ignore-rp-set-priority
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

ip pim ignore-rp-set-priority: this command is used to select RP for BSR to ignore the priority of CRP.

no ip pim ignore-rp-set-priority: this command is used to restore to the default configuration.

By default, this function is not enabled.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#ip pim ignore-rp-set-priority
```

14.12 Time Interval for PIM to Send Joined/Pruned Message

Command

```
ip pim jp-timer VALUE
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

VALUE: specifies the time interval for sending the join/pruning message, ranging from 1 to 65535 in seconds.

Description

Ip pim jp-timer: this command is used to globally configure the time interval for sending join/pruning messages.

no Ip pim jp-timer: this command is used to restore to the default value.

By default, the join/pruning message is sent at an interval of 60 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim jp-timer 120
```

14.13The Rate for the PIM Receive and Process Multicast Service Message

Command

```
ip pim register-rate-limit VALUE
no ip pim register-rate-limit
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

VALUE: the rate at which multicast messages are received and processed and the unit is in piece/second.

Description

ip pim regime-rate-limit: this command is used to globally configure the rate at which multicast messages are received and processed.

no ip pim register-rate-limit: this command is used to restore to the default value.

By default, the rate at which multicast messages are received and processed is not limited.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim register-rate-limit 1
```

14.14The PIM Checks the Accessibility of the RP

Command

```
ip pim register-rp-reachability
no ip pim register-rp-reachability
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

ip pim register-rp-reachability: this command is used to global configure whether the reachability of RP needs to be checked when sending registration packet. If it is not reachable, it means that registration cannot be carried out, and CouldRegister is False.

no ip pim register-rp-reachability: this command is used to restore to the default value. By default, DR need not to check the accessibility of the RP when sending registration messages.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim register-rp-reachability
```

14.15The VLAN Interface or Source IP Address of a PIM that Sends a Registered Message

Command

```
ip pim register-source < IFNAME | IP-ADDRESS >
no ip pim register-source
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

IFNAME: vlanif interface for sending registration messages.

IP-ADDRESS: the source IP address used to send the registration message, it must be the IP of the interface.

Description

ip pim register-source: this command is used to globally configure the VLAN interface or source IP address for sending registration messages.

no ip pim register-source: this command is used to restore to the default values.

By default, the source address of the registered message is the primary IP address of the outgoing interface to the RP in the routing table.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim register-source 192.168.1.100
```

14.16PIM Registration Suppression Time

Command

```
ip pim register-suppression VALUE
no ip pim register-suppression
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

VALUE: the time interval after receiving the registration stop message to send the registered message again, the VALUE range is 1 ~ 65535, in seconds.

Description

IP pim register-suppression: this command is used to configure the registration suppression time.

no ip pim register-suppression: this command is used to restore to the default value.

By default, the registration suppression time is 60 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim register-suppression 120
```

14.17PIM Static PR

Command

```
ip pim rp-address <RP-ADDRESS> [ ACL-NUMBER | ACL-NAME ]  
no ip pim rp-address <RP-ADDRESS> [ ACL-NUMBER | ACL-NAME ]
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

RP-ADDRESS: specifies the IP address of the static RP. The address must be a valid unicast IP address and cannot be configured as 127.0.0.0/8 network segment address.

ACL-NUMBER: standard acl number, ranging from 1 ~ 99 and 1300 ~ 1999.

ACL-NAME: extended acl name.

Description

ip pim rp-address: the command is used to configure the static RP.

no ip pim rp-address: the command is used to delete static RP.

By default, no static RP is configured.



Notes

- When the ACL rule referenced by a static RP changes, the RP needs to be re-elected for all the multicast groups.
 - Repeat this command to configure multiple static RPS. However, if the static RP address or ACL rule specified at configuration time is the same, the new configuration overrides the old configuration; If there are multiple static RPS serving the same multicast group, select the static RP with the largest IP address to serve that group.
 - Dynamic RP has higher priority than static RP.
 - If there is no ACL parameter, the configured static RP will serve all the multicast groups (224.0.0.0/4).
-

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#ip pim rp-address 192.168.1.100
```

14.18 PIM C-RP

Command

```
ip pim rp-candidate <IFNAME> [ priority <PRI> | interval <INTERVAL>
| group-list <ACL>]
no ip pim rp-candidate <IFNAME> [ priority <PRI> | interval
<INTERVAL> | group-list <ACL>]
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

IFNAME: specify C-RP vlanif interface.

INTERVAL: the sending interval of CRP-Adv message, ranging from 0 to 16383 in seconds.

PRI: specifies the priority of C-BSR, with values ranging from 0 to 255. The smaller the value, the higher the priority.

Description

ip pim rp-candidate: the command is used to configure an interface as C-RP.

no ip pim rp-candidate: the command is used to cancel the relevant configuration of C-RP.

By default C-RP is not configured.



Notes

- An interface that acts as C-RP must enable the PIM-SM.
 - If C-RP is not specified the scope of the multicast group it serves, the C-RP will serve all the multicast groups.
 - If the router wants to be C-RP for multiple groups, it needs to represent multiple group scopes with multiple rules when configuring the ACL corresponding to group-policy.
 - If executing this command on the same interface for multiple times, the latest configuration would override the old one.
-

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 20 deny 225.1.1.0 0.0.0.255
```



```
Switch(config)#ip pim rp-candidate vlanif1 priority 20 group-list  
1 interval 30
```

14.19 PIM KAT Timer Aging Time

Command

```
ip pim rp-register-kat VALUE  
no ip pim rp-register-kat
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

VALUE: aging time of KAT timer after receiving the registered message, ranging from 1 to 65535 in seconds.

Description

ip pim rp-register-kat: the command is used to globally configure the aging time of KAT timer after receiving the registered message.

The no ip pim rp-register-kat: the command is used to restore the mode configuration. By default, after receiving the registration message, the KAT timer's aging time is set to 3 times of the register-suppression time.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#ip pim rp-register-kat 120
```

14.20 PIM SPT Switch

Command

```
ip pim spt-threshold [ group-list <ACL-NUMBER | ACL-NAME> ]  
no ip pim spt-threshold [ group-list <ACL-NUMBER | ACL-NAME> ]
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

ACL-NUMBER: standard acl number, ranging from 1 ~ 99 and 1300 ~ 1999.

ACL-NAME: extended acl name.

Description

ip pim spt-threshold: this command is used for global configuration whether STP switch can be performed, can be applied ACL to specify the group address range, ACL action must be permit, if do not specify ACL, it means that all multicast groups need to perform SPT switch.

no ip pim spt-threshold: this command is used to cancel the recovery configuration. By default, STP switching is not performed.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip pim spt-threshold
```

14.21 Display BRS Running Information of PIM-SM

Command

```
show ip pim sparse-mode bsr-router
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

View the BRS running information of the PIM-SM of the current device.

Instance

```
Switch#show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
  BSR address: 172.24.0.10
  Uptime:      00:01:39, BSR Priority: 0, Hash mask length: 30
  Expires:     00:01:31
  Role: Candidate BSR
  State: Candidate BSR
```

```

Candidate RP: 172.24.0.3(vlanif50)
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:28

```

14.22 Display PIM-SM Interface Information

Command

```
show ip pim sparse-mode interface [ detail ]
```

View

Any

Default Level

1: View level

Parameters

Interface: specify vlanif interface.

Detail: specify to view details.

Description

The command is used to view PIM information on the interface.

Instance

```
Switch#show ip pim sparse-mode interface
```

Address	Interface	VIFindex	Ver/ Mode	Count	Nbr Prior	DR	DR
10.3.101.252	vlanif10	0	v2/S	1	1		
10.3.101.253							
11.1.1.2	vlanif11	2	v2/S	1	1	11.1.1.3	
172.24.0.2	vlanif50	3	v2/S	1	1	172.24.0.3	

```
Switch#show ip pim sparse-mode interface detail
```

```
vlanif10 (vif 0):
```

```
Address 10.3.101.252, DR 10.3.101.253
```

```
Hello period 30 seconds, Next Hello in 2 seconds
```

```
Triggered Hello period 5 seconds
```

```
Neighbors:
```

```
10.3.101.253
```

```
vlanif11 (vif 2):
```

```
Address 11.1.1.2, DR 11.1.1.3
```

```
Hello period 30 seconds, Next Hello in 2 seconds
```

```
Triggered Hello period 5 seconds
```

Secondary addresses:

11.1.1.1

Neighbors:

11.1.1.3

vlanif50 (vif 3):

Address 172.24.0.2, DR 172.24.0.3

Hello period 30 seconds, Next Hello in 3 seconds

Triggered Hello period 5 seconds

Neighbors:

172.24.0.3

14.23 View The Local Multicast Group Members of PIM-SM

Command

```
show ip pim sparse-mode local-members [<IFNAME> ]
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

IFNAME: specify vlanif interface.

Description

View the local multicast group members of PIM-SM of the current device.

Instance

```
Switch#show ip pim sparse-mode local-members vlanif10
PIM Local membership information
vlanif10:
  (*, 225.2.2.2) : Include
```

14.24 Displays the PIM-SM Multicast Routing Table Entry

Command

```
show ip pim sparse-mode mroute [ GROUP-ADDRESS | SOURCE-ADDRESS]
[ detail ]
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

GROUP-ADDRESS: specify multicast group address

SOURCE-ADDRESS: specify the source address of the multicast

Detail: specify to view details.

Description

View the current PIM-SM multicast routing table entry.

Instance

```
Switch#show ip pim sparse-mode mroute
IP Multicast Routing Table
```

```
(* , * , RP) Entries: 0
```

```
(* , G) Entries: 0
```

```
(S , G) Entries: 1
```

```
(S , G , rpt) Entries: 1
```

```
FCR Entries: 0
```

```
(10.3.101.111, 239.255.255.250)
```

```
RPF nbr: 0.0.0.0
```

```
RPF idx: None
```

```
SPT bit: 1
```

```
Upstream State: NOT JOINED
```

```
Local      .....
```

```
Joined     .....
```

```
Asserted   .....
```

```
Outgoing   .....
```

```
(10.3.101.111, 239.255.255.250, rpt)
```

```

RP: 0.0.0.0
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
  Local      .....
  Pruned     .....
  Outgoing   .....

*DUT4#show ip pim sparse-mode mroute detail
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(10.3.101.111, 239.255.255.250) Uptime: 00:09:05 Flags: 0x03
  RPF nbr: None, RPF idx: None
  Upstream:
    State: NOT JOINED, SPT Bit: on, JT: off, KAT Expiry: 85 secs
  Downstream:

(10.3.101.111, 239.255.255.250, rpt) Uptime: 00:09:05
  RP: 0.0.0.0, RPF nbr: None, RPF idx: None
  Upstream:
    State: RPT NOT JOINED, OT: off
  Macro state:
  Downstream:

```

14.25 Display PIM-SM Neighbor Information

Command

```
show ip pim sparse-mode neighbor [ <IFNAME> | detail ]
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

IFNAME: specify vlanif interface

Detail: specify to view details.

Description

View the currently learning PIM-SM neighborhood running status.

Instance

```
Switch#show ip pim sparse-mode neighbor
Neighbor      Interface      Uptime/Expires   Ver   DR
Address                               Priority/Mode
10.3.101.253   vlanif10        01:53:56/00:01:17 v2    1 /
DR
11.1.1.3       vlanif11        01:53:57/00:01:18 v2    1 / DR
172.24.0.3     vlanif50        01:53:56/00:01:17 v2    1 / DR
```

14.26 Display PIM-SM Next Hop Information

Command

```
show ip pim sparse-mode nexhop
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

View the next hop information used by the PIM-SM module in the current device.

Instance

```
Switch#show ip pim sparse-mode nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination Type Nexthop Nexthop Nexthop Nexthop Metric
Pref Refcnt
          Num Addr Ifindex Name
-----
10.3.101.111 ..S. 1 0.0.0.0 4 0
0 2
172.24.0.10 .R.. 1 0.0.0.0 6 0
0 1
```

14.27 Display PIM-SM Information

Command

```
show ip pim sparse-mode rp mapping
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

View RP-Set information of the PIM-SM of the current device.

Instance

```
Switch#show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
  RP: 172.24.0.10
    Info source: 172.24.0.10, via bootstrap, priority 192
    Uptime: 00:08:35, expires: 00:01:55
  RP: 172.24.0.3
    Info source: 172.24.0.10, via bootstrap, priority 192
    Uptime: 00:08:35, expires: 00:01:55
  RP: 172.24.0.2
    Info source: 172.24.0.10, via bootstrap, priority 192
    Uptime: 00:08:35, expires: 00:01:55
Group(s): 224.0.0.0/4, Static
  RP: 172.24.0.10
    Uptime: 02:28:07
```

14.28 Display the RP Address of the PIM-SM Multicast Group

Command

```
show ip pim sparse-mode rp-hash <GROUP-ADDRESS>
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

GROUP-ADDRESS: specify multicast group address.

Description

View the RP address of the specified multicast group address.

Instance

```
Switch#show ip pim sparse-mode rp-hash 226.1.1.1
RP: 172.24.0.2
Info source: 172.24.0.10, via bootstrap
```

15 VRRP Configuration

15.1 Create VRRP Group and Enter VRRP Configuration View

Command

```
router vrrp VIRTUAL-ROUTER-ID  
no router rip VIRTUAL-ROUTER-ID
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

virtual-router-id: VRRP backup group number, the value range is 1~255.

Description

router vrrp: this command is used to create a VRRP backup group session and enter session configuration mode.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router vrrp 1
```

15.2 VRRP Interface Enablement

Command

```
network interface <IFNAME>
```

```
no network interface <IFNAME>
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

IFNAME: interface name, only vlanif interface is supported.

Description

network interface: this command is used to enable VRRP on the specified network segment interface.

By default, VRRP function on the interface is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch (config)#router vrrp 1
Switch (config-router)#network interface vlanif1
```

15.3 VRRP Virtual IP Address

Command

```
virtual-ip <A.B.C.D >
no virtual-ip <A.B.C.D >
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

A.B.C.D: VRRP group virtual address.

Description

virtual-ip: this command is used for the virtual IP address of the VRRP group, which should be on the same subnet with the primary address of the interface specified by the network command.

Instance

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#router vrrp 1  
Switch(config- router)#virtual-ip 192.168.1.10
```

15.4 Preemption Mode Enablement

Command

```
preempt-mode (true | false)
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

True: enable preemption mode.

False: disable preemption mode.

Description

preempt-mode: this command is used to set the switch in the backup group to work in preemption mode. By default, the preempt-delay-time is 0 second and can be set by the preempt-delay-time command.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router vrrp 1  
Switch(config- router)#preempt-mode true
```

15.5 Preemption Delay Time

Command

```
preempt-delay-time DELAY-VALUE
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

DELAY-VALUE: preempt delay time, the value range is 0~255, the unit is seconds, the default value is 0 seconds.

Description

preempt-delay-time: this command is used to set the preemption delay for the VRRP backup group. In order to avoid frequent master/backup state transitions of the backup group members and make backup router have enough time to collect the necessary information (such as routing information), when backup router receives notification message with lower priority than the local priority, instead of immediately preempting to become Master, it will wait for a certain time - after the preemption delay time, VRRP notification message will be sent out to replace the original Master router.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config-router)#preempt-delay-time 5
```

15.6 Priority of VRRP Device

Command

```
priority PRIORITY-VALUE
no priority
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

PRIORITY-VALUE: the value of priority, ranging from 1 to 254. The larger the value, the higher the priority.

Description

priority: this command is used to set the priority of the router in the backup group.

no priority: this command is used to restore to the default value.

By default, the router has a priority of 100 in the backup group.



Notes

- Priority determines the router's status in the backup group, and the higher the priority, the more likely it is to become a Master router. Priority 0 is reserved by the system for special use and 255 is reserved by the system for IP address owners.

- If the router is the owner of the IP address, its priority is always 255, indicating that it is a Master router as long as it is working properly.
-

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config- router)#priority 150
```

15.7 VRRP Notification Message Interval

Command

```
advertisement-interval ADVER-INTERVAL
no advertisement-interval
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

ADVER-INTERVAL: the interval between the Master router in the backup group sending VRRP notification messages, with a value range of 1~10 in seconds.

Description

advertisement-interval: this command is used to set the time interval between VRRP notification messages sent by the Master router in the backup group.

no advertisement-interval: this command is used to restore to the default value.

By default, the Master router in the backup group sends VRRP notification messages every second.



Notes

Routers within the same backup group are configured at the same time interval.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config- router)#advertisement-interval 5
```

15.8 VRRP Message Authentication Mode

Command

```
authentication-mode (md5 | text)
no authentication-mode
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

Text: means authentication method is simple character authentication.

md5: md5 algorithm for authentication, not currently supported.

Description

authentication-mode: this command is used to configure how the backup group sends and receives VRRP messages.

no authentication-mode: this command is used to restore to the default value.

By default, authentication is not performed.



Notes

Different backup groups on an interface can set different authentication mode and authentication word; Members joining the same backup group need to set the same authentication mode and authentication word.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config-router)#authentication-mode text
```

15.9 Authentication Word of VRRP Message

Command

```
authentication-string KEY
no authentication-string
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

KEY: authentication word, case sensitive

Description

authentication-string: this command is used to configure how the backup group sends and receives authentication word of VRRP messages.

no authentication-string: this command is used to restore to the default value.

By default, authentication is not performed.

**Notes**

Different backup groups on an interface can set different authentication mode and authentication word; Members joining the same backup group need to set the same authentication mode and authentication word.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config-router)#authentication-string vrrpkey
```

15.10 Configure the Monitoring Specified Interface

Command

```
circuit-failover IFNAME PRIORITY-DELTA
no circuit-failover
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

IFNAME: interface name, physical ports and vlanif interfaces is supported.

PRIORITY -DELTA: amount of priority reduction, ranging from 1 to 253.

Description

circuit-failover: this command is used to configure to monitor the specified interface.

no circuit-failover: this command is used to cancel the monitor of the specified interface.

By default, no monitored interface is specified.

When the interface connecting the router to the uplink fails, the backup group cannot perceive the uplink failure. If the router is in the Master state at this time, the host in the LAN cannot access the external network. This problem can be solved by monitoring the function of the specified interface. When the interface connected to the upline is in the Down state, the router actively lowers its priority, making the priority of other routers in the backup group higher than that of this router, so that the router with the highest priority becomes Master and undertakes the forwarding task.



Notes

When the status of the monitored interface changes from Down to Up, the priority level of the corresponding router will be automatically restored.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config-router)#circuit-failover ge2 10
```

15.11Track ipdt Session

Command

```
track ipdt session SESSION-ID (increased | reduced) PRIORITY-DELTA
no track ipdt session SESSION-ID
```

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

SESSION-ID: ipdt session ID, ranging from 1 to 8.

Increased: upgrade priority, usually used for backup devices.

Reduced: reduce priority, usually used for master devices.

PRIORITY-DELTA: amount of priority upgrade or reduction, ranging from 1 to 253.

Description

track ipdt session: this command is used to set up sessions to track ipdt.

No track ipdt session: this command is used to cancel sessions to track ipdt.

By default, no traced ipdt session is specified.

Similar to circuit-failover, the VRRP backup group tracks an ipdt session, and with the up or down of the ipdt session, the priority is increased or decreased accordingly.

Usually reduced is set on the master device and increased is set on the backup device.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config-router)#track ipdt session 1 increased 20
```

15.12 Enable VRRP Backup Group

Command

enable

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

-

Description

enable: this command is used to enable the VRRP backup group, which is not enabled by default.



Notes

- When modifying any configuration of the backup group, enable must be turned off first.
 - The backup group must be configured with the virtual-ip and network interface commands to enable successfully.
-

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config- router)#enable
```

15.13Disable VRRP Backup Group

Command

disable

View

VRRP backup group session view

Default Level

2: Configuration level

Parameters

-

Description

disable : this command is used to disable the enabled VRRP backup group.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router vrrp 1
Switch(config- router)#disable
```

15.14Display VRRP Backup Group Information

Command

show vrrp [VIRTUAL-ROUTER-ID]

View

Privileged Exec Mode

Default Level

1: View level

Parameters

VIRTUAL-ROUTER-ID: backup group, the value range is 1~8.

Description

View the current configuration and operation of the specified VRRP backup group or all VRRP backup groups.

Instance

```
Switch> enable
Switch#show vrrp
VrId <10>
  State is Master
  Send Adv after 1 seconds
  Virtual IP is 11.1.1.1 (Not IP owner)
  Interface is vlanif11
  Priority is 151
  Advertisement interval is 1 sec
  Preempt mode is TRUE
  Preempt delay time is 30 sec
```

16 RIP Configuration

16.1 Enter RIP View

Command

```
router rip
no router rip
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

router rip: this command is used to start the RIP process and enter RIP process mode.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
```

16.2 RIP Interface Enablement

Command

```
network <A.B.C.D/M >
no network <A.B.C.D/M >
```

View

RIP View

Default Level

2: Configuration level

Parameters

A.B.C.D/M: network address and mask

Description

network: this command is used to enable RIP on the specified network segment interface.

RIP function on the interface is disabled by default.

Instance

```
Switch> enable
Switch#configure terminal
Switch (config)#router rip
Switch (config-router)#network 10.11.20.0/24
```

16.3 Configure IP Address of RIP Neighbor in NBMA Network

Command

```
neighbor <A.B.C.D >
no neighbor <A.B.C.D >
```

View

RIP View

Default Level

2: Configuration level

Parameters

A.B.C.D: neighbor interface address.

Description

neighbor: this command is used to configure the IP address of the RIP neighbor in the NBMA (non-broadcast multi-access) network and to send the update message to the opposite end as unicast rather than as normal multicast or broadcast.

no neighbor: this command is used to cancel the specified neighbor IP address.

By default, RIP does not send update message to any specified address.

**Notes**

This command is not recommended when a RIP neighbor is directly connected to the current device, as it may cause the opposite side to receive both multicast (or broadcast) and unicast message with the same routing information.

Instance

```
Switch>enable
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#neighbor 10.11.20.1
```

16.4 Add Static RIP Route

Command

```
route <A.B.C.D /M >
no route <A.B.C.D /M>
```

View

RIP View

Default Level

2: Configuration level

Parameters

A.B.C.D /M:IP address and prefix.

Description

route: this command is used to add a static RIP route. This command is primarily for debugging purposes. The route configured by this command does not appear in the core routing table, but the route exists in the RIP routing database.

Instance

```
Switch>enable
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#route 10.11.20.1/16
```

16.5 Add default Routing to RIP Routing Database

Command

```
default-information originate
no default-information originate
```

View

RIP View

Default Level

2: Configuration level

Parameters

-

Description

default-information originate: this command inserts the default route with a destination address of 0.0.0.0 into the RIP routing database and notifies the route like any other route.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#default-information originate
```

16.6 Default Route Metric

Command

```
default-metric <METRIC>
no default-metric
```

View

RIP View

Default Level

2: Configuration level

Parameters

<METRIC> : sets the default metric when routing is introduced. <value> values range from 0 -16.

Description

default-metric: the command is used to set the default routing weight used to introduce routes from other routing protocols into the RIP route. When redistribute command is used to introduce a route for another protocol, if no specific route weight is specified, the default route weight specified by default-metric is introduced.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#default-metric 10
```

16.7 RIP Route Management Distance

Command

```
distance <NUMBER> [ <A.B.C.D/M> ] [ <ACCESS-LIST-NAME |  
ACCESS-LIST-NUMBER > ]  
no distance <NUMBER> [ <A.B.C.D/M> ] [ <ACCESS-LIST-NAME |  
ACCESS-LIST-NUMBER > ]
```

View

RIP View

Default Level

2: Configuration level

Parameters

<NUMBER> : specifies the value of the distance, ranging from 1 to 255.

<A.B.C.D/ MB > : specifies the network prefix and prefix length.

<ACCESS-LIST-NAME|ACCESS-LIST-NUMBER>: specifies the access list number or name that applied.

Description

distance: this command is used to set the RIP routing management distance.

no distance: this command restores the default value.

Administrative distance is used to select routes when there are routes from two different routing protocols reach the same destination. The smaller the management distance value of the routing protocol, the more reliable the routing obtained by the protocol.

By default, RIP administrative distance is 120.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config- router)#distance 8 10.0.0.0/8 mylist
```

16.8 Access List Route Filtering

Command

```
distribute-list ( <ACCESS-LIST-NUMBER | ACCESS-LIST-NAME> |
prefix <PREFIX-LIST-NAME> ) ( in | out ) [ <IFNAME> ]
no distribute-list ( <ACCESS-LIST-NUMBER | ACCESS-LIST-NAME> |
prefix <PREFIX-LIST-NAME> ) ( in | out ) [ <IFNAME> ]
```

View

RIP View

Default Level

2: Configuration level

Parameters

< ACCESS-LIST-NUMBER |ACCESS-LIST-NAME> : the number or name of the access list to be applied.

<PREFIX-LIST-NAME> : the name of the list of prefixes to be applied.

<IFNAME>: specifies the interface name to which routing filtering is applied.

Description

distribute-list: the command is used to filter routing update message sent and received using an access list or prefix list. The no operation of this command is used to disable route filtering.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config- router)#distribute-list prefix myfilter in vlan 1
```

16.9 Other Routing Protocols Route Import

Command

```
redistribute { connected | static | ospf | bgp } [metric <VALUE> ]
```

```
[route-map <WORD>]  
no redistribute { connected| static| ospf|bgp} [metric <VALUE>]  
[route-map <WORD>]
```

View

RIP View

Default Level

2: Configuration level

Parameters

connected: connected route

static: static route;

ospf: OSPF route.

bgp: BGP route.

<VALUE> : the measure assigned to the introduced route, with a value range of 0-16.

<WORD>: a pointer to the route map used to introduce routes.

Description

redistribute: the command introduces routes learned from other routing protocols into BGP.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router rip  
Switch(config- router)#redistribute bgp metric 12
```

16.10Block RIP Broadcast

Command

```
passive-interface <IFNAME>  
no passive-interface <IFNAME>
```

View

RIP View

Default Level

2: Configuration level

Parameters

<IFNAME>: interface name.

Description

passive-interface: the command is used to block RIP broadcast on the specified interface, so RIP packets can only be sent to the interface configured with neighbor. The no operation of this command is to disable this function.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#passive-interface vlanif2
```

16.11 Time of RIP Timer

Command

```
timers basic <UPDATE> <INVALID> <GARBAGE>
no timers basic
```

View

RIP View

Default Level

2: Configuration level

Parameters

<UPDATE> : time interval for sending update message, the unit is second, value range: 5-2147483647.

<INVALID> : the time period in which RIP route is declared invalid, the unit is second, and the value range is 5-2147483647.

<GARBAGE> : the time period that can still exist in the routing table after declaring a route invalid, the unit is second, the value range is 5-2147483647.

Description

timers basic: the command sets the RIP timer update, timeout, and garbage collection time. The no operation of this command is to restore to the default values of the parameters.

By default, <update> defaults to 30; Invalid > defaults to 180; <garbage> defaults to 120. The system broadcasts RIP update message every 30 seconds. When the update message of a route cannot be received after 180 seconds, the route is considered invalid. But the route can also exist in the routing table for 120 seconds, after which the routing table can delete it.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config- router)#timers basic 20 80 60
```

16.12 RIP version

Command

```
version {1 | 2}
no version
```

View

RIP View

Default Level

2: Configuration level

Parameters

1 is rip version 1; 2 is rip version 2.

Description

Version 1: indicates that each interface only sends/receives RIP-I datagrams.
Version 2: indicates that each interface sends/receives RIP-II datagrams only.
By default, sending RIP-II as well as receiving RIP-II packets.
By default RIP version is 2.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config- router)#version 1
```

16.13 Maximum number of RIP route

Command

```
maximum-prefix <maximum-prefix>[<threshold>]
no maximum-prefixd
```

View

RIP View

Default Level

2: Configuration level

Parameters

<maximum-prefix> : the maximum number of RIP routes allowed, with a value range of 1-500;

<threshold> : when the percentage of the maximum number of routes exceeds, a warning will be generated by <threshold>. The value range is 1-100, and the default value is 75.

Description

maximum-prefix: the command is used to configure the maximum number of RIP routes in the routing table, and the no command removes the restriction on the number of routes.

The maximum number of RIP routes only limits the routes learned through RIP, excluding connected and introduced routes and RIP static routes configured with the route command. The comparison is based on the number of routes marked R in the show IP route database command. And also is based on the RIP route number shown by the show IP route statistics command.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#maximum-prefix 150
```

16.14 RIP Routing Measures Offset

Command

```
offset-list <ACCESS-LIST-NUMBER | ACCESS-LIST-NAME> {in | out}
<METRIC > [<IFNAME>]
no offset-list <ACCESS-LIST-NUMBER | ACCESS-LIST-NAME> {in | out}
<METRIC > [<IFNAME>]
```

View

RIP View

Default Level

2: Configuration level

Parameters

< access-list-number |access-list-name> : the number or name of the access list to be applied.

<metric> : the additional offset, and the value range is 0-16.

<ifname> : the specific interface name.

Description

offset-list: this command is used to configure the metric of the route learned through RIP plus an offset.

By default, RIP message is not validated.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config- router)#offset-list 1 in 5 vlanif1
```

16.15 RIP Route UDP to Receive Cache Size

Command

```
recv-buffer-size <SIZE>
no recv-buffer-size
```

View

RIP View

Default Level

2: Configuration level

Parameters

<SIZE> : buffer size in bytes, value range 8192-2147483647.

Description

recv-buffer-size: UDP receive buffer size of the command RIP; No operation restores to system defaults.

By default, it is 8192 bytes.

Instance

```
#Configure vlanif1 to use plaintext authentication mode
Switch> enable
Switch#configure terminal
Switch(config)#router rip
Switch(config- router)#recv-buffer-size 10240
```

16.16 RIP Message Authentication Mode

Command

```
ip rip authentication mode {text|md5}
no ip rip authentication mode [text|md5]
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

Text: means text authentication.

Md5: means md5 authentication.

Description

ip rip authentication mode: the command sets the used type of authentication; the no operation of this command is to restore the default authentication type, that is text authentication.

By default, the relative interfaces do not configure passwords and keys.

RIP-I does not support authentication, and RIP-II supports two types of authentication: text authentication (that is, Simple authentication) and datagram authentication (that is, MD5 authentication). This command needs to be used in combination with ip rip authentication key-chain or ip rip authentication string. Configuration alone does not perform authentication processing.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip rip authentication mode md5
```

16.17 RIP Message Authentication Key Chain

Command

```
ip rip authentication key-chain <name-of-chain>
no ip rip authentication key-chain [<name-of-chain>]
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<name-of-chain> : the name of the key chain used, the string can contain spaces, the input ends with enter key, and the string length should not exceed 256.

Description

ip rip authentication key-chain: the command is used to enable RIPv2 authentication on an interface and to configure the used key chain. The no operation of this command is used to cancel authentication.

If authentication mode is configured only and the key chain or password used by the interface is not configured, authentication will not work at all. If mode is not set before this command is configured, it will be set to plaintext authentication. The no operation of this command will cancel authentication, it does not mean that mode will be set to the non-authenticated type, but authentication will not be processed when sending or receiving packets. The ip rip authentication key-chain my key command can be entered, which means the key chain name is my key, a total of 6 characters

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip rip authentication key-chain my key
```

16.18 RIP Message Authentication Password

Command

```
ip rip authentication string <TEXT>
no ip rip authentication string
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<text> : the password used for authentication, with a length of 1-16 characters.
Password can include space and end it with enter key.

Description

ip rip authentication string: the command is used to set the password used for RIP authentication. The no operation of this command is used to cancel authentication. The ip rip authentication key chain command cannot be configured if this command is configured. Key id value is required when using MD5 authentication. If this command is used to configure the command, the key id value is equivalent to 1. If mode is not set before this command is configured, it will be set to plaintext authentication. The no operation of this command will cancel authentication, it does not mean that mode will be set to the non-authenticated type, but authentication will not be processed when sending or receiving packets. The ip rip authentication string aaa aaa command can be entered, which means the key is aaa aaa, a total of 7 characters.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip rip authentication string guest
```

16.19Receive RIP Message enablement

Command

```
ip rip receive-packet
no ip rip receive-packet
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

-

Description

ip rip receive-packet: this command is used to set whether the interface can receive RIP packets; The no operation of this command means cannot receive RIP message. By default, the interface can receive RIP message.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
```

```
Switch(config- vlanif1)#ip rip receive-packet
```

16.20 Accept Message of Specified RIP Version

Command

```
ip rip receive version { 1 | 2 | 1 2 }  
no ip rip receive version [ 1 | 2 | 1 2]
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

1 and 2 represent RIP version 1 and RIP version 2, respectively. 1 and 2 represent RIP version 1 and 2.

Description

ip rip receive-packet: the command is used to set the version information of the RIP packet received by the interface. RIP version 2 is received by default; The no operation of this command restores to the value set by the version command. By default, the RIP message version received by the interface is 2.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#interface vlanif1  
Switch(config- vlanif1)#ip rip receive version 1 2
```

16.21 Send RIP Message Enablement

Command

```
ip rip send-packet  
no ip rip send-packet
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

-

Description

ip rip send-packet: the command is used to set whether the interface can send RIP message; The no operation of this command means that RIP message cannot be sent.

By default, the interface can send RIP message.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config- vlanif1)#ip rip send -packet
```

16.22Send the Message of the Specified RIP Version

Command

```
ip rip send version { 1 | 2 | 1 2 }
no ip rip send version [ 1 | 2 | 1 2 ]
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

1 and 2 represent RIP version 1 and RIP version 2, respectively, 1 and 2 represent RIP versions 1 and 2.

Description

ip rip send-packet: the command is used to set the version information of the RIP packet sent by the interface. RIP version 2 is sent by default; The no operation of this command restores to the value set by the version command.

By default, the version that the interface sends RIP message is 2.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config- vlanif1)#ip rip send version 1 2
```

16.23 RIP Horizontal Split Enablement

Command

```
ip rip split-horizon [ poisoned ]  
no ip rip split-horizon
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

[poisoned] : it means the configuration with reverse poison horizontal segmentation.

Description

ip rip split-horizon: the command is used to enable horizontal split. The no operation of this command disables horizontal split.

By default, enable horizontal segmentation with reverse poisoning.

Horizontal segmentation is used to prevent Routing Loops, which prevent the interface of the device from broadcasting routes learned from itself. In general, horizontal segmentation is necessary to prevent routing loops, so it is not recommended to disable it. When it is necessary to disable horizontal segmentation for special reasons, such as ensuring proper execution of the protocol, be sure to confirm whether it is necessary.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#interface vlanif1  
Switch(config- vlanif1)#ip rip split-horizon poisoned
```

16.24 Display Routing Information learned by RIP

Command

```
show ip rip
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

show ip rip: the command is used to display the routing information learned by rip protocol.

Note:

The show ip route rip command is used to display the route information that learned by rip protocol and show in the routing table.

Instance

```
SwitchA> enable
SwitchA#configure terminal
SwitchA(config)#interface vlanif1
SwitchA(config- vlanif1)#ip address 192.168.1.1/24
SwitchA(config- vlanif1)#exit
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#ip interface vlan 2
SwitchA(config)#interface vlanif2
SwitchA(config- vlanif2)#ip address 192.168.2.2/24
SwitchA(config- vlanif2)#exit
SwitchA(config)#router rip
SwitchA(config-router)#network 192.168.1.0/24
SwitchA(config-router)#network 192.168.2.0/24
```

```
SwitchB> enable
SwitchB#configure terminal
SwitchB(config)#vlan database
SwitchB(config-vlan)#vlan 2
SwitchB(config-vlan)#exit
SwitchB(config)#ip interface vlan 2
SwitchB(config)#interface vlanif2
SwitchB(config- vlanif2)#ip address 192.168.2.1/24
SwitchB(config- vlanif2)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#network 192.168.2.0/24
SwitchB(config-router)#end
Switch#show ip rip
```

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,

C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

Network	Next Hop	Metric	From	If	Time
R 192.168.1.0/24	192.168.2.2	2	192.168.2.2		
vlanif2 02:41					
Rc 192.168.2.0/24		1		vlanif2	

Switch#**show ip route rip**

R 192.168.1.0/24 [120/2] via 192.168.2.2, vlanif2, 00:00:32

16.25 Display the Routing Information in the RIP Routing information Base

Command

show ip rip database

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

show ip rip database: the command is used to display routing information in the rip routing information database.

Instance

```
SwitchA> enable
SwitchA#configure terminal
SwitchA(config)#interface vlanif1
SwitchA(config-vlanif1)#ip address 192.168.1.1/24
SwitchA(config-vlanif1)#exit
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#ip interface vlan 2
SwitchA(config)#interface vlanif2
SwitchA(config-vlanif2)#ip address 192.168.2.2/24
SwitchA(config-vlanif2)#exit
```

```

SwitchA(config)#router rip
SwitchA(config-router)#network 192.168.1.0/24
SwitchA(config-router)#network 192.168.2.0/24

SwitchB> enable
SwitchB#configure terminal
SwitchB(config)#vlan database
SwitchB(config-vlan)#vlan 2
SwitchB(config-vlan)#exit
SwitchB(config)#ip interface vlan 2
SwitchB(config)#interface vlanif2
SwitchB(config- vlanif2)#ip address 192.168.2.1/24
SwitchB(config- vlanif2)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#network 192.168.2.0/24
SwitchB(config-router)#end
Switch#show ip rip database

```

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

Network	Next Hop	Metric	From	If	Time
R 192.168.1.0/24	192.168.2.2	2	192.168.2.2	vlanif2	02:57
Rc 192.168.2.0/24			1		vlanif2

16.26 Display RIP Interface Information

Command

```
show ip rip interface <IFNAME>
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

show ip rip interface: the command is used to display rip interface information.

Instance

```
SwitchA> enable
SwitchA#configure terminal
SwitchA(config)#interface vlanif1
SwitchA(config- vlanif1)#ip address 192.168.1.1/24
SwitchA(config- vlanif1)#exit
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#ip interface vlan 2
SwitchA(config)#interface vlanif2
SwitchA(config- vlanif2)#ip address 192.168.2.2/24
SwitchA(config- vlanif2)#exit
SwitchA(config)#router rip
SwitchA(config-router)#network 192.168.1.0/24
SwitchA(config-router)#network 192.168.2.0/24
```

```
SwitchB> enable
SwitchB#configure terminal
SwitchB(config)#vlan database
SwitchB(config-vlan)#vlan 2
SwitchB(config-vlan)#exit
SwitchB(config)#ip interface vlan 2
SwitchB(config)#interface vlanif2
SwitchB(config- vlanif2)#ip address 192.168.2.1/24
SwitchB(config- vlanif2)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#network 192.168.2.0/24
SwitchB(config-router)#end
Switch#show ip rip interface vlanif2
vlanif2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled
    IP interface address:
      192.168.2.1/24
```

17 OSPF Configuration

17.1 Enter OSPF Router Configuration View

Command

```
router ospf [<PROCESS-ID>]  
no router ospf [<PROCESS-ID>]
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

process-id: range 1-65535, default to process 1.

Description

router ospf [PROCESS-ID]: the command is used to start the OSPF process and enter OSPF process mode.

Instance

```
# configuration starts and enters the OSPF process 1  
Switch> enable  
Switch#configure terminal  
Switch(config)#router ospf
```

17.2 OSPF Route ID

Command

```
router-id <A.B.C.D>  
no router-id [<A.B.C.D>]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: router ID.

Description

router-id [< A.B.C.D>] : the command is used to configure the OSPF router ID of the device.

The same configuration command router-id <A.B.C.D> is available in configuration mode with a lower priority

Instance

```
# Configure device router ID to 1.1.1.1
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config- router)#router-id 1.1.1.1
```

17.3 OSPF Area and Enablement

Command

```
network (A.B.C.D/M | A.B.C.D) area (A.B.C.D | <0-4294967295>)
no network (A.B.C.D/M | A.B.C.D) area (A.B.C.D|<0-4294967295>)
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D/M | A.B.C.D: network address and mask.

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

Description

network: the command is used to configure the OSPF region the various network interfaces of the device belong to and enable OSPF functions.

By default, the interface does not belong to any region and OSPF function is disabled.

Instance

```
# specifies that the primary IP address of the interface running
the OSPF protocol is on the network segment 10.11.20.0/24, and the
OSPF region ID of the interface is 1
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#network 10.11.20.0 0.0.0.255 area 1
Or Switch(config-router)#network 10.11.20.0/24 area 1
```

17.4 Configure and Publish a Host Route

Command

```
host (A.B.C.D) area (A.B.C.D | <0-4294967295>) [cost <COST>]
no host (A.B.C.D) area (A.B.C.D | <0-4294967295>) [cost <COST>]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: host address.

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

<cost> : host routing cost value, integer in range 0~65535, default value is 0.

Description

host: the command is used to configure and publish a host route.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#host 172.16.10.100 area 1
```

17.5 Configure Neighbor Interface Address in the NBMA Network

Command

```
neighbor <A.B.C.D> [priority <PRIORITY-ID>] [poll-interval <SECONDS>] [cost <METRIC>]  
no neighbor <A.B.C.D> [priority <PRIORITY-ID>] [poll-interval <SECONDS>] [cost <METRIC>]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: neighbor interface address.

priority-id: priority of neighbors in NBMA network, invalid in P2MP network, default value is 0, value range is <0-255>.

seconds: interval of HELLO package before establishing neighborhood relationship, value range is <1-65535>.

metric: neighborhood link cost, value range is <1-65535>.

Description

neighbor: the command is used to configure neighbors in the NBMA network.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router ospf  
Switch(config- router)#neighbor 10.11.20.1
```

17.6 Create Virtual Connection

Command

```
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D  
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D  
Command options are numerous and not enumerated
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

A.B.C.D: virtual link neighbor router ID, IP address format.

Hello-interval seconds: the time interval for the interface to send hello message, ranging from 1 to 65535 in seconds. The default value is 10 seconds. This value must equal the value of hello seconds on its connected virtual connection router.

retransmit-interval seconds: the time interval for retransmission of LSA packets of the interface, ranging from 1 to 65535 in seconds. The default value is 5 seconds.

transmit-delay seconds: the time interval for transmitting LSA packets, ranging from 1 to 65535 in seconds. The default value is 1 second.

Dead-interval seconds: dead interval seconds, ranging from 1 to 65535 in seconds, with a default value of 40 seconds. This value must equal the dead-interval seconds value of its virtual connected router and be at least 4 times the hello seconds value.

Authentication: plaintext authentication mode.

Message-digest: MD5 authentication mode, it is optional, if unselected it will be simple authentication mode (password in plaintext).

Null: null is unauthenticated.

Authenticate-key: plaintext authentication password.

Message-digest-key: MD5 key with range 1-255.

Description

virtual-link: this command is used to create and configure a virtual connection.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 1 virtual-link 1.1.1.1
```

17.7 Routing Within the Aggregation Area

Command

```
area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M) [advertise |
not-advertise]
```

```
no area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M) [advertise |  
not-advertise]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

A.B.C.D/M: aggregate address and mask.

advertise | not-advertise: whether to publish the aggregation route or not. This aggregation route is published if the parameter advertise or not-advertise is not specified.

Description

area range: the command is used to aggregate the routers of an area. If the network addresses in the region are configured in a discontinuous manner, configuring this command on ABR notifies a summary route that contains all the individual networks in the region that belong to a particular range.

By default this function is not configured.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router ospf  
Switch(config-router)#area 1 range 10.11.20.0/24
```

17.8 Type-3 LSA Filter

Command

```
area (A.B.C.D|<0-4294967295>) filter-list (access|prefix) <name>  
(in|out)  
no area area (A.B.C.D|<0-4294967295>) filter-list (access|prefix)  
<name> (in|out)
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

Access: specifies to use access-list.

Prefix: specifies to use prefix-list; <name> the name of the filter, the length is 1-256.

In: from other areas to this area.

Out: from this area to other areas.

Description

area filter-list: the command is used to configure the filtering of Type-3 LSA in and out of the area.

By default this function is not configured.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255
Switch(config)#access-list 1 permit any-
Switch(config)#router ospf
Switch(config- router)#area 1 filter-list access 1 in
```

17.9 Stub Area

Command

```
area (A.B.C.D|<0-4294967295>) stub [no-summary]
no area (A.B.C.D|<0-4294967295>) stub [no-summary]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

No-summary: this parameter is only used for the ABR of the Stub region. After configuration, the ABR only publishes a type-3 LSA for the default route to the Stub region, and does not generate any other type-3 LSAs (this region is also known as the Totally Stub region).

Description

area stub: the command is used to configure a region as a Stub region.

By default, no region is set to Stub region.

If user want to configure a zone as a Stub zone, all routers in the zone must configure this property. For configuration, refer to the command default-cost.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 1 stub
```

17.10 NSSA Area

Command

```
area (A.B.C.D|<0-4294967295>) nssa
[default-information-originate | translator-role | no-summary |
no-redistribution]
no area (A.B.C.D|<0-4294967295>) nssa
[default-information-originate | translator-role | no-summary |
no-redistribution]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

Default-information-spanish [metric <0-16777214>] [metric <1-2>] : generates LSA of type-7 metric <0-16777214> specifies the metric value, and metric-type <1-2> specifies the metric type of external-LSA, 2 is the default value.

translator-role {candidate|never|always} : specify LSA transformation behavior of router:

Candidate means that if the router is elected as translator, NSSA-LSA can be converted to Type-5 LSA, which is candidate by default.

Never means that the router never converts NSSA-LSA to Type 5 LSA.

Always means that the router always converts NSSA-LSA to Type 5 LSA.

No-summary: this parameter is only used for the ABR of the NSSA region. After configuration, NSSA ABR only publishes a default route to the region through the Summary-LSA of Type-3, and no other Summary-LSAs (this region is also called Totally NSSA region) to the region.

Summary-LSA publishes a default route to the region and no other Summary-LSAs (this region is also known as the Totally NSSA region) is published to the region.

No-redistribution: means do not distribute EXTERNAL - LSA to NSSA.

Description

area nssa: the command is used to configure a region as a nssa region.

By default, no region is set to nssa region.

If user want to configure a zone as a NSSA zone, all routers in the zone must configure this command. For configuration, refer to the command default-cost.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 1 nssa
```

17.11 Area Shortcut Mode

Command

```
area (A.B.C.D|<0-4294967295>) shortcut {default|enable|disable}
no area (A.B.C.D|<0-4294967295>) shortcut
{default|enable|disable}
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

Default: set the default shortcut behavior of the area.

Enable: forced to shortcut when through the area.

Disable: not to shortcut when through the area.

Default: the default configuration is set to default.

Description

area shortcut: the command is used to configure shortcut mode of a region.

Whether the region boundary router is connected to a backbone router or not, enabling region shortcut allows traffic to pass through non-backbone regions with lower magnitude.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 1 shortcut enable
```

17.12 Default Costs for Introduced Default Routes

Command

```
area (A.B.C.D|<0-4294967295>) default-cost <cost>
no area (A.B.C.D|<0-4294967295>) default-cost
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

<cost>: value range is 0-16777215. Default value is 1.

Description

area default-cost: this command used to configure stub/nssa zone to introduce the default cost of default routing.

This command only applies to an ABR router connected to a stub region or NSSA region.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config- router)#area 1 default-cost 20
```

17.13 Configure Aggregation of External Routes and Notify or Suppress

Command

```
summary-address <A.B.C.D/M> [{not-advertise|tag<tag-value>}]
no summary-address <A.B.C.D/M> [{not-advertise|tag<tag-value>}]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D/M: aggregate address and mask.

Not-advertised: control the external routing.

Tag <tag-value> : the tag number of the external route, the value range is 0~4294967295, the default is 0.

Description

summary-address: this command is used to introduce OSPF from other routing protocols, demanding that each route be notified separately in an external LSA. Using this command, only one summary route can be notified for introduced routes that are covered by specific network addresses and masks, which can greatly reduce the size of the link-state database.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config- router)#summary-address 10.11.0.0/16
```

17.14 Link Cost Bandwidth Reference Value

Command

```
auto-cost reference-bandwidth <bandwidth>  
no auto-cost reference-bandwidth
```

View

OSPF View

Default Level

2: Configuration level

Parameters

< bandwidth > : the reference bandwidth value in megabits per second, ranging from 1~4294967.

Description

reference-bandwidth: this command is used to configure the bandwidth reference values by which link cost is calculated.

By default, link cost is calculated based on a bandwidth reference value of 100Mbps. If the link cost value configuration is not displayed, OSPF calculates the cost based on link bandwidth (cost = bandwidth reference value ÷ bandwidth, the maximum cost is 65535 when the calculated cost value is greater than 65535).

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router ospf  
Switch(config- router)#auto-cost reference-bandwidth 50
```

17.15 Opaque LSA Publishing and Receiving Capabilities

Command

```
capability opaque  
no capability opaque
```

View

OSPF View

Default Level

2: Configuration level

Parameters

-

Description

capability opaque: the command is used to enable OSPF opaque LSA to publish and receive Type9, Type10, and Type11 opaque LSA.

The no capability opaque: this command is used to restore the default value.

By default, Opaque LSA publish receiving capability of OSPF is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#capability opaque
```

17.16 Compatibility with RFC1583

Command

```
compatible rfc1583
no compatible rfc1583
```

View

OSPF View

Default Level

2: Configuration level

Parameters

-

Description

compatible rfc1583: the command is used to enable the compatibility of RFC 1583 with external routing rules.

no compatible rfc1583: the command is used to disable the compatibility of RFC 1583 with external routing rules.

By default, enable the compatibility of RFC 1583 with external routing rules.

When multiple AS-External-LSA publish routes to the same destination address, the priority rules defined by RFC 1583 and RFC 2328 differ in how to select the optimal route. When RFC 2328 is compatible with RFC 1583, the regional routing in the

backbone area is optimized. When RFC 2328 is incompatible with RFC 1583, intra-region routing in non-backbone area is preferred to minimize the burden of backbone area.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#compatible rfc1583
```

17.17 Introduce Default Route

Command

```
default-information originate [always | metric | metric-type |
route-map]
no default-information originate [always | metric | metric-type
| route-map]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

Always: notify default routing whether or not there is one in the software.

metric = metric <value> : sets the metric used to create the default route, and <value> ranges from 0 to 16777214. The default metric is 10.

Metric -type = metric-type {1|2} :sets the OSPF external link type of the default route.

- 1: Set the external type 1 metric of OSPF.
- 2: Set the external type 2 metric of OSPF.

route-map = route-map <WORD> : <WORD> specifies the policy name of the applied routing. Only if the default route exists in the routing table of the current router and the route matches the routing policy specified by route-map can a Type-5 LSA describing the default route be published, and the specified routing policy will affect the value in the Type-5 LSA. If the always parameter is specified at the same time, as long as a route matches the specified routing policy, a Type-5 LSA describing the default route will be published regardless of whether there is a default route in the routing table of the current router, and the specified routing policy will affect the value in the Type-5 LSA.

Description

default-information originate: the command is used to introduce the default route into the OSPF routing area.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config- router)#default-information originate always
```

17.18 OSPF Routing Default Metric

Command

```
default-metric < metric >
no default-metric
```

View

OSPF View

Default Level

2: Configuration level

Parameters

<metric> : sets the default metric when routing is introduced. <value> ranging from 0 to 16777214.

Description

default-metric: sets the default metric for the OSPF routing protocol, and the no command restore to the default values. When metric are incompatible due to default, routing introductions still can continue. If the metric cannot be converted, the default metric provides an alternative option that enables the routing introduction to proceed. This command causes the current routing protocols to use the same metric for all introduced routes. This command should be used in combination with the command redistribute.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config- router)#default-metric 100
```


17.19 OSPF Route Management Distance

Command

```
distance { <value> | ospf }  
no default { < value > | ospf }
```

View

OSPF View

Default Level

2: Configuration level

Parameters

< value > : OSPF route management distance value, value range 1~255.

ospf { external | inter-area | intra-area }:

- external <external distance> sets the management distance value of the routes learned from other routing fields, <external distance> management distance value, and its value range is 1~255.
- inter-area <inter-distance> sets the value of route management distance from one area to another. <inter-distance> management distance value, which ranges from 1 to 255.
- intra-area <intra-distance> sets the managed distance value of all routes in an area <intra-distance> management distance value, which ranges from 1 to 255.

Description

distance: the command is used to set the OSPF route management distance based on the route type configuration, and the no command restores the default value.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router ospf  
Switch(config-router)#distance ospf inter-area 20 intra-area 10  
external 40
```

17.20 Ingress Route Information Filter

Command

```
distribute-list <access-list-name> in  
no distribute-list <access-list-name> in
```

View

OSPF View

Default Level

2: Configuration level

Parameters

<access-list-name> : specifies the name of the access-list used.

Description

istribute-list in: the command is used to filter routing information in the incoming direction, and can not filter the LSA.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#distribute-list 10 in
```

17.21Egress Route Information Filter

Command

```
distribute-list <access-list-name> out {kernel |connected|
static| rip| isis| bgp}
distribute-list <access-list-name> out {kernel |connected|
static| rip| isis| bgp}
```

View

OSPF View

Default Level

2: Configuration level

Parameters

<access-list-name> : specifies the name of the access-list used.

out: routing updates sent by filter.

kernel: kernel route.

connected: connected route

static: static route;

rip: RIP route.

isis: ISIS route.

bgp: BGP route.

Description

distribution-list out: The command is used to filter outgoing routes when routes from other routing protocols are introduced into the OSPF routing table, and this command is used only by ASBR.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 11 permit 172.10.0.0 0.0.255.255
Switch(config)#router ospf
Switch(config-router)#distribute-list 1 out bgp
Switch(config-router)#redistribute bgp
```

17.22Introduce Additional Routing Information

Command

```
redistribute {connected|static|rip|bgp} [metric<value>]
[metric-type {1|2}] [route-map<word>] [tag<tag-value>]
no redistribute {connected|static|rip|bgp} [metric<value>]
[metric-type {1|2}] [route-map<word>] [tag<tag-value>]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

connected: connected route

static: static route;

rip: RIP route.

bgp: BGP route.

metric: <value> the metric assigned to the introduced route, with a value range of 0-16777214.

metric -type: {1|2} the introduced metric type of the external route and can only be 1 or 2, default value is 2.

Route-map: <word> points to the route map used to introduce the route.

Tag: <tag-value> the tag number of the external route, the value range is 0~4294967295, the default value is 0.

Description

1. redistribute: the command is used only by ASBR to introduce routes from other routing protocols into the OSPF routing table.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#redistribute bgp metric 12
```

17.23 Interface Hello Message Control

Command

```
passive-interface<ifname> [<ip-address>]
no passive-interface<ifname> [<ip-address>]
```

View

OSPF View

Default Level

2: Configuration level

Parameters

<ifname>: interface name.

<ip-address>: interface IP address.

Description

passion-interface: the command is used to configure not to send hello messages on a specific interface.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#passive-interface vlanif2
```

17.24 SPF Timer

Command

```
timers spf <spf-delay> <spf-holdtime>
no timers spf
```

View

OSPF View

Default Level

2: Configuration level

Parameters

<spf-delay> : The default value is 5 seconds.

<spf-holdtime> : The default value is 10 seconds.

Description

timers spf: the command is used to configure the delay time between receiving a topological change and SPF computation, and the hold time between two discrete SPF computations.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#timers spf 6 12
```

17.25The Maximum Number of LSA

Command

```
overflow database <maxdbsize > [{hard|soft}]
no overflow database
```

View

OSPF View

Default Level

2: Configuration level

Parameters

< maxdbsize > : maximum number of LSA, ranging from 0 to 4294967294.

Soft: soft limit,a warning will be sent when crossing a line.

Hard: hard limit,the ospf instance will be close directly when crossing the line.

By default, it is processed as hard.

Description

overflow database: the command is used to configure the maximum number of LSA.

No operation does not limit the maximum number.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config- router)#overflow database 10000
```

17.26 Maximum Concurrent Number of Current DD Packet

Command

```
max-concurrent-dd <value>
no max-concurrent-dd
```

View

OSPF View

Default Level

2: Configuration level

Parameters

<value> : the value range is <1-65535>, the upper limit of the process of maximum concurrent dd packet.

Description

max-concurrent-dd: the command is used to configure the OSPF course to process the maximum number of concurrent dd currently, and the no command restores the default value.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config- router)#max-concurrent-dd 25
```

17.27 Regional OSPF Message Validation

Command

```
area (A.B.C.D|<0-4294967295>) authentication [message-digest]
no area (A.B.C.D|<0-4294967295>) authentication
```

View

OSPF View

Default Level

2: Configuration level

Parameters

A.B.C.D: area identification, IP address format.

<0-4294967295> : area identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

Message-digest: MD5 authentication mode, it is optional, if unselected it will be simple authentication mode (password in plaintext).

Description

area-id authentication: the command is used to configure the OSPF zone to authenticate OSPF messages and the authentication mode.

no area-id authentication: the command is used to cancel the configured authentication mode for this area.

By default, regions do not authenticate OSPF packets

Instance

```
#Configure OSPF zone 0 to use MD5 authentication mode
Switch> enable
Switch#configure terminal
Switch(config)#router ospf
Switch(config- router)#area 0 authentication message-digest
Switch(config- router)#no area 0 authentication
```

17.28 OSPF ABR Type

Command

```
ospf abr-type (cisco | ibm | shortcut | standard)
no ospf abr-type
```

View

OSPF View

Default Level

2: Configuration level

Parameters

Cisco: using the cisco (RFC3509) ABR implementation, the router connects multiple active areas, one of which is the backbone area.

ibm: using the ibm (RFC3509) ABR implementation, the router connects multiple active areas and backbone areas, backbone areas should not be the active areas.

Shortcut: using standard (draft-ietf-ospf-shortcut-abr-02) specify a shortcut-ABR.

Standard: using the standard (RFC2328) ABR implementation, the router connects multiple active areas.

Description

ospf abr-type: The command is used to configure the ABR type of the OSPF region. Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#router ospf
```

```
Switch(config-router)# ospf abr-type standard
```

17.29Interface OSPF Message Validation

Command

```
ip ospf authentication [message-digest]
```

```
ip ospf authentication null
```

```
no ip ospf authentication
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

Message-digest: MD5 authentication mode, optional, unselected simple authentication mode (password in plaintext).

Null: null is unauthenticated.

Description

ip ospf [A.B.C.D] authentication [message-digest]: the command is used to configure the interface to authenticate ospf messages and the authentication mode.

ip ospf [A.B.C.D] authentication null and no ip ospf authentication: the commands are used to cancel the authentication mode configured by the associated interface.

By default, relative interface do not authenticate OSPF packets

Instance

```
#Configure vlanif1 to use plaintext authentication mode
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config- vlanif1)#ip ospf authentication
Switch(config- vlanif1)#no ip ospf authentication
```

Note:

- The authentication mode of the interface has a higher priority than the authentication mode of the region. When the authentication mode is not configured in the interface and the regional configuration is simple plaintext password authentication, the password needs to be set using ip ospf authentication-key command in the interface mode. If it is MD5 authentication, user need to configure the MD5 key using ip ospf message-digest-key in interface mode. When the authentication mode of an interface is configured, the authentication of the region in which the interface is located cannot affect the authentication behavior of the interface.
 - Priority: ip ospf authentication is higher than area <area-id> authentication.
 - Ip ospf authentication [message-digest] and other commands of the layer 2 interface are invalid.
-

17.30Interface OSPF Message Authentication Key

Command

```
ip ospf authentication-key <line>
no ip ospf authentication-key
ip ospf authentication message-digest-key <key-id> md5 <line>
no ip ospf message-digest-key <key-id>
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

Line: plaintext authentication password.

key-id: MD5 key, the range is 1-255.

Description

ip ospf authentication-key <line> : the command is used to configure the password of OSPF message plaintext encryption authentication of relevant interface, the no operation of this command is used to restore the default value.

`ip ospf message-digest-key <key-id> md5<line>`: the command is used to configure the key value and password of the relevant interface for md5 encryption verification of ospf message, and restore the default value through the no operation of this command.

By default, the relative interfaces do not configure passwords and keys.

Instance

```
# Configure vlanif1 to use MD5 authenticated key values and
passwords.
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf message-digest-key 2 md5
yourpassword
Switch(config- vlanif1)#no ip ospf message-digest-key 2
```

Note:

Use MD5 encryption authentication to achieve security between OSPF routers on the network. This command must configure the same key id and key between neighbors, otherwise an adjacency relationship cannot be established. The subsequent configuration of this command covers the previous configuration to prevent the system from continuing to communicate using the previous key id.

17.31Interface OSPF Cost

Command

```
ip ospf cost <cost>
no ip ospf cost
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<cost>:value range is 1-65535.

Description

ip ospf cost: the command is used to configure the cost required to run the ospf protocol on the interface. The no operation of this command is to restore the default value.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config- vlanif1)#ip ospf cost 20
```

17.32Interface LSA Database Filter

Command

```
ip ospf database-filter all out
no ip ospf database-filter
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

-

Description

Ip ospf database-filter all out: the command is used to configure to enable the LSA database filter switch on a specific interface.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config- vlanif1)#ip ospf database-filter all out
```

17.33Interface OSPF Neighbor Failure Time

Command

```
ip ospf dead-interval <time>
no ip ospf dead-interval
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<time>: OSPF neighbor failure time, in seconds, value range 1 ~ 65535

Description

ip ospf dead-interval: the command is used to configure the OSPF neighbor failure time.

By default, the failure time of OSPF neighbors of P2P and Broadcast interfaces is 40 seconds. The failure time of OSPF neighbors of P2MP and NBMA interfaces is 120 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf dead-interval 60
```

17.34Time Interval of Sending Hello Message

Command

```
ip ospf hello-interval <time>
no ip ospf hello-interval
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<time> : the time interval for the interface to send Hello message, in seconds, with a value range of 1 ~ 65535.

Description

ip ospf hello-interval: the command is used to configure the time interval for the interface to send the Hello message.

By default, the time interval for P2P and Broadcast type interfaces to send Hello message is 10 seconds. The time interval for P2MP and NBMA type interface to send Hello message is 30 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf hello-interval 20
```

17.35Interface Retransmission LSA Interval

Command

```
ip ospf retransmit-interval <time>
no ip ospf retransmit -interval
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<time> : the time interval for the interface to retransmit LSA, in seconds, with a value range of 1 ~ 65535.

Description

ip ospf retransmit-interval command is used to configure the time interval for the interface to retransmit LSA.

By default, the time interval for interface to retransmit LSA is 5 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf retransmit-interval 10
```

17.36Interface to LSA Transmission Delay Time

Command

```
ip ospf transmit-delay <time>
no ip ospf transmit-delay
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<time> : transmission delay time of LSA of the interface, in seconds, with a value range of 1 ~ 65535.

Description

ip ospf retransmit-delay: the command is used to configure the transmission delay of LSA of the interface.

By default, the transmission delay for interface to retransmit LSA is 1 second.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf transmit-delay 2
```

17.37Disable the OSPF Function of the Interface

Command

```
ip ospf disable all
no ip ospf disable all
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

-

Description

ip ospf disable all: disable OSPF function on the interface.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf disable all
```

17.38 Interface OSPF MTU Value

Command

```
ip ospf mtu <mtu>
no ip ospf mtu
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

< mtu>: interface mtu value, ranging from 576 to 65535.

Description

ip ospf mtu: the command is used to configure the mtu value of the interface as the basis for the OSPF grouping. The interface values configured by this command are used only by the ospf protocol and are not updated to the kernel.

By default, the interface mtu value obtained from the kernel is used.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf mtu 1480
```

17.39 Interface DD Exchanges Ignore MTU

Command

```
ip ospf <ip-address> mtu-ignore
no ip ospf <ip-address> mtu-ignore
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<ip-address>: interface IP address format.

Description

ip ospf mtu-ignore: the command does not check the mtu size when configuring the DD switching for the interface. By default check is necessary.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf mtu-ignore
```

17.40Interface OSPF Network Type

Command

```
ip ospf network
{broadcast|non-broadcast|point-to-point|point-to-multipoint}
no ip ospf network
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

broadcast: set OSPF network type to broadcast.
non-broadcast: set OSPF network type to NBMA.
point-to-point: set OSPF network type to point-to-point.
point-to-multipoint: set OSPF network type to point-to-multipoint.

Description

ip ospf network: the command is used for the OSPF network type of the interface.
By default, the OSPF network type of the interface is the broadcast type.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf network non-broadcast
```


17.41 The DR Priority of the Interface

Command

```
ip ospf priority <priority>
no ip ospf priority
```

View

Layer 3 Interface View

Default Level

2: Configuration level

Parameters

<priority> : DR priority of the interface, ranging from 0 to 255.

Description

ip ospf priority: the command is used to configure the DR priority of the interface.

By default, the DR priority of the interface is 1.

The DR priority determines the qualification of the interface for election of DR/BDR.

The higher the value, the higher the priority. High priority will be taken into account when voting rights conflict. If a device has a priority of 0, it will not be elected as DR or BDR.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip ospf priority 2
```

17.42 Display OSPF Route Information

Command

```
show ip ospf route
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

show ip ospf route: the command is used to display the routing information learned by ospf protocol.

Note: The show ip route ospf command is used to display the route information shown in the routing table that learned by ospf protocol.

Instance

```
SwitchA> enable
SwitchA#configure terminal
SwitchA(config)#interface vlanif1
SwitchA(config- vlanif1)#ip address 192.168.1.1/24
SwitchA(config- vlanif1)#exit
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#ip interface vlan 2
SwitchA(config)#interface vlanif2
SwitchA(config- vlanif2)#ip address 192.168.2.2/24
SwitchA(config- vlanif2)#exit
SwitchA(config)#router ospf
SwitchA(config-router)#network 192.168.1.0/24 area 0
SwitchA(config-router)#network 192.168.2.0/24 area 0

SwitchB> enable
SwitchB#configure terminal
SwitchB(config)#vlan database
SwitchB(config-vlan)#vlan 2
SwitchB(config-vlan)#exit
SwitchB(config)#ip interface vlan 2
SwitchB(config)#interface vlanif2
SwitchB(config- vlanif2)#ip address 192.168.2.1/24
SwitchB(config- vlanif2)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#network 192.168.2.0/24 area 0
SwitchB(config-router)#end
Switch#show ip ospf route
O 192.168.1.0/24 [2] via 192.168.2.2, vlanif2, Area 0.0.0.0
C 192.168.2.0/24 [1] is directly connected, vlanif2, Area 0.0.0.0

Switch#show ip route ospf
O      192.168.1.0/24 [110/2] via 192.168.2.2, vlanif2, 00:26:23
```

17.43 Display OSPF Database Information

Command

```
show ip ospf database
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

show ip ospf database: the command is used to display the routing status database information of the ospf protocol.

Instance

```
SwitchA> enable
SwitchA#configure terminal
SwitchA(config)#interface vlanif1
SwitchA(config- vlanif1)#ip address 192.168.1.1/24
SwitchA(config- vlanif1)#exit
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#ip interface vlan 2
SwitchA(config)#interface vlanif2
SwitchA(config- vlanif2)#ip address 192.168.2.2/24
SwitchA(config- vlanif2)#exit
SwitchA(config)#router ospf
SwitchA(config-router)#network 192.168.1.0/24 area 0
SwitchA(config-router)#network 192.168.2.0/24 area 0
```

```
SwitchB> enable
SwitchB#configure terminal
SwitchB(config)#vlan database
SwitchB(config-vlan)#vlan 2
SwitchB(config-vlan)#exit
SwitchB(config)#ip interface vlan 2
SwitchB(config)#interface vlanif2
SwitchB(config- vlanif2)#ip address 192.168.2.1/24
```

```
SwitchB(config- vlanif2)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#network 192.168.2.0/24 area 0
SwitchB(config-router)#end
SwitchB#show ip ospf database
```

Router Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
192.168.2.1	192.168.2.1	570	0x80000003	0xe0bd	1
192.168.2.2	192.168.2.2	552	0x80000005	0xf825	2

Net Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	CkSum
192.168.2.2	192.168.2.2	571	0x80000001	0x881d

17.44 Display OSPF Neighbor Information

Command

```
show ip ospf neighbor
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

show ip ospf neighbor: the command is used to display neighbor information of the ospf protocol.

Instance

```
SwitchA> enable
SwitchA#configure terminal
SwitchA(config)#interface vlanif1
SwitchA(config- vlanif1)#ip address 192.168.1.1/24
SwitchA(config-vlanif1)#exit
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2
```

```
SwitchA(config-vlan) #exit
SwitchA(config) #ip interface vlan 2
SwitchA(config) #interface vlanif2
SwitchA(config- vlanif2) #ip address 192.168.2.2/24
SwitchA(config) #router ospf
SwitchA(config-router) #network 192.168.1.0/24 area 0
SwitchA(config-router) #network 192.168.2.0/24 area 0
```

```
SwitchB> enable
SwitchB#configure terminal
SwitchB(config) #vlan database
SwitchB(config-vlan) #vlan 2
SwitchB(config-vlan) #exit
SwitchB(config) #ip interface vlan 2
SwitchB(config) #interface vlanif2
SwitchB(config- vlanif2) #ip address 192.168.2.1/24
SwitchB(config-vlanif2) #exit
SwitchB(config) #router ospf
SwitchB(config-router) #network 192.168.2.0/24 area 0
SwitchB(config-router) #end
SwitchB#show ip ospf neighbor
```

OSPF process 0:

Neighbor ID	Pri	State	Dead Time	Address
Interface				
192.168.2.2	1	Full/DR	00:00:37	192.168.2.2
vlanif2				

18 BGP Configuration

18.1 Enter BGP Route Configuration View

Command

```
router bgp < AS-NUMBER >  
no router bgp < AS-NUMBER >
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

As-number: autonomous system number and the range is 1-4294967295.

Description

router bgp: the command is used to start the BGP process and enter BGP process mode.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100
```

18.2 Enter the IPv4 or IPv6 Address Family

Command

```
address-family { ipv4 | ipv6 }
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

address-family: the command is used to enter the ipv4/ ipv6 address family to configure BGP configuration mode.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4
Switch(config-router-af) #
```

18.3 BGP Route Aggregation Address

Command

```
aggregate-address <A.B.C.D/M > [as-set] [summary-only]
no aggregate-address <A.B.C.D/M > [as-set] [summary-only]
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

A.B.C.D/M: network address and mask.
as-set: generates a route with AS collection segments.
Summary-only: only the aggregated routes are announced, all routes are announced by default.

Description

aggregate-address: the command is used to create an aggregate route in the BGP routing table.

By default, routing aggregation is not performed.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #aggregate-address 10.0.0.0 255.0.0.0
as-set
```

18.4 BGP Always Comparison MED Value

Command

```
bgp always-compare-med
no bgp always-compare-med
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp always-compare-med: the command is used to set the BGP always compare MED.

By default, MED is only compared when AS is the same.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp always-compare-med
```

18.5 The BGP optimal Path Ignore the AS-Path Length

Command

```
bgp bestpath as-path ignore
no bgp bestpath as-path ignore
```


View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp bestpath as-path ignore: the command is used to configure to ignore the as-path length.

By default, the as-path length is considered when selecting the optimal path.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp bestpath as-path ignore
```

18.6 Comparison of AS-Path Length of BGP Optimum Path

Command

```
bgp bestpath compare-confed-aspath
no bgp bestpath compare-confed-aspath
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp bestpath compare-confed-aspath: the command is used to allow the same external routing to compare the aspath path length of the federation, the smaller the aspath length within the federation, the higher the path priority.

By default, the optimal path is chosen not by comparing ASPATHS from EBGp peer routes within the same federation, routing is optimized according to other conditions.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp bestpath compare-confed-aspath
```

18.7 BGP Optimum Path Routing ID Comparison

Command

```
bgp bestpath compare-routerid
no bgp bestpath compare-routerid
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp bestpath compare-routerid: the command is used for router ID that allows the same external routing comparison path, the smaller the router ID, the higher the path priority.

By default, when selecting the optimal path, two paths with the same path attributes will be received by different EBGp peers, The first one is not the one with the highest priority.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp bestpath compare-routerid
```

18.8 MED Property of BGP Optimum Path

Command

```
bgp bestpath med {[confed] [missing-as-worst]}
no bgp bestpath med {[confed] [missing-as-worst]}
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

Confed: compare MED in alliance path.

missing-as-worst: consider that the value of MED is the greatest when it is missing.

Description

bgp bestpath med confed: the command is used to compare the properties of med in the alliance path and to consider its value to be the maximum when the med is missing.

By default, the MED value of the path of the peers is not compared when selecting the optimal path.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp bestpath med confed
```

18.9 BGP Route Reflection

Command

```
bgp client-to-client reflection
no bgp client-to-client reflection
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp client-to-client reflection: the command is used to configure whether to process route reflection.

By default, route reflection is performed when the client is configured.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp client-to-client reflection
```

18.10 Configure the Group Identifier for the Routing Reflector

Command

```
bgp cluster-id {(A.B.C.D) | <0-4294967295>}
no bgp cluster-id
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

A.B.C.D: group identification, IP address format.

<0-4294967295> : group identification, decimal integer, value range is 0 ~ 4294967295, the system will process it into IP address format.

Description

bgp cluster-id: the command is used to configure the group identification of the route reflector.

By default, the identification is router-id of the router reflector.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp cluster-id 1.1.1.1
```

18.11 Configure the Identifier for the AS Alliance

Command

```
bgp confederation identifier <number>
no bgp confederation identifier [<number>]
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

Number: confederation identifier

Description

bgp confederation identifier: the command is used to configure the identifier for the AS confederation.

By default confederation identifier is not configured.

Confederation is another way to reduce the number of IBGP peer connections in autonomous systems. An autonomous system is divided into multiple sub-autonomous systems, and these sub-autonomous systems are formed into a confederation by setting a unified federation ID(i.e., confederation AS number). For the outside of the confederation, the whole confederation is still regarded as an AS, and only the AS number of the confederation is visible to the external. Within the confederation, full IBGP peer-to-peer connections are still established between BGP speakers within the sub-autonomous systems and EBGP connections between BGP speakers in the sub-autonomous systems. Although EBGP links have been established between BGP speakers in sub-autonomous systems, information exchange remains the same for next hop, MED, local priority, etc.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp confederation identifier 65000
```

18.12Configure the Member AS for the AS Alliance

Command

```
bgp confederation peers <as-number> [<as-number>]
no bgp confederation peers <as-number> [<as-number>]
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

as-number: AS, a member of the confederation. range :1-65535.

Description

bgp confederation peers: the command is used to configure the identifier for the AS confederation.

By default confederation member is not configured.

Confederation is a way to reduce the number of IBGP peer connections in autonomous systems. An autonomous system is divided into multiple sub-autonomous systems, and these sub-autonomous systems are formed into a confederation by setting a unified federation ID(i.e., confederation AS number). For the outside of the confederation, the whole confederation is still regarded as an AS, and there are other AS numbers of the confederation are visible to the external. Within the confederation, full IBGP peer-to-peer connections are still established between BGP speakers within the sub-autonomous systems and EBGP connections between BGP speakers in the sub-autonomous systems. Although EBGP links have been established between BGP speakers in sub-autonomous systems, information exchange remains the same for next hop, MED, local priority, etc. This command specifies AS, a member of the alliance.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp confederation peers 100 110
```

18.13 EBGP Route Suppression

Command

```
bgp dampening { [<half-life>] [<reusing> <suppressing> <duration>]
| [route-map <WORD>] }
no bgp dampening { [<half-life>] [<reusing> <suppressing>
<duration>] | [route-map [<WORD>]] }
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

Half-life: Specifies how long to interval the penalty value is halved in minutes, ranging from 1 to 45 minutes, default is 15 minutes.

Reusing: do not dampen the routing when the penalty value drops to this value, ranging from 1-20000, default to 750.

Suppressing: dampen the routing when the penalty value reaches the value, the range is 1-20000, the default value is 2000.

duration: the maximum duration of routing suppression, beyond which the routing suppression is automatically unmounted, is in minutes, ranging from 1 to 255, default is 60 minutes.

WORD: the name of oute-map, which applies routing attenuation to specific routes via route-map.

Route attenuation is applied to all routes by default.

Description

bgp dampening: the command is used to suppress unstable EBGp route and is invalid to the IBGP routing.

By default confederation member is not configured.

BGP uses the concept of penalty values to describe the stability of the route. The higher the penalty value, the more unstable the route. The penalty value is increased by 1000 per routing concussion (when withdraw message is received). When the penalty value increases to a certain level, it will not increase again. This value is called the penalty upper limit. The value depends on the duration value configured by the user, and the calculation formula is: $\text{Penalty upper limit} = 2^{\text{duration} / \text{half-life}}$ * reusing. At the same time, the upper limit of penalty value cannot be greater than 20000, so duration, half-life and reusing values should be adjusted according to the network conditions during configuration. These parameters roughly satisfy the following requires: 1) half-time and duration : half-time $\leq$ duration; 2) reusing, suppressing and penalty upper limit: reusing $\leq$ suppressing $\leq$ penalty upper limit.

The user can also specify other half - life value, the value of duration is (half - life * 4), and reusing and suppressing values are 750 and 2000 respectively. EBGp routes with penalty value exceeds suppressing value will be suppressed, suppressed routing in BGP routing in the process of the election will not be used, also won't notice to other BGP peers. If the suppressed route continues concussion, the penalty will continue to rise to the penalty upper limit. For every half-life time a suppressed route

passes, the penalty is reduced by half. When the penalty value is reduced to the reusing value, the route that was updated at the last update will re-participate in the BGP routing election. When the penalty value is reduced to 0, the route that is withdraw message at the last update will be deleted from the BGP routing table.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp dampening 30 1200 10000 120
```

18.14 Set the BGP Address Family to IPv4 Unicast by Default

Command

```
bgp default ipv4-unicast
no bgp default ipv4-unicast
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp default ipv4-unicast: the command is used to set the address family to a unicast address that defaults to ipv4.

By default, IPv4 unicast is used for neighbor relationship build.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp default ipv4-unicast
```


18.15 The Default Local Priority Value for BGP

Command

```
bgp default local-preference <0-4294967295>
no bgp default local-preference [<0-4294967295>]
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

<0-4294967295>: default local priority.

Description

bgp default local-preference: the command is used to set the default local-preference property value.

By default, the local priority value is 100.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp default local-preference 200
```

18.16 Compare MED Values of the Same AS Counterparts

Command

```
bgp deterministic-med
no bgp deterministic-med
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp deterministic-med: the command is used to set path precedence for comparing med values from peers of the same AS.

By default, comparisons are made in path receive order, the most recently received path being compared first.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp deterministic-med
```

18.17 Force the AS-Path of the First Location to be the EBGp Route

Command

```
bgp enforce-first-as
no bgp enforce-first-as
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp enforce-first-as: the command is used to set up that when BGP receives an external route, the forced route's as-path must contain the neighbor's as number in the position of the first as or break the peer's connection.

By default it is not configured.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp enforce-first-as
```

18.18 Reset the Direct Connection EBGP Fault Interface

Command

```
bgp fast-external-failover
no bgp fast-external-failover
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp fast-external-failover: the command is used to set up a BGP session connection to be quickly closed when the network interface used by the directly connected EBGP peer to establish the connection fails.

By default this function is configured.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp fast-external-failover
```

18.19 Record BGP Status Change Information

Command

```
bgp log-neighbor-changes
no bgp log-neighbor-changes
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

bgp log-neighbor-changes: the command is used to enable the state message of the BGP to be recorded when the debug is not turned on.

By default this function is configured.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp log-neighbor-changes
```

18.20 BGP Route ID

Command

```
bgp router-id <A.B.C.D >
no bgp router-id [<A.B.C.D >]
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

A.B.C.D: router ID

Description

bgp router-id: the command is used to set the ID of the router.

By default, the router ID is automatically obtained.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp router-id 1.1.1.1
```

18.21 BGP Next Hop Detection Interval

Command

```
bgp scan-time <interval>
no bgp scan-time [<interval>]
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

interval: the interval between checks.

Description

bgp scan-time: the command is used to set the time interval between which BGP periodically checks whether the next hop of the route is valid.

By default, the interval is 60.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #bgp scan-time 45
```

18.22 Specifies the Management Distance for the Routing Prefix

Command

```
distance <distance> <A.B.C.D/M>
no distance <distance> <A.B.C.D/M>
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

distance: management distance, the range is 1-255.

A.B.C.D/M: route prefix.

Description

distance: the command is used to set the administrative distance for the specified route prefix.

By default it is not configured.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #distance 100 10.12.1.0/24
```

18.23 Managed Distances for Internal/External/Local BGP Routes

Command

```
distance bgp <EXTERNAL> <INTERNAL> <LOCAL>
no distance bgp <EXTERNAL> <INTERNAL> <LOCAL>
```

View

BGP Configuration View

Default Level

2: Configuration level

Parameters

External: BGP external (EBGP) management distance, the range is 1-255.

Internal: BGP internal (IBGP) management distance, the range is 1-255.

local: local management distance, the range is 1-255.

Description

distance bgp: the command is used to set different management distances for different types of BGP routes.

By default, EBGP management distance is 20, IBGP management distance is 200, and local route management distance is 200.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #distance bgp 30 180 180
```

18.24 Exit the BGP IPv4 or IPv6 Address Family

Command

```
exit-address-family
```

View

IPv4 or IPv6 Address Family of BGP Configuration View

Default Level

2: Configuration level

Parameters

-

Description

The exit-address-family: the command is used to exit the BGP IPv4 or IPv6 address family configuration view.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router) #address-family ipv4
Switch(config-router-af) #exit-address-family
```

18.25Network Segment Routing Notification BGP Routing Table

Command

```
network {<A.B.C.D > |<A.B.C.D/M >} [route-map <map-name>]
[backdoor]
no network {<A.B.C.D > |<A.B.C.D/M >} [route-map <map-name>]
[backdoor]
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D/M: network address and mask.

Map-name: the name of the route-map. Route map name should be no more than 32 characters.

backdoor: this route is backdoor route. Enables router to select the route learned from IGP first instead of the route learned from IBGP neighbors.

Description

network: the command is used to notify segment route to the BGP route table.
By default, BGP does not notify any network segment route.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#network 10.11.20.0/24
```

18.26Route Synchronization Notify Network Information

Command

```
network synchronization
no network synchronization
```

View

BGP configuration view,the IPv4 or IPv6 address family configuration view of the BGP

Default Level

2: Configuration level

Parameters

-

Description

network synchronization: the command is used to configure the synchronize of BGP and the local route before announcing the network information configured by the network.

By default, BGP directly announces the network route, regardless of whether it is synchronized with the local route.

It is not recommended to turn off the switch, which may cause a routing black hole.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#network synchronization

Switch > enable
```



```
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config)#address-family ipv4  
Switch(config- router r-af)#network synchronization
```

18.27 Configure BGP Peers/Peer Groups

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} remote-as < AS-number >  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} remote-as <  
AS-number >
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

As-number: BGP peer (group) autonomous system number and the range is 1-65535.

Description

neighbor remote-as: the command is used to configure the BGP peer/peer group.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
```

18.28 Activate the Specified Peer/Peer Group

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} activate  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} activate
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group

Description

neighbor activate: the command is used to activate the specified peer/peer group.

By default, it is active.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 activate
```

18.29The Time Interval between Sending BGP Routing Update Packets

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} advertisement-interval
< seconds >
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>}
advertisement-interval < seconds >
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

seconds: the time interval in which routing updates are sent. Range: 0-600 seconds.

Description

neighbor advertisement-interval: the command is used to set the time interval between sending BGP routing updates.

By default, the same routing update message is sent to an internal peer group at a 5-second interval and to an external peer group at a 30-second interval.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#neighbor 1.1.1.1 remote-as 200
Switch(config-router)#neighbor 1.1.1.1 advertisement-interval 10
```

18.30The Number of Occurrences of the Same AS in the Neighbor Route AS List

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} allowas-in [< numbers >]
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} allowas-in [< numbers>]
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Numbers: the times an AS number is allowed to repeat. range :1-10.

Description

neighbor allowas-in: the command is used to specify the number of times the same AS is allowed in the neighbor's routing AS list.

By default, AS is not allowed to be repeated on the same route. When repetition is configured to allow , the default repeat times allowed without the <1-10> parameter is 3.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 allowas-in 10
```

18.31The Time Interval Between Sending the Local Originating BGP Route

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} as-origination-interval
<seconds >
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>}
as-origination-interval <seconds >
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group

seconds: the time interval between sending local originating BGP routes. Range:
1-600 seconds.

Description

The neighbor as-origination interval command is used to configure the time interval between notifying a specified peer of a local originating BGP route.

By default, the time interval for sending a local originating BGP route is 15 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 as-origination-interval
100
```

18.32 The Routing Properties Associated with the Transport Neighbors Remain Unchanged

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} attribute-unchanged  
[as-path] [med] [next-hop]  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} attribute-unchanged  
[as-path] [med] [next-hop]
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group

as-path: as-path property.

med: med property.

next-hop : next-hop property

Description

The neighbor attribute-unchanged command is used to configure that the related routing property will not be changed when passed to the specified neighbor.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch (config)#router bgp 100  
Switch(config-router)#neighbor 1.1.1.1 remote-as 200  
Switch(config-router)#neighbor 1.1.1.1 attribute-unchanged
```

18.33 Dynamic Updates and Routing Refreshes with Neighbors

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} capability {dynamic  
| route-refresh}  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} capability {dynamic  
| route-refresh}
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group

Dynamic: dynamic update capability negotiation.

route-refresh: route refresh capability negotiation.

Description

neighbor capability: The command is used to configure dynamic update and routing refresh capability negotiation with neighbors. Through this configuration, negotiate the capability supported by both parties in the OPEN message. If the capability is supported by the end, a response will be given; otherwise, NOTIFICATION will be sent, and the initiator will send OPEN without the capability to re-establish the connection. Dynamic capability means that a connection does not have to be restarted when the supported address family negotiation changes. Routing refresh is to issue a routing refresh request when some properties can be configured for soft reset and the other party can resend the existing route to the originating end. With the routing refresh property configured, user can use the `clear ip bgp * soft` in command to refresh when changing policy without rebuilding the connection. By default: configure routing refresh capability instead of dynamic update capability.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100
```

```
Switch(config- router)#neighbor 1.1.1.1 remote-as 200  
Switch(config- router)#neighbor 1.1.1.1 capability dynamic
```

18.34Egress Route Filter with Neighbor

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} capability orf  
prefix-list {<both>|<send>|<receive>}  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} capability orf  
prefix-list {<both>|<send>|<receive>}
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address

X:X::X:X: IPv6 peer interface address

WORD: name of the peer group

both: receives and sends the prefix-list filter rule

send: sends the prefix-list filter rule

receove: receives the prefix-list filter rule

Description

neighbor capability orf prefix-list: the command is used to configure the outlet with the neighbor to be negotiated by the filter function. Through this configuration, negotiate the capability supported by both parties in the OPEN message. If the capability is supported by the end, a response will be given; otherwise, NOTIFICATION will be sent, and the initiator will send OPEN without the capability to re-establish the connection. After this capability is configured, the party that has the prefix-list filter rule configured sends its own filter rule to the peer when the connection is established, and the peer applies its own rule to avoid sending the route that will be filtered on the other side.

By default ORF function is not configured.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100
```

```
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 capability orf
prefix-list both
```

18.35 TCP Connection Collision Detection with Neighbor

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} collide-established
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} collide-established
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group

Description

neighbor collide-established: the command is used to enable conflict detection and resolution in the event of a TCP connection conflict.

By default, it is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 collide-established
```

18.36 Send a Default Route to a Peer/Peer Group

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} default-originate
[route-map <WORD>]
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} default-originate
[route-map <WORD>]
```


View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

WORD: the name of the route map.

Description

neighbor default-originate: the command is used to send the default route to the peer/peer group.

By default: no default route is sent to peer/peer groups.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#neighbor 1.1.1.1 remote-as 200
Switch(config-router)#neighbor 1.1.1.1 default-originate
```

18.37Peer/Peer Group Description Information

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} description <LINE>
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} description [<LINE >]
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

LINE: description information for peers.

Description

neighbor description: the command is used to configure description information for peer/peer groups.

By default: peer/peer group does not have description information.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 description test
```

18.38 Filtering Strategy Based on ACL

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} distribute-list
{<access-list-number> | <WORD>} {in | out}
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} distribute-list
{<access-list-number> | <WORD>} {in | out}
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

access-list-number: ACL number.

WORD: ACL name.

Description

neighbor distribution-list: the command is used to set up acl-based filtering policies for peer and peer groups.

By default: no ACL based filtering policy is set for peer/peer groups.

Whether for the input (in) or output rules (out), at any time, the command and neighbor prefix-list can not coexist, only one command is effective.

Instance

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 distribute-list 1 in
```

18.39No Capacity Negotiation when Establishing a Connection

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>}
dont-capability-negotiate
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>}
dont-capability-negotiate
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address

X:X::X:X: IPv6 peer interface address

WORD: name of the peer group

Description

neighbor dont-capability-negotiate: the command is used to configure that do not carry out the ability negotiation when a connection is established.

By default, ability negotiation is carried out.

By default, capability negotiation occurs when the connection is established with the other side, so this configuration allows users to establish a connection without capability negotiation when knowing that the other side is an older version of BGP that does not support capability negotiation.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1
dont-capability-negotiate
```

18.40 Allows Non-directly Connected Neighbors to Establish EBGp Sessions

Command

```
neighbor {<A.B.C.D> | <X:X::X:X> | <WORD>} ebgp-multihop [<count>]  
no neighbor {<A.B.C.D> | <X:X::X:X> | <WORD>} ebgp-multihop  
[<count>]
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Count: number of hops allowed, range 1-255.

Description

neighbor ebgp-multihop: the command is used to configure to allow EBGp sessions to be established with neighbors on non-directly connected networks.

By default: EBGp sessions are not allowed with neighbors on indirectly connected networks.

Set the parameter count to configure the maximum router hops for EBGp sessions at the same time, and 255 hops without the parameter count.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config- router)#neighbor 1.1.1.1 remote-as 200  
Switch(config- router)#neighbor 1.1.1.1 ebgp-multihop
```

18.41 Force Direct Contact with Neighbors for Multiple Hop

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} enforce-multihop  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} enforce-multihop
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor enforce-multihop: the command is used to configure the connection to the neighbor to multihop.

By default, it is not configured.

Direct connection routing cannot be forced to be multi-hop, but with this configuration, the system can be forced to treat the connection as a multi-hop connection. That is to say, the checks that were originally made only for IBGP and EBGP of non-directly connected routes, all are checked after this property is set. At the ingress, there is no direct connection check for the next jump in case of forced multi-jump.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config- router)#neighbor 1.1.1.1 remote-as 200  
Switch(config- router)#neighbor 1.1.1.1 enforce-multihop
```

18.42 AS-Path Access List Filtering

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} filter-list <WORD> {in  
| out}
```

```
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} filter-list <WORD>
{in | out}
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group

WORD: as-path list name.

Description

neighbor filter-list: the command is used to configure access list control for AS-PATH when routing information is sent and received with a specified BGP peer (group).

By default, it is not configured.

After the IP AS-PATH access list is first configured and applied to the specified neighbor, user can control to send/receive route with the specified AS number in the AS list to that neighbor. Accept and reject depend on settings of the access list, while issue and receive are set by this command.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ip as-path access-list test deny 100
Switch(config)#router bgp 100
Switch(config-router)#neighbor 1.1.1.1 remote-as 200
Switch(config-router)#neighbor 1.1.1.1 filter-list test out
```

18.43 Configure the Interface to the BGP Peer/Peer Group

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} interface <WORD>
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} interface <WORD>
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

WORD: interface name.

Description

neighbor interface: the command is used to configure the interface connected to the BGP peer (group).

By default, it is not configured.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#router bgp 100
```

```
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
```

```
Switch(config- router)#neighbor 1.1.1.1 interface vlanif2
```

18.44Number of Received Peer Prefixes

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} maximum-prefix <limit>  
[threshold] [warning-only]
```

```
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} maximum-prefix <limit>  
[threshold] [warning-only]
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

limit: the upper limit of the number of items allowed to receive routing information, ranging from 1-4294967295.

threshold: specifies a value that starts generation of warnings and a maximum number of percentages, ranging from 1 to 100, and defaults to 75.

Warning-only: when routing information reaches the limit, the BGP connection is terminated and a log message is generated.

Description

neighbor maximum-prefix: the command is used to configure the limit on the number of prefixes received from the specified BGP peer.

By default, it is not limited.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#neighbor 1.1.1.1 remote-as 200
Switch(config-router)#neighbor 1.1.1.1 maximum-prefix 100
```

18.45 Force Next-hop Addresses as Neighbors

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} next-hop-self
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} next-hop-self
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor next-hop-self: the command is used to configure a route that requires the neighbor to make the next hop to the local route.

By default, it is not configured.

In the EBGp environment, the next hop automatically points to the source neighbor, but in the IBGP environment, if the same network segment is routed, the original next hop remains unchanged. But if it is not a broadcast network, there will be a problem,

so this command can be used to force to use itself as neighbor's next hop as long as it is in IBGP.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 next-hop-self
```

18.46Ignore the Results of Peer Capacity Negotiation

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} override-capability
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} override-capability
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor override-capability: the command is used to configure the result of ignoring the BGP peer (group) capability negotiation.

By default, it is not configured.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 override-capability
```

18.47The Peer Connection is Passive

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} passive  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} passive
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor passive: the command is used to configure the connection to the BGP peer (group) to be passive and not to actively send the connection request.

By default: initiate the connection.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config- router)#neighbor 1.1.1.1 remote-as 200  
Switch(config- router)#neighbor 1.1.1.1 passive
```

18.48Create a BGP Peer Group

Command

```
neighbor <WORD> peer-group  
no neighbor <WORD> peer-group
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

WORD: name of the peer group

Description

neighbor <WORD>peer-group: the command is used to create the BGP peer group.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor test peer-group
```

18.49Add a Peer Group Member

Command

```
neighbor {<A.B.C.D > | <X:X::X:X>} peer-group <WORD>
no neighbor {<A.B.C.D > | <X:X::X:X> } peer-group <WORD>
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address

X:X::X:X: IPv6 peer interface address

WORD: name of the peer group

Description

neighbor {< A.B.C.D> | <X:X: X:X>} peer group <WORD> : the command is used to add a specified BGP peer to a peer group.

By default, it have not joined the peer group.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor test peer-group
Switch(config- router)#neighbor 1.1.1.1 peer-group test
```

18.50 TCP Port Number for Communicating with Neighbors

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} port < number >  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} port < number >
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.
X:X::X:X: IPv6 peer interface address.
WORD: name of the peer group.
number: TCP port number, the range is 0-65535.

Description

neighbor passive: The command is used to configure the TCP port number to communicate with the neighbor.

By default, the port number is 179.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config-router)#neighbor 1.1.1.1 remote-as 200  
Switch(config-router)#neighbor 1.1.1.1 port 1022
```

18.51 Routing Filtering Strategy based on IP Prefix List

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} prefix-list < WORD >  
{in | out}  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} prefix-list < WORD >  
{in | out}
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

WORD: IP prefix list name.

Description

neighbor prefix-list: the command is used to set a routing filter policy based on the IP prefix list for peer/peer groups.

By default, no route filtering strategy based on IP prefix list.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#neighbor 1.1.1.1 remote-as 200
Switch(config-router)#neighbor 1.1.1.1 prefix-list test
```

18.52BGP Update Message Removes Private AS

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} remove-private-AS
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} remove-private-AS
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor remote-private-AS: the command is used to configure sending BGP update messages without carrying a private autonomous system number.

By default, BGP update messages are sent with a private autonomous system number.

Private AS numbers range from 64512 to 65535.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 remove-private-AS
```

18.53Route Mapping Strategy

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} route-map < WORD > {in
| out}
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} route-map < WORD >
{in | out}
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

WORD: IP prefix list name.

Description

neighbor route-map: the command is used to configure the route mapping policy to be applied when sending or receiving routes from a neighbor.

Default: no filtering policy based on routing map .

Instance

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#router bgp 100  
Switch(config- router)#neighbor 1.1.1.1 remote-as 200  
Switch(config- router)#neighbor 1.1.1.1 route-map test
```

18.54Route Reflection

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} route-reflector-client  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>}  
route-reflector-client
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor route-reflector-client: the command is used to configure native as the route reflector and peer/peer groups as the route reflector client.

By default: route reflector and its clients are not configured.

Route reflection is used to reduce the number of peers when the IBGP router inside the AS is larger, and its clients only exchange information with the route reflector, which handles the exchange of information between clients and with other IBGP and EBGp routers. This command configure itself as a route reflector and the specified peer (group) as its client. Note: this configuration can only be conducted within AS.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config- router)#neighbor 1.1.1.1 remote-as 200  
Switch(config- router)#neighbor 1.1.1.1 route-reflector-client  
Switch(config- router)#neighbor 3.3.3.3 remote-as 200  
Switch(config- router)#neighbor 3.3.3.3 route-reflector-client
```

18.55 Router Server

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} route-server-client  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} route-server-client
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor route-server-client: the command is used to configure the native as the routing server and the peer/peer group as the routing server client.

By default: no routing server and its clients are configured.

Routing service is used to reduce the number of peers between AS routers in EBGp environment. When the clients exchange information through the routing server, the server transparently transmits the routing message to other clients.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config- router)#neighbor 1.1.1.1 remote-as 200  
Switch(config- router)#neighbor 1.1.1.1 route-server-client  
Switch(config- router)#neighbor 3.3.3.3 remote-as 300  
Switch(config- router)#neighbor 3.3.3.3 route-server-client
```

18.56 Community Property Transfer

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} send-community [both  
| extended | standard]  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} send-community [both  
| extended | standard]
```


View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

both: both standard and extended groups are transmitted

extended: only extended groups are transmitted.

Standard: only standard groups are transmitted.

Description

neighbor send-community: the command is used to specify the transmission of group attributes to the specified BGP neighbor.

By default: group attributes is sent.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 send-community
```

18.57Disable BGP Connection

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} shutdown
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} shutdown
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor shutdown: the command is used to close a BGP connection with a specified BGP peer.

By default: the connection is not closed.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 shutdown
```

18.58Store BGP Original Routing Information

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} soft-reconfiguration
inbound
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} soft-reconfiguration
inbound
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor soft-reconfiguration: the command is used to allow the storage of original routing information from BGP peers.

By default: storage is not allowed.

When configured to allow the storage of original routing information from BGP peers, the system will first store the original routing information in the cache and apply it to the end immediately after restart, thus reducing the consumption of exchange with other routers. This command makes sense when the routing refresh capability is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#neighbor 1.1.1.1 remote-as 200
Switch(config-router)#neighbor 1.1.1.1 soft-reconfiguration
inbound
```

18.59 Strict Ability Matching Connection

Command

```
neighbor {<A.B.C.D> | <X:X::X:X> | <WORD>} strict-capability-match
no neighbor {<A.B.C.D> | <X:X::X:X> | <WORD>}
strict-capability-match
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor strict-capability-match: the command is used to configure a capability match that is strictly required when establishing a connection.

By default, strict capability matching is not configured.

This command is only valid for BGP multi-protocol. After the use of this command, the neighbor can only be established when the BGP multi-protocol capabilities of both parties match. Otherwise, it cannot be established. Whether or not other abilities are matched does not affect the establishment of neighbors.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#neighbor 1.1.1.1 remote-as 200
Switch(config-router)#neighbor 1.1.1.1 strict-capability-match
```

18.60BGP Session Timer with the Specified Peer

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} timers { <keepalive>
<holdtime> | connect < connect -time>}
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} timers { <keepalive>
<holdtime> | connect < connect -time>}
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

keepalive: the time interval between sending KEEPALIVE messages to a specified BGP peer, range: 0-65535 seconds.

holdtime: specifies the interval between BGP peer sending KEEPALIVE messages, range: 0-65535 seconds.

connect-time: time interval for initiating a reconnection to a specified BGP peer, range: 1-65535 seconds.

Description

neighbor timers: the command is used to configure the alive time interval and hold times of BGP sessions established with a specified peer/peer group, as well as the reconnection interval.

By default, keepalive time is 60s, holdtime is 240s and connect-time is 120s.

It is recommended that keepalive value should not be greater than one third of holdtime.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#neighbor 1.1.1.1 remote-as 200
Switch(config-router)#neighbor 1.1.1.1 timers 50 150
```

18.61 Unsuppress the Routing Map

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} unsuppress-map <WORD>  
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} unsuppress-map <WORD>
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

WORD: the name of the route-map.

Description

neighbor unsuppress-map: the command is used to configure or cancel unsuppress of cases that match the specified routing map.

By default, it is not configured.

This function is mainly for specific routes that are aggregated and summary-only suppressed. Routes that meet the routing mapping conditions are not suppressed in this case and are still issued separately.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch#access-list 3 permit 100.1.3.0  
Switch(config)#route-map test permit 10  
Switch (config-route-map)#match ip address 3  
Switch (config-route-map)#exit  
Switch(config)#router bgp 100  
Switch(config- router)#neighbor 1.1.1.1 remote-as 200  
Switch(config- router)#neighbor 1.1.1.1 unsuppress-map test
```

18.62 Specify the BGP Connection Interface

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} update-source < WORD >
```

```
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} update-source <WORD >
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

WORD: interface name or address.

Description

neighbor update-source: the command is used to set up the network interface to be used when establishing a BGP connection in a specified IBGP peer.

By default: use the best local interface as the output interface.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 update-source vlanif1
```

18.63Configure the BGP Version of the Peer

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} version
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} version
```

View

BGP configuration view,IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Description

neighbor version: the command is used to configure the BGP version number of the peer, currently only version 4 available.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 version 4
```

18.64 Configure the Weight Value of the Peer

Command

```
neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} weight <value>
no neighbor {<A.B.C.D > | <X:X::X:X> | <WORD>} weight <value>
```

View

BGP configuration view, IPv4 or IPv6 address family of BGP configuration view

Default Level

2: Configuration level

Parameters

A.B.C.D: IPv4 peer interface address.

X:X::X:X: IPv6 peer interface address.

WORD: name of the peer group.

Value: neighbor's weight. value range is 0-65535.

Description

neighbor weight: the command is used to configure the weights of the peer.

By default: routes from other routers have a default weight of 0. The weight of the local static configuration defaults to 32768.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config- router)#neighbor 1.1.1.1 remote-as 200
Switch(config- router)#neighbor 1.1.1.1 weight 40
```

18.65 Introduce Additional Routing Information to the BGP

Command

```
redistribute { connected| static| ospf |rip} [route-map<word>]  
no redistribute { connected| static| ospf| rip} [route-map<word>]
```

View

BGP View

Default Level

2: Configuration level

Parameters

connected: connected route

static: static route;

ospf: OSPF route.

rip: RIP route.

<word>: a pointer to the route map used to introduce routes.

Description

redistribute: the command introduces routes learned from other routing protocols into BGP.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#router bgp 100  
Switch(config- router)#redistribute ospf
```

18.66 BGP Connection Survival Interval and Holdtime

Command

```
timers bgp <keepalive> <holdtime>  
no timers basic
```

View

BGP View

Default Level

2: Configuration level

Parameters

keepalive: keepalive interval, the range is 0-65535 seconds.

holdtime: the range is 0-65535 seconds.

Description

timers bgp: the command is used to configure the intervals of the BGP connection alive time and hold time.

By default, BGP connections have a survival interval of 60 seconds and a retention time of 180 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#router bgp 100
Switch(config-router)#timers bgp 80 200
```

18.67 Display BGP Route Information

Command

```
show ip bgp [<A.B.C.D >] [<A.B.C.D/M >]
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: IP address.

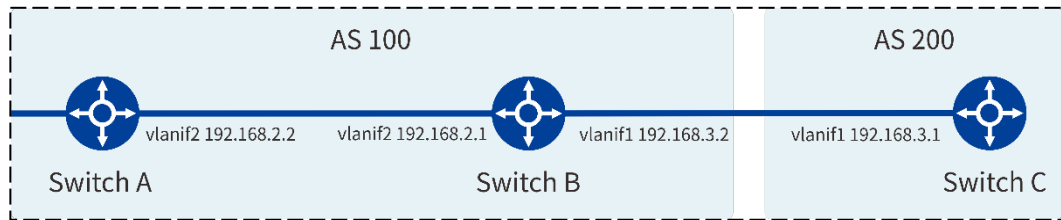
A.B.C.D/M: IP address and mask.

Description

show ip bgp: command is used to display routing information maintained by BGP.

Instance

Networking: As shown in the figure below, device A is connected to device B through VLANIF2, and device B is connected to device C through VLANIF1. Device C displays routing information maintained by BGP via command.



```

SwitchA> enable
SwitchA#configure terminal
SwitchA(config)#interface vlanif1
SwitchA(config- vlanif1)#ip address 192.168.1.1/24
SwitchA(config- vlanif1)#exit
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#ip interface vlan 2
SwitchA(config)#interface vlanif2
SwitchA(config- vlanif2)#ip address 192.168.2.2/24
SwitchA(config- vlanif2)#exit
SwitchA(config)#ip interface loopback 0
SwitchA(config)#interface loopback0
SwitchA(config- loopback0)#ip address 2.2.2.2/32
SwitchA(config- loopback0)#exit
SwitchA(config)#router ospf
SwitchA(config-router)#router-id 2.2.2.2
SwitchA(config-router)#network 192.168.1.0/24 area 0
SwitchA(config-router)#network 192.168.2.0/24 area 0
SwitchA(config-router)#network 2.2.2.2/32 area 0
SwitchA(config-router)#exit
SwitchA(config)#router bgp 100
SwitchA(config-router)#bgp router-id 2.2.2.2
SwitchA(config-router)#network 192.168.1.0/24
SwitchA(config-router)#network 192.168.2.0/24
SwitchA(config-router)#neighbor 1.1.1.1 remote-as 100

SwitchB> enable
SwitchB#configure terminal
SwitchB(config)#interface vlanif1
SwitchB(config- vlanif1)#ip address 192.168.3.2/24
SwitchB(config- vlanif1)#exit
SwitchB(config)#vlan database
SwitchB(config-vlan)#vlan 2
SwitchB(config-vlan)#exit
SwitchB(config)#ip interface vlan 2
SwitchB(config)#interface vlanif2

```

```
SwitchB(config- vlanif2)#ip address 192.168.2.1/24
SwitchB(config-vlanif2)#exit
SwitchB(config)#ip interface loopback 0
SwitchB(config)#interface loopback0
SwitchB(config-loopback0)#ip address 1.1.1.1/32
SwitchB(config-loopback0)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#router-id 1.1.1.1
SwitchB(config-router)#network 1.1.1.1/32 area 0
SwitchB(config-router)#network 192.168.2.0/24 area 0
SwitchB(config-router)#network 192.168.3.0/24 area 0
SwitchB(config-router)#exit
SwitchB(config)#router bgp 100
SwitchB(config-router)#bgp router-id 1.1.1.1
SwitchB(config-router)#network 192.168.1.0/24
SwitchB(config-router)#network 192.168.2.0/24
SwitchB(config-router)#neighbor 2.2.2.2 remote-as 100
SwitchB(config-router)#neighbor 3.3.3.3 remote-as 200

SwitchC> enable
SwitchC#configure terminal
SwitchC(config)#interface vlanif1
SwitchC(config- vlanif1)#ip address 192.168.3.1/24
SwitchC(config- vlanif1)#exit
SwitchC(config)#ip interface loopback 0
SwitchC(config)#interface loopback0
SwitchC(config- loopback0)#ip address 3.3.3.3/32
SwitchC(config- loopback0)#exit
SwitchC(config)#router ospf
SwitchC(config-router)#router-id 3.3.3.3
SwitchC(config-router)#network 192.168.3.0/24 area 0
SwitchC(config-router)#network 3.3.3.3/32 area 0
SwitchC(config- router)#exit
SwitchC(config)#router bgp 200
SwitchC(config-router)#bgp router-id 3.3.3.3
SwitchC(config-router)#network 192.168.3.0/24
SwitchC(config-router)#neighbor 1.1.1.1 remote-as 100
SwitchC(config-router)#end
SwitchC#show ip bgp
BGP table version is 1, local router ID is 3.3.3.3
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
*> 192.168.3.0	0.0.0.0		100	32768	i

Total number of prefixes 1

18.68 Display BGP IPv4 Unicast Route Information

Command

```
show ip bgp ipv4 unicast [<A.B.C.D >] [<A.B.C.D/M >]
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: IP address.

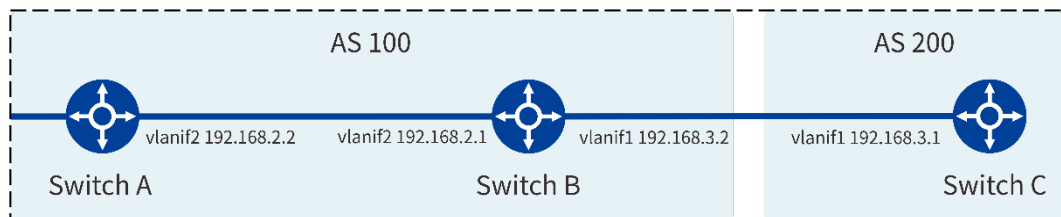
A.B.C.D/M: IP address and mask.

Description

show ip bgp: the command is used to display ipv4 unicast routing information maintained by BGP.

Instance

Networking: device A is connected to device B via VLANIF2, and device B is connected to device C via VLANIF1 as shown in the figure below. Device C displays the IPv4 unicast routing information maintained by BGP via command.



```
SwitchA> enable
```

```
SwitchA#configure terminal
```

```
SwitchA(config)#interface vlanif1
```

```
SwitchA(config-vlanif1)#ip address 192.168.1.1/24
```

```
SwitchA(config-vlanif1)#exit
```

```
SwitchA(config)#vlan database
```

```
SwitchA(config-vlan)#vlan 2
```

```
SwitchA(config-vlan)#exit
```

```
SwitchA(config)#ip interface vlan 2
```

```
SwitchA(config)#interface vlanif2
SwitchA(config- vlanif2)#ip address 192.168.2.2/24
SwitchA(config- vlanif2)#exit
SwitchA(config)#ip interface loopback 0
SwitchA(config)#interface loopback0
SwitchA(config- loopback0)#ip address 2.2.2.2/32
SwitchA(config- loopback0)#exit
SwitchA(config)#router ospf
SwitchA(config-router)#router-id 2.2.2.2
SwitchA(config-router)#network 192.168.1.0/24 area 0
SwitchA(config-router)#network 192.168.2.0/24 area 0
SwitchA(config-router)#network 2.2.2.2/32 area 0
SwitchA(config-router)#exit
SwitchA(config)#router bgp 100
SwitchA(config-router)#bgp router-id 2.2.2.2
SwitchA(config-router)#network 192.168.1.0/24
SwitchA(config-router)#network 192.168.2.0/24
SwitchA(config-router)#neighbor 1.1.1.1 remote-as 100
```

```
SwitchB> enable
SwitchB#configure terminal
SwitchB(config)#interface vlanif1
SwitchB(config- vlanif1)#ip address 192.168.3.2/24
SwitchB(config- vlanif1)#exit
SwitchB(config)#vlan database
SwitchB(config-vlan)#vlan 2
SwitchB(config-vlan)#exit
SwitchB(config)#ip interface vlan 2
SwitchB(config)#interface vlanif2
SwitchB(config- vlanif2)#ip address 192.168.2.1/24
SwitchB(config-vlanif2)#exit
SwitchB(config)#ip interface loopback 0
SwitchB(config)#interface loopback0
SwitchB(config- loopback0)#ip address 1.1.1.1/32
SwitchB(config- loopback0)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#router-id 1.1.1.1
SwitchB(config-router)#network 1.1.1.1/32 area 0
SwitchB(config-router)#network 192.168.2.0/24 area 0
SwitchB(config-router)#network 192.168.3.0/24 area 0
SwitchB(config-router)#exit
SwitchB(config)#router bgp 100
SwitchB(config-router)#bgp router-id 1.1.1.1
```

```

SwitchB(config-router)#network 192.168.1.0/24
SwitchB(config-router)#network 192.168.2.0/24
SwitchB(config-router)#neighbor 2.2.2.2 remote-as 100
SwitchB(config-router)#neighbor 3.3.3.3 remote-as 200

SwitchC> enable
SwitchC#configure terminal
SwitchC(config)#interface vlanif1
SwitchC(config- vlanif1)#ip address 192.168.3.1/24
SwitchC(config- vlanif1)#exit
SwitchC(config)#ip interface loopback 0
SwitchC(config)#interface loopback0
SwitchC(config- loopback0)#ip address 3.3.3.3/32
SwitchC(config- loopback0)#exit
SwitchC(config)#router ospf
SwitchC(config-router)#router-id 3.3.3.3
SwitchC(config-router)#network 192.168.3.0/24 area 0
SwitchC(config-router)#network 3.3.3.3/32 area 0
SwitchC(config- router)#exit
SwitchC(config)#router bgp 200
SwitchC(config-router)#bgp router-id 3.3.3.3
SwitchC(config-router)#network 192.168.3.0/24
SwitchC(config-router)#neighbor 1.1.1.1 remote-as 100
SwitchC(config-router)#end
SwitchC#show ip bgp ipv4 unicast
BGP table version is 1, local router ID is 3.3.3.3
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
*> 192.168.3.0         0.0.0.0                100  32768 i

Total number of prefixes 1

```

18.69 Display BGP Summary Information

Command

```
show ip bgp summary
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: IP address.

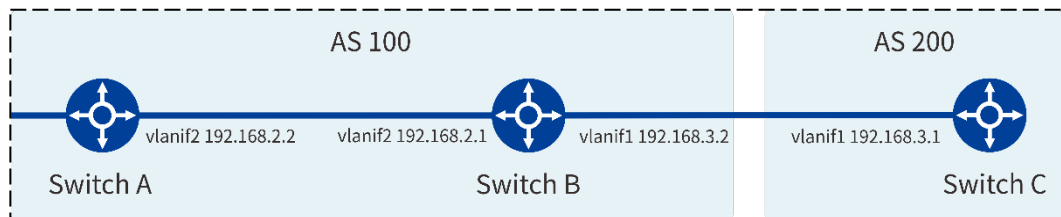
A.B.C.D/M: IP address and mask.

Description

show ip bgp summary: The command is used to display BGP summary information.

Instance

Networking: device A is connected to device B via VLANIF2, and device B is connected to device C via VLANIF1 as shown in the figure below. Device C displays BGP summary information via command.



```

SwitchA> enable
SwitchA#configure terminal
SwitchA(config)#interface vlanif1
SwitchA(config- vlanif1)#ip address 192.168.1.1/24
SwitchA(config- vlanif1)#exit
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#ip interface vlan 2
SwitchA(config)#interface vlanif2
SwitchA(config- vlanif2)#ip address 192.168.2.2/24
SwitchA(config- vlanif2)#exit
SwitchA(config)#ip interface loopback 0
SwitchA(config)#interface loopback0
SwitchA(config- loopback0)#ip address 2.2.2.2/32
SwitchA(config- loopback0)#exit
SwitchA(config)#router ospf
SwitchA(config-router)#router-id 2.2.2.2
SwitchA(config-router)#network 192.168.1.0/24 area 0
SwitchA(config-router)#network 192.168.2.0/24 area 0
SwitchA(config-router)#network 2.2.2.2/32 area 0
SwitchA(config-router)#exit
SwitchA(config)#router bgp 100
SwitchA(config-router)#bgp router-id 2.2.2.2
  
```

```
SwitchA(config-router)#network 192.168.1.0/24  
SwitchA(config-router)#network 192.168.2.0/24  
SwitchA(config-router)#neighbor 1.1.1.1 remote-as 100
```

```
SwitchB> enable  
SwitchB#configure terminal  
SwitchB(config)#interface vlanif1  
SwitchB(config- vlanif1)#ip address 192.168.3.2/24  
SwitchB(config- vlanif1)#exit  
SwitchB(config)#vlan database  
SwitchB(config-vlan)#vlan 2  
SwitchB(config-vlan)#exit  
SwitchB(config)#ip interface vlan 2  
SwitchB(config)#interface vlanif2  
SwitchB(config- vlanif2)#ip address 192.168.2.1/24  
SwitchB(config-vlanif2)#exit  
SwitchB(config)#ip interface loopback 0  
SwitchB(config)#interface loopback0  
SwitchB(config- loopback0)#ip address 1.1.1.1/32  
SwitchB(config- loopback0)#exit  
SwitchB(config)#router ospf  
SwitchB(config-router)#router-id 1.1.1.1  
SwitchB(config-router)#network 1.1.1.1/32 area 0  
SwitchB(config-router)#network 192.168.2.0/24 area 0  
SwitchB(config-router)#network 192.168.3.0/24 area 0  
SwitchB(config-router)#exit  
SwitchB(config)#router bgp 100  
SwitchB(config-router)#bgp router-id 1.1.1.1  
SwitchB(config-router)#network 192.168.1.0/24  
SwitchB(config-router)#network 192.168.2.0/24  
SwitchB(config-router)#neighbor 2.2.2.2 remote-as 100  
SwitchB(config-router)#neighbor 3.3.3.3 remote-as 200
```

```
SwitchC> enable  
SwitchC#configure terminal  
SwitchC(config)#interface vlanif1  
SwitchC(config- vlanif1)#ip address 192.168.3.1/24  
SwitchC(config- vlanif1)#exit  
SwitchC(config)#ip interface loopback 0  
SwitchC(config)#interface loopback0  
SwitchC(config- loopback0)#ip address 3.3.3.3/32  
SwitchC(config- loopback0)#exit  
SwitchC(config)#router ospf
```



```
SwitchC(config-router)#router-id 3.3.3.3
SwitchC(config-router)#network 192.168.3.0/24 area 0
SwitchC(config-router)#network 3.3.3.3/32 area 0
SwitchC(config-router)#exit
SwitchC(config)#router bgp 200
SwitchC(config-router)#bgp router-id 3.3.3.3
SwitchC(config-router)#network 192.168.3.0/24
SwitchC(config-router)#neighbor 1.1.1.1 remote-as 100
SwitchC(config-router)#end
```

```
SwitchC#show ip bgp summary
```

```
BGP router identifier 3.3.3.3, local AS number 200
```

```
BGP table version is 1
```

```
1 BGP AS-PATH entries
```

```
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
1.1.1.1	4	100	0	53	0	0	0	never
Active								

```
Total number of neighbors 1
```

19 IPv6 Configuration

19.1 Create Layer 3 Interface

Command

```
ip interface vlan <VLAN-ID>
```

View

Configure Mode

Parameters

<vlan-id> : create a layer 3 vlan interface, the range is 2-4094.

Description

ip interface vlan: the command is used to create the specified layer 3 vlan interface.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#ip interface vlan 2
```

19.2 IPV6 address:

Command

```
ipv6 address (X:X::X:X/M | prefix X:X::X:X eui-64)
```

View

Layer 3 Interface View

Parameters

X:X::X:X/M: X:X::X:X is IPv6 address, M is mask length

prefix X:X::X:X eui-64: use the EUI-64 format to form an IPv6 address.

Description

ipv6 address: The command is used to configure the ipv6 address of the interface.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ipv6 address 3ffe:506::1/48 //ordinary
ipv6 address
Switch(config-vlanif1)#ipv6 address prefix 3ffe:501:ffff:100::
eui-64 //eui-64 //eui-64 format ipv6 address
```

19.3 Static IPv6Route

Command

```
ipv6 route X:X::X:X/M X:X::X:X INTERFACE
no ipv6 route X:X::X:X/M X:X::X:X INTERFACE
```

View

Configure Mode

Parameters

X:X::X:X/M: specify the static route destination network segment

X:X::X:X: specify ipv6 address of static routing next hop

INTERFACE: outgoing interface for specifying static routing

Description

ipv6 route: command is used to add static ipv6 routing.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ipv6 route ::/0 fe80::200:ff:fe00:a0a0 vlanif2
```

19.4 Configure RA message related parameters

Operation	Command	Description
Enter Privileged	enable	-

Operation	Command	Description
Exec Mode		
Enter Configure Mode	configure terminal	-
Enter Interface View	interface IFNAME	-
Cancel the restrain in RA messages	no ipv6 nd suppress-ra	Publish RA messages are restrained by default
Configure the maximum time interval for RA message publishing	ipv6 nd ra-interval <4-1800>	By default, the maximum time interval of RA message publishing is 600 seconds, and the minimum time interval is 198 seconds when RA messages are periodically published. The time interval between two consecutive times is a random value between the maximum time interval and the minimum time interval as the time interval for periodically publishing RA messages. Configure that the minimum interval should be less than or equal to 0.75 times of the maximum interval.
Configure the minimum time interval for RA message publishing	ipv6 nd minimum-ra-interval <3-1350>	
Configure the hop limit	ipv6 nd current-hoplimit <0-255>	The default router is limited to 64 hops
Configure prefix information of RA messages	ipv6 nd prefix {X:X::X:X/M no-autoconf offlink preferred-lifetime <0-4294967295> valid-lifetime <-4294967295>}	The prefix information in the RA message is not configured by default. In this case, the IPv6 address of the interface

Operation	Command	Description
		sending the RA message will be used as the prefix information in the RA message. Its effective life span is 2592000 seconds (30 days), and the preferred life span is 604800 (7 days).
Configure that the MTU option is not carried in the RA message	no ipv6 nd link-mtu	By default, the MTU option is carried in the RA message
Sets the managed address configuration flag bit to 1	ipv6 nd managed-config-flag	The default managed address flag bit is 0, meaning that the host gets IPv6 addresses through stateless automatic configuration
Set the other configuration flag bit to 1	ipv6 nd other-config-flag	The default other configuration flag bit is 0, which means that the host gets additional information through stateless automatic configuration
Set the router lifetime in the RA message	ipv6 nd ra-lifetime <0-9000>	By default, the lifetime of the router in the RA message is 1800 seconds
Configure the neighbor request message retransmission interval	ipv6 nd retransmission-time <1000-3600000>	The default interface sends NS messages at 1000ms intervals; The value of the Retrans Timer field in the RA message published by the interface is 0, which means the host is not

Operation	Command	Description
		specified
Configure the time to keep neighbors reachable	ipv6 nd reachable-time <0-3600000>	The default interface remains accessible for 30000 ms. The value of the Retrans Timer field in the RA message published by the interface is 0, which means the host is not specified

19.5 Enable IPv6Multicast Function

Command

```
ipv6 mif
no ipv6 mif
```

View

Interface Mode

Parameters

-

Description

The **ipv6 mif**: command is used to enable ipv6 multicast function of the interface

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ipv6 mif
```

19.6 Static IPv6Multicast Route

Command

```
ipv6 mroute source X:X::X:X group X:X::X:X in-interface IFNAME
out-interface IFNAME
no ipv6 mroute source X:X::X:X group X:X::X:X in-interface IFNAME
out-interface IFNAME
```

View

Configure Mode

Parameters

X:X::X:X: source IPv6 address or multicast IPv6 address.

IFNAME: ingress or egress interface

Description

ipv6 mroute: the command is used to add static ipv6 multicast routing

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ipv6 mroute source
3ffe:501:ffff:100:200:ff:fe00:0100 group ff1e::1:2 in-interface
vlanif2 out-interface vlanif3
```

19.7 The Maximum Transmission Unit

Command

mtu <MTU-VALUE>

View

Layer 3 Interface View

Parameters

MTU-VALUE:configure the maximum transmission unit of message, the range is 128-1500, the unit is byte.

Description

mtu: command is used to configure the maximum transmission unit of a layer 3 interface message.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#mtu 1400
```

19.8 Ping IPv6Address

Command

```
ping ipv6 WORD {count <1-4294967295> | size <1-8100> | interface  
IFNAME | quiet | }
```

View

Privileged Exec Mode

Parameters

WORD: specifies the destination ipv6 address of the ping message.

count <1-4294967295> : specifies the number of ping message.

size <1-8100> : specifies the size of the contents to be filled in the ping message.

interface IFNAME: specify the egress interface of ping message.

quiet: does not display the details of the ping process, only the result of the ping.

Description

ping ipv6: command is used to detect whether a specified ipv6 address is reachable and to test whether an ipv6 network connection has break down.

Instance

```
Switch> enable
```

```
Switch#ping ipv6 fe80::0200:00ff:fe00:0100 size 2 count 1 interface  
vlanif2
```


20 DHCP Configuration

20.1 Global DHCP Service Enablement

Command

```
ip dhcp service
no ip dhcp service
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

No.

Description

ip dhcp service: command is used to globally enable the dhcp server service.

Instance

```
#Configure to enabled DHCP server service globally
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
```

20.2 Enable Interface DHCP Relay

Command

```
ip dhcp relay enable
no ip dhcp relay enable
```

View

Layer 3 Interface Configuration View

Default Level

2: Configuration level

Parameters

No.

Description

ip dhcp relay enable: the command is used to enable the dhcp relay function of the interface.

no ip dhcp relay enable: the command is used to disable the dhcp relay function of the interface.

Instance

```
# Enable dhcp relay on vlanif1
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable

# disable DHCP relay on vlanif1
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#no ip dhcp relay enable
```

20.3 InterfaceDHCP Relay Address

Command

```
ip dhcp relay-to <A.B.C.D>
no ip dhcp relay-to [<A.B.C.D>]
```

View

Layer 3 Interface Configuration View

Default Level

2: Configuration level

Parameters

A.B.C.D: dhcp server IP address.

Description

This command is in the Interface view and only configure the corresponding Interface relay and dhcp server IP addresses.

ip dhcp relay-to <A.B.C.D>: the command is used to set the dhcp server ip address required by the relay. This command can be executed repeatedly to configure multiple server IP addresses, which up to 9 relay servers can be configured.

no ip dhcp relay-to [<A.B.C.D>]: used to delete a relay server ip address, the function is opposite to ip dhcp relay-to <A.B.C.D>; With no parameter, the command deletes all relay server ip addresses of the corresponding interface.

Instance

Configure the dhcp relay server IP address for vlanif 1, the parameter IP address is 192.168.1.1

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp relay-to 192.168.1.1
```

Remove the DHCP relay server address with IP of 192.168.1.1 under vlanif 1

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#no ip dhcp relay-to 192.168.1.1
```

Remove all the dhcp relay server address under vlanif 1

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#no ip dhcp relay-to
```

20.4 DHCP Option82 Enablement

Command

ip dhcp option
no ip dhcp option

View

Layer 3 Interface Configuration View

Default Level

2: Configuration level

Parameters

-

Description

ip dhcp option: enable the option 82 function of dhcp relay, and enable the relay message sent by the relay process to carry option 82.

no ip dhcp option: disable option 82 function of dhcp relay.

Instance

For vlanif1 interface, enable option 82 function of dhcp relay

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface vlanif1
```

```
Switch(config-vlanif1)#ip dhcp relay enable
```

```
Switch(config-vlanif1)#ip dhcp option
```

For vlanif1 interface, enable option 82 function of dhcp relay

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface vlanif1
```

```
Switch(config-vlanif1)#no ip dhcp option
```

20.5 Treatment Strategy of DHCP Option82

Command

```
ip dhcp relay-information policy (append | discard | replace |  
untouched )
```

```
no ip dhcp relay-information policy
```

View

Layer 3 Interface Configuration View

Default Level

2: Configuration level

Parameters

append: configure the option check policy as Append.

discard: configure the option check policy as Discard.

replace: configure the option check policy as Replace.

untouched: configure the option check policy as Untouched.

Description

ip dhcp relay-information policy <append | discard | replace | untouched >: set an option processing policy of dhcp relay, the relay process will process the received dhcp message with option 82 according to the policy.

no ip dhcp relay - information policy: disable the option processing strategy of dhcp relay, strategy will restore to the default strategy, namely only forward received dhcp message with the option 82 (Untouched).

Instance

```
# configure option 82 with the policy replace for vlanif1 port.
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp option
Switch(config-vlanif1)#ip dhcp relay-to 192.168.1.1
Switch(config-vlanif1)#ip dhcp relay-information policy replace

#Disable option 82 policy on port vlanif1.
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#no ip dhcp relay-information policy
```

20.6 Relay Identity of DHCP Option82

Command

ip dhcp relay-information circuitid (basic | string OPTION)

View

Interface Mode

Default Level

2: Configuration level

Parameters

Basic: configure sub option circuitid is the base (default) configuration.

String: configure sub option circuitid as the string given by option.

Description

ip dhcp relay-information circuitid (basic | string OPTION): Set the value of option82 suboption circuitid of DHCP relay.

Instance

```
#Configure the value of suboption circuited of option 82 is the
string "vlan2:ge10" for vlanif1 port.
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp option
Switch(config-vlanif1)#ip dhcp relay-information circuitid string
vlan2:ge10
```

20.7 Remote Identity of DHCP Option82

Command

```
ip dhcp relay-information remoteid (basic | string OPTION)
```

View

Layer 3 Interface Configuration View

Default Level

2: Configuration level

Parameters

Basic: configure sub option remoteid is the base (default) configuration.

String: configure sub option remoteid as the string given by option.

Description

ip dhcp relay-information remoteid (basic | string OPTION): Set the value of option82 suboption remoteid of DHCP relay.

Instance

```
Configure the value of sub option circuited of option 82 is the
string "00:11:22:33:44:55" for vlanif1 port.
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp option
Switch(config-vlanif1)#ip dhcp relay-information remoteid string
00:11:22:33:44:55
```

20.8 Create DHCP Address Pool

Command

```
ip dhcp pool <WORD>
no ip dhcp pool <WORD>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

WORD: the name of dhcp address pool

Description

ip dhcp pool: the command is used to create the dhcp address pool.

no ip dhcp pool: the command is used to delete the dhcp address pool.

Instance

#Create a dhcp address pool named "test" :

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#ip dhcp service
```

```
Switch(config)#ip dhcp pool test
```

```
Switch(dhcp-config)#
```

#Delete a dhcp address pool named "test" :

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#no ip dhcp pool test
```

20.9 DHCP Address Pool Subnet Segment

Command

```
network (<A.B.C.D A.B.C.D>/<A.B.C.D/M>)
no network
```

View

DHCP Configuration View

Default Level

2: Configuration level

Parameters

A.B.C.D: IP address & mask, used to represent subnet segments.

A.B.C.D/M: IP address and mask, used to represent subnet segments.

Description

Network:: configure the subnet segment of DHCP pool, among which the parameters give the specific subnet segment value.

no network: deletes the subnet segment configuration of a specified DHCP pool.

Instance

```
#Configure network for address pool "test"
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#network 192.168.1.1/24

#Delete network configuration of address pool "test"
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no network
```

20.10 Default Route of DHCP Address Pool

Command

```
default-router A.B.C.D
no default-router
```

View

dhcp View

Default Level

2: Configuration level

Parameters

A.B.C.D: The default routing address used by dhcp.

Description

default-router: configure the default routing IP address of DHCP pool.

no default-router: delete the default routing configuration of DHCP pool.

Instance

```
#Configure the default route to 192.168.1.1 of dhcp pool test
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#default-router 192.168.1.1

#delete the default routing configuration of dhcp pool test
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no default-router 192.168.1.1
```

20.11 DHCP Address Pool

Command

```
range <A.B.C.D A.B.C.D>
no range (<A.B.C.D A.B.C.D>|)
```

View

dhcp View

Default Level

2: Configuration level

Parameters

A.B.C.D: The lowest and highest addresses of dhcp pool.

Description

range: configure the address range of DHCP pool, that is, the addresses that belong to the range can be allocated effectively by DHCP.

no range: delete the address range of DHCP pool. If no range parameters are given, delete all range configurations.

Instance

```
Configuration the address range of dhcp pool test to: 192.168.1.10
192.168.1.20
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
```

```
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#range 192.168.1.10 192.168.1.20
```

```
Delete the address range of dhcp pool test: 192.168.1.10
192.168.1.20
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no range 192.168.1.10 192.168.1.20
```

```
Delete all the address range of dhcp pool test:
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no range
```

20.12 The Lease Time of DHCP Address Pool

Command

```
lease-time <0-30> <0-24> <0-60>
no lease-time
```

View

```
dhcp View
```

Default Level

```
2: Configuration level
```

Parameters

```
<0-30> : days.
<0-24> : hours.
<0-60> : minutes.
```

Description

lease -time: configure the address lease duration of dhcp pool. When the IP address obtained by the dhcp client is about to reach the lease duration, it is necessary to renew the lease. Otherwise, the IP address will be invalid, and the dhcp client needs to re-request the IP address.

no lease-time: delete the address lease duration configuration of dhcp pool and restore the lease duration to the default value.

Instance

```
# set the lease-time of dhcp pool test to 30 minutes.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#lease-time 0 0 30

# set the lease-time of dhcp pool test.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no lease-time
```

20.13 The Threshold of DHCP Address Pool

Command

```
threshold <1-254>
no threshold
```

View

```
dhcp View
```

Default Level

```
2: Configuration level
```

Parameters

```
<1-254> : threshold value.
```

Description

threshold: threshold value to configure dhcp pool.

no threshold: Delete the threshold value of DHCP pool (that is, restore to the default value).

Instance

```
# set the threshold of dhcp pool test to 8.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
```

```
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#threshold 8

# set the threshold of dhcp pool test.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no threshold
```

20.14 DNS Server Address

Command

```
ip dhcp dns-server <A.B.C.D> [<A.B.C.D>] [<A.B.C.D>]
no ip dhcp dns-server
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

< A.B.C.D>: dns server ip address.

Description

ip dhcp dns-server: configure dns servers for all dhcp pools, up to three different dns servers can be configured (this configuration is global).

no ip dhcp dns-server: delete all dns server configurations.

Instance

```
# set the DNS -serve of DHCP pool to 114.114.114.114 8.8.8.8.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp dns-server 114.114.114.114 8.8.8.8

Remove all dns-serve configurations.
Switch> enable
Switch#configure terminal
Switch(config)#no ip dhcp dns-server
```

20.15 Log Server Address

Command

```
ip dhcp log-server <A.B.C.D> [<A.B.C.D>] [<A.B.C.D>]  
no ip dhcp log-server
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

< A.B.C.D>: log server ip address.

Description

ip dhcp log-server: configure log servers for all dhcp pools, up to three different log servers can be configured (this configuration is global).

no ip dhcp log-server: delete all log server configurations.

Instance

```
# set the log-server of dhcp pool to 192.168.1.1 192.168.1.2  
192.168.1.3.
```

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#ip dhcp service
```

```
Switch(config)#ip dhcp dns-server 192.168.1.1 192.168.1.2  
192.168.1.3
```

```
#Remove all log-server configurations.
```

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#no ip dhcp log-server
```

20.16 WINS Server Address

Command

```
ip dhcp wins-server <A.B.C.D> [<A.B.C.D>] [<A.B.C.D>]  
no ip dhcp wins-server
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

< A.B.C.D>: wins server ip address.

Description

ip dhcp wins-server: configure wins servers for all dhcp pools, up to three different wins servers can be configured (this configuration is global).

no ip dhcp win-server: delete all winserver configurations.

Instance

```
# configure the wins-server of dhcp pool to be 192.168.1.1
192.168.1.2 192.168.1.3.
```

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#ip dhcp service
```

```
Switch(config)#ip dhcp wins-server 192.168.1.1 192.168.1.2
192.168.1.3
```

```
#Delete all wins-server configurations.
```

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#no ip dhcp wins-server
```

20.17 Display DHCP Information

Command

```
show ip dhcp global
```

```
show ip dhcp lease ((interface [IFNAME]) | (summary [IFNAME]))
```

```
show ip dhcp pool [WORD]
```

```
show ip dhcp relay [IFNAME]
```

```
show ip dhcp statistics [IFNAME]
```

```
show ip dhcp status
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

[IFNAME]: interface name.

[WORD]: address pool identification.

Description

show ip dhcp global: view DHCP global information.
show ip dhcp lease: view DHCP lease information.
show ip dhcp pool: view DHCP address pool information.
show ip dhcp relay: view DHCP relay information.
show ip dhcp statistics: view DHCP statistics information.
show ip dhcp status: view DHCP status information.

Instance

Switch#**show ip dhcp status**

Interface	IP Address	DHCP Status

vlanif1	192.168.1.254	DHCP Relay

21 SNMP Configuration

21.1 SNMP Enablement

Command

```
snmp-server enable traps
no snmp-server enable traps
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

snmp-server enable traps: command is used to enable SNMP server.

no snmp-server enable: command is used to disable SNMP server.

By default, SNMP function is enabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server enable traps
Switch(config)#no snmp-server enable traps
```

21.2 SNMP View

Command

```
snmp-server view VIEWNAME OID ( included | excluded )
```



```
no snmp-server view VIEWNAME OID
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

VIEWNAME: VIEWNAME, ranging from 1 to 32 bytes.

OID: OID MIB subtree of MIB object subtree, variable OID only allows digital input (such as 1.3.6.1).

Included: means that this MIB view includes the MIB subtree.

excluded: means that this MIB view excludes the MIB subtree.

Description

snmp-server view: command is used to create or update information about the MIB view to restrict the MIB objects that can be accessed by the NMS.

no snmp-server view: The command is used to cancel the current Settings.

The MIB is a collection of managed objects, and the MIB view is a subset of the MIB, and the user can bind the community name/user name to the MIB view to restrict the MIB objects that can be accessed by the NMS. The user can configure the MIB object to excluded or included within the view. Excluded means that the current view does not include all the modes of the MIB subtree; Included means that the current view includes all nodes of the MIB subtree.

By default, the view name is system. The OID included is 1.3.6.1.

SNMP community name or group name configuration needs to determine the MIB view permissions of the community name or group, related configuration can refer to the command snmp-server community, snmp-server group.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server view viewname 1.3.6.1.5 included
Switch(config)#no snmp-server view viewname 1.3.6.1.5
```

21.3 SNMP Community Name

Command

```
snmp-server community NAME {view VIEWNAME| } (ro | rw)
no snmp-server community {COMMUNITYNAME | }
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

NAME: community name, ranging from 1 to 32 bytes.

View: MIB view name, this parameter is optional, if not entered, by default it is the default view.

Ro: read only means read-only access to MIB objects. Communities with read-only access can only view device information.

Rw: read and write indicates read and write access to MIB objects, and communities with read and write permissions can configure devices.

Description

snmp-server community: command is used to set the community name, SNMP v1/v2c version uses the group name to restrict access rights. This command can be used to configure the group name, read or write view rights and access control policies. **no snmp-server community**: command is used to cancel group access name settings.

Normally, "public" is used as the name of the read permission group. For security reasons, it is recommended that network administrators configure other community names.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server community communityname view viewname
rw
Switch(config)#no snmp-server community communityname
```

21.4 SNMP Group

Command

```
snmp-server group NAME v3 (auth | noauth | priv ) { notify | read
| write } VIEWNAME
no snmp-server group NAME v3 (auth | noauth | priv )
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

NAME: group name, ranging from 1 to 32 bytes.

v3: SNMP v3 version.

Auth: indicates that the message is authenticated but not encrypted.

Noauth: indicates that the message is neither authenticated nor encrypted.

Priv: indicates that the message is authenticated and encrypted.

VIEWNAME: view name, ranging from 1 to 32 bytes. By default, the Trap message view is not configured, meaning that the Agent does not send Traps to the NMS.

Read: specifies the read view of the group.

write: specifies the write and read view of the group.

VIEWNAME: view name

Description

snmp-server group: command is used to configure a new SNMP group and set the secure mode and corresponding SNMP view of the SNMP group.

no snmp-server group: The command is used to remove a specified SNMP group. For SNMP v3, the group name and the security mode (authentication or not, encryption or not) together determine a group, with the same group name but different security mode are two different groups.

This system defaults to snmp v2, so there is no default configuration for group. If the view name for read is not specified in the command, it defaults to the default view.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server group groupname v3 priv read viewname
write viewname
Switch(config)#no snmp-server group groupname v3 priv
```

21.5 SNMP User

Command

```
snmp-server user USERNAME GROUPNAME
snmp-server user USERNAME GROUPNAME v3
snmp-server user USERNAME GROUPNAME v3 auth md5 MD5
snmp-server user USERNAME GROUPNAME v3 auth md5 MD5 priv ( aes |
des) password
```

```
no snmp-server user USERNAME GROUPNAME v3
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

USERNAME: user name, ranging from 1 to 32 bytes.

GROUPNAME: group name

v3: specifies that it is SNMP v3 version user, and defaults to v1 version user.

Auth: indicates that security mode requires authentication. If do not enter this parameter, the default is no authentication, no encryption mode.

md5: specifies the authentication protocol as the HMAC MD5 algorithm.

MD5: authentication password, string, value range of plaintext is 1 ~ 64 characters. If MD5 algorithm is adopted in ciphertext form, the authentication key is 32-bit hexadecimal number. If SHA algorithm is used, the authentication key is a 40-bit hexadecimal number.

priv: indicates that security mode requires authentication.

aes: the encryption algorithm is specified as AES (Advanced Encryption Standard), which has higher security than DES.

des: the encryption algorithm is specified as DES (Data Encryption Standard).

password: encrypted password, string, value range of plaintext is 1 ~ 64 characters. If MD5 algorithm is adopted in ciphertext form, the authentication key is 32-bit hexadecimal number. If SHA algorithm is used, the authentication key is a 40-bit hexadecimal number.

Description

snmp-server user: The command is used to add a new user to an SNMP group.

no snmp-server user: command is used to delete a user of an SNMP group.

This command applies to SNMP v3 version. If the Agent interact with the message of NMS using SNMP v3 version, then SNMP v3 users need to be created. For the configured user to take effect, a group must be created first. Authentication and encryption are configured when the group is created, and the specific algorithm and password for authentication and encryption are configured when the user is created.



Notes

This command is used several times to configure the same user (that is, the user name is the

same, no other parameters are required), and the configuration results are subject to the last configuration.

Instance

```
Switch> en
Switch#configure terminal
Switch(config)#snmp-server user admin groupname v3
Switch(config)#no snmp-server user username groupname v3
```

21.6 SNMP Trap Destination

Command

```
snmp-server host IP traps (version ( 1 | 2c )) NAME
no snmp-server host IP traps NAME
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

traps: specify the host to be Trap host.

IP: the IPV4 address of a host that accepts Traps.

1: represents SNMP v1 version.

2c: represents SNMP v2c version.

NAME: when there is a parameter version, NAME represents SNMPv1/v2c community. When there is no version parameter, NAME represents SNMPv3 user name.

Description

snmp-server host: command is used to set the destination host to receive SNMP Trap messages.

no snmp-server host: command is used to cancel the current configurations.

Depending on network management needs, users can configure multiple destination hosts to receive Trap messages through this command.

If a device is needed to send Trap messages, the snmp -server host command should be used in conjunction with the snmp -server enable trap command (the default is to send all traps).

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server host 192.168.5.123 traps version 2c
communityname
Switch(config)#no snmp-server host 192.168.5.123 traps name
```

22 LLDP Configuration

22.1 LLDP enablement

Command

```
lldp enable
no lldp enable
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

lldp enable: command is used to enable the LLDP function.

no lldp enable: The command is used to turn off the LLDP function.

By default, global LLDP function is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#lldp enable
```

22.2 LLDP Port Operating Mode

Command

```
lldp admin-status (tx-enable | rx-enable | txrx-enable | disable )
no lldp admin-status disable
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

tx-enable: working mode is Tx, only sending and not receiving LLDP message.

rx-enable: working mode Rx, only receiving and not sending LLDP message.

txrx-enable: working mode is TxRx, both sending and receiving LLDP message.

disable: working mode Disable, neither receiving nor sending LLDP message.

Description

lldp admin-status: command is used to configure the lldp working mode of the port.

no lldp admin-status disable: command is used to restore the default working mode of the port.

By default, the working mode of LLDP works in TxRx when global LLDP is enabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#lldp admin-status tx-enable
```

22.3 Time Interval of Sending LLDP Message

Command

```
lldp timer <INTERVAL>
no lldp timer
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

Interval: the time interval between ports to send LLDP message, ranging from 5-300 in seconds.

Description

lldp timer: command is used to set the time interval for sending LLDP message.

no lldp timer: command is used to restore the default packet time interval for LLDP.

By default, the interval between LLDP message is 30 seconds

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#lldp timer 50
```

22.4 LLDP Interface Management Address

Command

```
lldp management-address A.B.C.D
no lldp management-address
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: administrative address published in LLDP message.

Description

lldp management-address: command is used to configure the management address published in the LLDP message.

no lldp management-address: command is used to restore the default management address published in the LLDP message.

The management address released by the port in the LLDP message defaults to the main IP address of the smallest VLAN of the VLANs this port is in. If the VLAN is not configured with a main IP address, it will be 0.0.0.0.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#lldp management-address 2.2.2.2
```

22.5 Encapsulation Format of LLDP Message

Command

```
lldp frame-format (snap | ethernet2)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

snap: encapsulation format of LLDP message is snap.

ethernet2: encapsulation format of LLDP message is ethernet2

Description

lldp frame-format: command is used to configure the encapsulation format of LLDP message.

By default, the encapsulation format of LLDP message is ethernet2.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface ge8
```

```
Switch(config-ge8)#lldp frame-format snap
```

22.6 Display LLDP neighbor information

Command

```
show lldp neighbor-information (brief | )
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Brief: displays a summary of the neighbor device, or neighbor information of all ports without this parameter.

Description

show lldp neighbor-information: command is used to display information about the neighbor device.

Instance

```
Switch> enable
Switch#show lldp neighbor-information
LLDP neighbor information of port ge2
-----
Neighbor index                : 1
Update time                   : 1hours 57minutes 40seconds
Ageing time                   : 114seconds
Chassis ID type               : MAC Address
Chassis ID                    : 0022.6f55.5556
Port ID type                  : Interface Name
Port ID                       : ge10
Time to live                   : 120 seconds
Port description              : ge10
System name                   : SW5
System capabilities supported  : Bridge/Switch,Router
System capabilities enabled    : Bridge/Switch,Router
Management address subtype    : IPv4
Management address            : 192.168.1.254
Interface number subtype      : System Port Number
Interface number              : 5010
Object ID                     : Standard LLDP MIB
MAC/PHY Configuration/Status :
    Auto-Negotiation supported : Yes
    Auto-Negotiation enabled   : Yes
    Operational MAU type       : 1000BASE-T full duplex mode
Link Aggregation              :
    Link aggregation supported  : Yes
    Link aggregation enabled    : No
    Aggregated port ID         : 0
Maximum Frame Size            : 1518
Port VLAN ID                  : 1
-----

LLDP Neighbors Number        : 1

Switch#show lldp neighbor-information brief
```

Local Intf	Neighbor System Name	Neighbor Port	ID
Ageing-time(s)			
ge2	SW5	ge10	91

LLDP Neighbors Number	: 1

22.7 Display LLDP Statistics Information

Command

```
show lldp statistics (interface IFNAME | )
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

interface IFNAME: displays statistics information of the specified port.

Description

show lldp statistics: command is used to display statistics for all ports, or for the specified port.

Instance

```
Switch> enable
Switch#show lldp statistics
Global LLDP traffic statistics:
    Total frames out: 268
    Total ages out: 0
    Total frames discarded: 0
    Total frames received in error: 0
    Total frames received in: 260
    Total frames TLVs discarded: 0
    Total frames TLVs unrecognized: 0

Switch#show lldp statistics ge2
Interface ge2 LLDP traffic statistics:
    Total frames out: 269
    Total ages out: 0
    Total frames discarded: 0
    Total frames received in error: 0
    Total frames received in: 260
```

```
Total frames TLVs discarded: 0
Total frames TLVs unrecognized: 0
```

22.8 Display LLDP Local Information

Command

```
show lldp local-information (interface IFNAME | )
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Interface IFNAME: displays local information of the specified port.

Description

show lldp local-information: command is used to display all LLDP local information, or LLDP local information of the specified port.

Instance

```
Switch> enable
Switch#show lldp local-information
*Switch#show lldp local-information
LLDP local-information of port ge2:
    Chassis ID subtype : MAC address
    Chassis ID       : 0022.6f01.cca3
    Port ID subtype  : Interface name
    Port ID          : ge2
    Port description : ge2

    Management address type      : IPv4
    Management address          : 192.168.1.254
    Management address interface type : ifIndex
    Management address interface ID  : 5002
    Management address OID         : 0

    Port VLAN ID(PVID) : 1

    Port and protocol VLAN ID(PPVID) : 0
    Port and protocol VLAN supported : not supported
    Port and protocol VLAN enabled  : no enabled
```

```

VLAN name of VLAN 1 : default

Link aggregation supported : supported
Link aggregation enabled  : not enabled
Aggregated port ID       : 0

Auto-negotiation supported      : supported
Auto-negotiation enabled       : enabled
PMD auto-negotiation advertised :
    10BASE-T half duplex mode
    10BASE-T full duplex mode
    100BASE-TX half duplex mode
    100BASE-TX full duplex mode
    1000BASE-T half duplex mode
    1000BASE-T full duplex mode
Operational MAU type           : speed(1000)/duplex(full)

```

22.9 Display LLDP Status Information

Command

```
show lldp status (interface IFNAME | )
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

Interface IFNAME: displays state information of the specified port.

Description

show lldp status: command is used to display global LLDP status information, or LLDP status information on the specified port.

Instance

```

Switch> enable
Switch#show lldp status
LLDP running-information
    System running status      : Running
    System description         : Switch
    Transmit interval          : 30 s

```

```
Hold multiplier           : 4
Reinit delay              : 2 s
Transmit delay            : 2 s
Notification enable       : Enable
Notification Interval     : 5 s
```

```
Switch#show lldp status interface ge2
```

```
Interface[ge2] lldp status
```

```
Port status of LLDP      : Enable
Admin status              : Rx_Tx
Trap flag                 : No
Number of neighbors       : 1
Number of sent optional TLV : 9
```

23 QOS Configuration

23.1 Configure Global QOS Enable/Disable

Command

```
mls qos enable
no mls qos
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

On is enable, disable is no

Description

For configuring global QOS on and off, the MLS QOS switch must be on for all qos configurations.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
Switch(config)#no mls qos
```

23.2 Configure the queue bitmap

Command

```
mls qos cos-map <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
no mls qos cos-map
```



```
show mls qos cos-map
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

Parameter 1: select a queue for COS 0 message;

Parameter 2: select a queue for COS 1 message;

Parameter 3: select a queue for COS 2 message;

Parameter 4: select a queue for COS 3 message;

Parameter 5: select a queue for COS 4 message;

Parameter 6: select a queue for COS 5 message;

Parameter 7: select a queue for COS 6 message;

Parameter 8: select a queue for COS 7 message;

Description

Configure the queue value for each COS. No is to deleted and show is to view configuration.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#mls qos enable
```

```
Switch(config)#mls qos cos-map 1 2 3 4 5 6 7 0
```

```
Switch(config)#show mls qos cos-map
```

```
Switch(config)#no mls qos cos-map
```

23.3 Configure queue mode

Command

```
mls qos scheduler (sp|wrr <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10>)
```

```
no mls qos scheduler
```

```
show mls qos scheduler
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

sp: represents strict priority; WRR means to configure each queue with a weight according to weight priority <1-10>.

no: means delete. The default mode is simple polling mode.

Show: to view the configuration.

Description

SP: Strict Priority, the SP schedule sends packets in the higher-priority queue in Strict Priority order from highest to lowest, and then sends packets in the lower-priority queue when the higher-priority queue is empty. Queue 7 has the highest priority and queue 0 has the lowest priority.

WRR, weighted scheduling based on message, can configure how many messages are scheduled per queue as possible and then transfer to the next queue.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
Switch(config)#mls qos sschedule sp // configured to SP mode
Switch(config)#show mls qos sschedule
Switch(config)#mls qos sschedule wrr 1 2 3 4 5 6 7 0 // the
configuration effect is: each queue takes away the message with
the corresponding weight ratio
Switch(config)#no mls qos schedule // restore default configuration
SRR
```

23.4 Configure DSCP -COS bitmap

Command

```
mls qos map dscp-cos NAME (<0-63>|<0-63> <0-63>|<0-63> <0-63>
<0-63>|<0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63>
<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63> <0-63> <0-63> <0-63>) to <0-7>
no mls qos map dscp-cos (NAME|all)
show mls qos dscp-cos (NAME|all)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

NAME: create a name for the dscp-cos map.

<0-63> to <0-7>: transfer each DSCP value to the corresponding COS queue.

No means to delete.

Show: means to view the configuration.

Description

The default dscp-cos map is 0-7 to cos 0 8-15 to cos 1 16-23 to cos 2 24-31 to cos 3 32-39 to cos 4 40-47 to cos 5 48-55 to cos 6 56-63 to cos 7.

The configuration is only issued when it is referenced. No means to delete NAME, specifying which one to delete.

Instance

```

Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
Switch(config)# mls qos dscp-cos dscp1 10 46 56 6// means that the
message DSCP value is 10 46 56 and so on will be transfered to queue
6
Switch(config)#show mls qos dscp-cos dscp1
Switch(config)#no mls qos map dscp-cos dscp1// specify to delete
dscp1

```

23.5 Configure DSCP -DSCP bitmap

Command

```

mls qos map dscp-mutation NAME (<0-63>|<0-63> <0-63>|<0-63> <0-63>
<0-63>|<0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63>
<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63> <0-63> <0-63> <0-63>) to <0-63>
no mls qos map dscp-mutation (NAME |all)
show mls qos map dscp-mutation(NAME|all)

```

View

Configure Mode

Default Level

2: Configuration level

Parameters

By default, it is dscp-mutation map 0-63 to dscp 0-63

No means to delete, name is to specify which MAP to delete, all means to delete all.

Show means to view, NAME means to specify which MAP to view, all means to view all.

Description

When different DSCP values received, some changes can be made to the DSCP and then transfer to different queues.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos map dscp-mutation dscp2 2 61
Switch(config)#show mls qos map dscp-mutation dscp2
Switch(config)#no mls qos map dscp-mutation dscp2
```

23.6 Create a CLASS-MAP

Command

```
class-map NAME
no class-map NAME
show class-map (NAME|)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

No means to delete.

Show: means to view the specified class-map or all class-maps including the information configured therein.

Description

Class map: Class map is a definition of a Class map that groups different types of data flows.

Instance

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#class-map ac
Switch(config)#show class-map
Switch(config)#no class-map ac
```

23.7 Create a POLICY-MAP

Command

```
policy-map NAME
no policy-map NAME
show policy-map (NAME|)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

No means to delete.

show: means to view the information specified or all included in it.

Description

policy map: It is a definition of a policy map that matches a class map to

determine the bandwidth and/or priority of a class of data flows.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#policy-map ad
Switch(config)#show policy-map (ad)
Switch(config)#no policy-map ad
```

23.8 Configure the CLASS-MAP Property

Command

```
match ip-dscp (<0-63>|<0-63> <0-63>|<0-63> <0-63> <0-63>|<0-63>  
<0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>|<0-63>  
<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
```

```

<0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63>
<0-63> <0-63>)
no match ip-dscp

match ip-precedence (<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-7>|<0-7>
<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7>
<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>|<0-7>
<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>)
no match ip-precedence <0-7>

match layer4 (source-port|destination-port) <1-65535>
no match layer4 (source-port|destination-port) <1-65535>

match vlan <1-4094>
match vlan-range <1-4094> to <1-4094>
no match vlan

```

View

CLASS-MAP Configuration View

Default Level

2: Configuration level

Parameters

The ip - dscp ip - precedence command is used to configure fields layer4 of dscp precedence, matching L4 port protocol number, vlan < 1-4094 > message forwarded to the new vlan.

Description

-

Instance

```

Switch> enable
Switch#configure terminal
Switch(config)#class-map ac
*Switch(config-cmap)#match layer4 destination-port 80
*Switch(config-cmap)#do show class-map
    CLASS-MAP-NAME: ac
    Match Destination Port: 80
*Switch(config-cmap)#no match layer4 destination-port 80

```

23.9 Configure the POLICY-MAP property

Command

```
class NAME
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

Enter config-pmap-c mode.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
*Switch(config)#policy-map ac
*Switch(config-pmap)#class aa
*Switch(config-pmap-c)#
```

23.10 Configure the POLICY-MAP-C Property

Command

```
set cos (<0-7>|cos-inner)
no set cos
```

```
set ip-dscp <0-63>
no set ip-dscp
```

```
set ip-predence <0-7>
no set ip-predence
```

```
police <64-1000000> <0-64000> exceed-action drop
no police <64-1000000> <0-64000> exceed-action drop
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

COS sets the priority, cos-inner copies the vlanID of the ingress to the priority, and no means restore to the default value.

The ip-dscp ip-predence command is to set the priority.

police <64-1000000> <0-64000> exceed-action drop performs the discard action when the rate within this range and the rate should be a multiple of 64.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
*Switch(config)#policy-map ad
*Switch(config-pmap)#class ac
*Switch(config-pmap-c)#police 2000 2000 exceed-action drop
*Switch(config-pmap-c)#do show policy-map
POLICY-MAP-NAME: ad
State: detached
CLASS-MAP-NAME: ac
Police: average rate (2000 kbps)
burst size (2000 bytes)
exceed-action (drop)
excess burst size (2000 bytes)
flow control mode (none)
```

23.11 Configure QOS Interface Mode

Command

```
service-policy input NAME
no service-policy input NAME

mls qos trust dscp
no mls qos trust dscp

mls qos cos <0-7>
no mls qos cos
```



```
mls qos dscp-cos NAME
```

```
no mls qos dscp-cos NAME
```

```
mls qos dscp-mutation NAME
```

```
no mls qos dscp-mutation NAME
```

```
wrr-queue bandwidth <1-65535> <1-65535> <1-65535> <1-65535>
```

```
<1-65535> <1-65535> <1-65535> <1-65535>
```

```
no wrr-queue bandwidth <0-7>
```

View

Ethernet port configuration view

Default Level

2: Configuration level

Parameters

Name

Description

service-policy input NAME: means to install the contents of the policy-map into the specified interface.

No means cancel the installation.

mls qos trust dscp: Indicates that the packet received at the specified port is queued according to the DSCP value, and the default mode is COS. No means restore to default value.

mls qos dscp-cos NAME: Installs the dscp-cos map of the specified name on the specified port. No means to delete.

mls qos dscp-mutation NAME: Install a dscp-mutation map with the specified name on the specified port. No means to delete.

mls qos cos <0-7>: Configure the default priority of the specified port. No means to restore the default value, which is 0-7 to 0-7

```
wrr-queue bandwidth <1-65535> <1-65535> <1-65535> <1-65535>
```

```
<1-65535> <1-65535> <1-65535> <1-65535>:
```

limit the speed of one or more queues on a specified port, enter a multiple of 64. No means contact speed limit.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
*Switch(config)#interface ge1
```

```
*Switch(config-ge1)#service-policy input ad
```

```
*Switch(config-gel)#do show policy-map
POLICY-MAP-NAME: ad
State: attached
CLASS-MAP-NAME: ac
  Police: average rate (2000 kbps)
          burst size (2000 bytes)
          exceed-action (drop)
          excess burst size (2000 bytes)
          flow control mode (none)

*Switch(config-gel)#do show mls qos interface gel
INPUT-POLICY-MAP-NAME: ad
CLASS-MAP-NAME: ac
  Police: average rate (2000 kbps)
          burst size (2000 bytes)
          exceed-action (drop)
          excess burst size (2000 bytes)
          flow control mode (none)
Trust Mode: Ports default priority
Port Default Priority: 0
VLAN Priority Override: Not Configured
Egress Traffic Shaping: Not Configured
View all information on configuring MLS qos within a port.
```

24 ACL Configuration

24.1 Configure IPV4 standard ACL based on IP addresses

Command

```
access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D
access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D
access-list (<1-99>|<1300-1999>) (deny|permit) host A.B.C.D
access-list (<1-99>|<1300-1999>) (deny|permit) any
no access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D
no access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D
no access-list (<1-99>|<1300-1999>) (deny|permit) host A.B.C.D
no access-list (<1-99>|<1300-1999>) (deny|permit) any
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

(<1-99>|<1300-1999>) : represents the scope of the standard ACL.

(deny|permit) : ACL action, deny, permit.

A.B.C.D A.B.C.D: represents the source IP address and mask. The mask adopts the anti-code mechanism, such as 192.168.1.1 0.0.0.0 means only match 192.168.1.1 source IP message.

host A.B.C.D: indicates that the source IP address is A.B.C.D 0.0.0.0.

any: indicates that the source IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

Description

Access-list: command is used to create a standard filter rule group. A group can support up to 32 rules. No is to delete a rule group. When the message matches the corresponding rule, the action will be executed. For example, the configuration rule is as follows: access-list 1 deny 192.168.1.1 0.0.0.0. When the message from 192.168.1.1 is received, the action performed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 1 deny 192.168.1.1 0.0.0.0
```

24.2 Configure IPV4 Extended ACL based on IP addresses

Command

```
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D A.B.C.D A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D any
access-list (<100-199>|<2000-2699>) (deny|permit) ip any A.B.C.D
A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip any any
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D host A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host
A.B.C.D A.B.C.D A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D
host A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip any host
A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D
any
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D A.B.C.D A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D any
```

```

no access-list (<100-199>|<2000-2699>) (deny|permit) ip any
A.B.C.D A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip any any
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D host A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host
A.B.C.D A.B.C.D A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host
A.B.C.D host A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip any host
A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host
A.B.C.D any

```

View

Configure Mode

Default Level

2: Configuration level

Parameters

(<100-199>|<2000-2699>) : indicates extending the scope of the ACL.

(deny|permit) : ACL action, deny, permit.

A.B.C.D A.B.C.D: represents the source IP address and mask. The mask adopts the anti-code mechanism. For example: 192.168.1.1 0.0.0.0 represents messages that only matches 192.168.1.1 source IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

No means to delete the corresponding rule.

Description

Access-list: command is used to create a standard filter rule group. A group can support up to 32 rules. No is to delete a rule group. When the message matches the corresponding rule, the action will be executed. For example, the configuration rule is as follows: access-list 101 deny 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0 When the message from 192.168.1.1 to 192.168.2.1 is received, the action performed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

Instance

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#access-list 101 deny 192.168.1.1 0.0.0.0
192.168.2.1 0.0.0.0
```

24.3 Configure other IPV4 protocols based on IP addresses to extend ACL

Command

```
access-list (<100-199>|<2000-2699>) (deny|permit)
(<0-255>|ahp|eigrp|esp|gre|ipinip|ospf|pcp|pim ) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) ((A.B.C.D A.B.C.D)|(any)|(host
A.B.C.D))
no access-list (<100-199>|<2000-2699>) (deny|permit)
(<0-255>|ahp|eigrp|esp|gre|ipinip|ospf|pcp|pim ) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) ((A.B.C.D A.B.C.D)|(any)|(host
A.B.C.D))
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

(<100-199>|<2000-2699>) : indicates extending the scope of the ACL.

(deny|permit) : ACL action, deny, permit.

(<0-255>| ahp | eigrp | esp | gre | ipinip | ospf | PCP |pim) : configure IP protocol type:

- <0-255>: An IP protocol number
- Ahp: Authentication Header Protocol
- Eigrp: EIGRP routing protocol
- Esp: Encapsulation Security Payload
- Gre: General Routing Encapsulation
- Ipinip: iP in IP tunneling
- Ospf: OSPF routing protocol
- Pcp: Payload Compression Protocol
- Pim: Protocol Independent Multicast

((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) : configure the source IP address.

((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) : configure the destination IP address.

No means to delete.

Description

Since the message has a corresponding protocol port number, it can be configured to filter based on the protocol port number. For example, the configuration rules are as follows: `access-list 101 deny ahp 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0`. When the ahp message from 192.168.1.1 to 192.168.2.1 is received, the action performed is discarded. These rules only take effect when activated on a port using the `ip-access-group` command. And has the "first activation first effect" feature.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 101 deny ahp 192.168.1.1 0.0.0.0
192.168.2.1 0.0.0.0
```

24.4 Configure IPV4 ICMP Extend ACL Based on IP Addresses

Command

```
access-list (<100-199> | <2000-2699>) (deny | permit) (icmp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) ((A.B.C.D A.B.C.D)
| (any) | (host A.B.C.D))
(<0-255>|echo|echo-reply|redirect|ttl-exceeded|unreachable|)
no access-list (<100-199> | <2000-2699>) (deny | permit) (icmp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) ((A.B.C.D A.B.C.D)
| (any) | (host A.B.C.D))
(<0-255>|echo|echo-reply|redirect|ttl-exceeded|unreachable|)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

(<100-199>|<2000-2699>) : indicates extending the scope of the ACL.

(deny|permit) : ACL action, deny, permit.

Icmp: filter Icmp protocol message.

A.B.C.D A.B.C.D: represents the source/destination IP address and mask, and the mask adopts the anti-code mechanism. For example, 192.168.1.1 0.0.0.0 means that only matches the message with 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

(< 0-255 > | echo | echo - reply | redirect | ttl - exceeded | | unreachable |) :

corresponding icmp message type, echo (ping), echo reply, All redirects, TTL exceeded, All unreachables.

No means to delete.

Description

Configure extended ACL icmp protocol based on IPV4. For example, the configuration rule is as follows: access-list 103 deny icmp 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0 echo. Therefore, when receiving echo message from icmp 192.168.1.1 to icmp 192.168.2.1, the action executed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

Instance

```
Switch> en
Switch#configure terminal
Switch(config)#access-list 103 deny icmp 192.168.1.1 0.0.0.0
192.168.2.1 0.0.0.0 echo
```

24.5 Configure IPV4 ICMP Extend ACL Based on IP Addresses

Command

```
access-list (<100-199>|<2000-2699>) (deny|permit) (icmp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) (<0-255>|query|reportv1|reportv2|
leave|reportv3|)
no access-list (<100-199>|<2000-2699>) (deny|permit) (icmp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) (<0-255>|query|reportv1|reportv2|
leave|reportv3|)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

(<100-199>|<2000-2699>) : indicates extending the scope of the ACL.

(deny|permit) : ACL action, deny, permit.

Igmp: filter Igmp protocol message.

A.B.C.D A.B.C.D: represents the source/destination IP address and mask, and the mask adopts the anti-code mechanism. For example, 192.168.1.1 0.0.0.0 means that only matches the message with 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

(<0-255>|query|reportv1|reportv2|leave|reportv3|): corresponding to different igmp message types, IGMP Membership Query, IGMPv1 Membership Report, IGMPv2 Membership Report, IGMPv2 Leave Group, IGMPv3 Membership Report.

no: means to delete.

Description

Configure extended ACL igmp protocol based on IPV4, destination address should be configured as multicast address, otherwise the corresponding rule cannot be matched.

For example, the configuration rule is as follows: access-list 103 deny igmp

192.168.1.1 0.0.0.0 224.1.2.3 0.0.0.0 leave. Therefore, when the leave message from 192.168.1.1 to igmp of group 224.1.2.3 is received, the action executed is discarded.

These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

Instance

```
Switch> en
Switch#configure terminal
Switch(config)#access-list 103 deny igmp 192.168.1.1 0.0.0.0
224.1.2.3 0.0.0.0 leave
```

24.6 Configure IPV4 based on IP addresses TCP extend ACL

Command

```
access-list (<100-199> | <2000-2699>) (deny | permit) (tcp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) | ) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
```

```
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) | )
(fin|syn|rst|psh|ack|urg| )
```

```
access-list (<100-199> | <2000-2699>) (deny | permit) (tcp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) ((eq | lt | gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) | )
(fin|syn|rst|psh|ack|urg| )
```

```
access-list (<100-199> | <2000-2699>) (deny | permit) (tcp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) | ) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) ((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
(fin|syn|rst|psh|ack|urg| )
```

```
access-list (<100-199> | <2000-2699>) (deny | permit) (tcp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
(fin|syn|rst|psh|ack|urg| )
```

```
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) ((eq|lt|gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) (((eq|lt|gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
(fin|syn|rst|psh|ack|urg|)
```

```
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) (ftp|ftp-data
|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) (((eq|lt|gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
(fin|syn|rst|psh|ack|urg|)
```

```
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (((eq|lt|gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
(fin|syn|rst|psh|ack|urg|)

no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) (ftp|ftp-data
|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) (ftp|ftp-data|po
p3|smtp|telnet|www|<1-65535>))) (fin|syn|rst|psh|ack|urg|)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

(<100-199>|<2000-2699>) : indicates extending the scope of the ACL.

(deny|permit): ACL actions, deny, permit.

Tcp: filter tcp protocol message.

A.B.C.D: represents the source/destination IP address and mask, and the mask adopts the anti-code mechanism. For example, 192.168.1.1 0.0.0.0 means that only matches the message with 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

(eq|lt|gt):

- Match only packets on a given port number
- Match only packets with a lower port number
- Match only packets with a greater port number.

((ftp|ftp-data|pop3|SMTP|Telnet|WWW|<1-65535>))) : corresponding to different

TCP message types:

- File Transfer Protocol (21),
- FTP data connections (20),
- Post Office Protocol v3 (110),
- Simple Mail Transport Protocol (25),

- Telnet (23),
- World Wide Web (HTTP, 80),
- Port number(1-65535)。
- (fin|syn|rst|psh|ack|urg|):
- Match on the FIN bit,
- Match on the Syn bit,
- Match on the Rst bit,
- Match on the Psh bit,
- Match on the Ack bit,
- Match on the Urg bit.

No means to delete.

Description

Configure extended ACL igmp protocol based on IPV4, destination address should be configured as multicast address, otherwise the corresponding rule cannot be matched. For example, the configuration rule is as follows: access-list 101 deny tcp host 192.168.1.1 eq ftp host 192.168.2.1 eq pop3 fin, then when receiving the tcp message from 192.168.1.1 to 192.168.2.1, the action executed is discard. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 101 deny tcp host 192.168.1.1 eq ftp
host 192.168.2.1 eq pop3 fin
Switch(config)#access-list 102 deny tcp host 192.168.1.1 range ftp
ftp host 192.168.2.1 range pop3 pop3 fin
```

24.7 Configure IPV4 based on IP addresses UDP extend ACL

Command

```
access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | ) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | )
```

```

access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp)) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) ((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | )

```

```

access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | ) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((range) (<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))

```

```

access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp)) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((range) (<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))

```

```

no access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | ) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | )

```

```

no access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp)) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | )

```

```

no access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | ) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((range) (<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))

```

```

no access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (hostA.B.C.D)) ( ((range)
(<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp)) ((A.B.C.D A.B.C.D) | (any)

```

```
| (host A.B.C.D)) ((range) (<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

(<100-199>|<2000-2699>) : indicates extending the scope of the ACL.

(deny|permit) : ACL action, deny, permit.

udp: filter udp protocol message.

A.B.C.D A.B.C.D: represents the source/destination IP address and mask, and the mask adopts the anti-code mechanism. For example, 192.168.1.1 0.0.0.0 means that only matches the message with 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

((eq|lt|gt):

- Match only packets on a given port number,
- Match only packets with a lower port number,
- Match only packets with a greater port number.

(<1-65535>|rip|snmp|snmp-trap|tftp): corresponding to different tcp message types:

- Port number(1-65535) (21),
- Routing Information Protocol (router, in.routed, 520),
- Simple Network Management Protocol (161),
- SNMP Traps (162),
- Trivial File Transfer Protocol (69).W

Description

Configure extended ACL igmp protocol based on IPV4, destination address should be configured as multicast address, otherwise the corresponding rule cannot be matched. For example, the configuration rule is as follows: access-list 101 deny udp host 192.168.1.1 eq tftp host 192.168.2.1 eq tftp, then when receiving the tcp tftp message from 192.168.1.1 to 192.168.2.1, the action executed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#access-list 101 deny tcp host 192.168.1.1 eq tftp
host 192.168.2.1 eq tftp
Switch(config)#access-list 102 deny tcp host 192.168.1.1 range tftp
tftp host 192.168.2.1 range 10 30
```

24.8 Configure character type ACL based on IPV4 addresses

Command

```
access-list swos WORD (deny|permit)
(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>)
(A.B.C.D/M|A.B.C.D A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
((label(1-65535)|precedence<0-7>) | tos (0-255) | range <0-255>
<0-255> | pkt-size ((lt|gt)<0-65535> | range <0-65535> <0-65535>)
| fragments | log | interface (in|out) IFNAME)

access-list swos WORD (deny|permit) (icmp) (A.B.C.D/M|A.B.C.D
A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any) ((icmp-type
ICMP-TYPE|label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

access-list swos WORD (deny|permit) (udp) (A.B.C.D/M|A.B.C.D
A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>)
(A.B.C.D/M|A.B.C.D A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>) ((label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

access-list swos WORD (deny|permit) (tcp) (A.B.C.D/M|A.B.C.D
A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>)
(A.B.C.D/M|A.B.C.D A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>) ((label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no access-list swos WORD (deny|permit) (udp) (A.B.C.D/M|A.B.C.D
A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>)
(A.B.C.D/M|A.B.C.D A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>) ((label(1-65535)|precedence<0-7>)|tos (0-255)
```

```
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
no access-list swos WORD (deny|permit) (icmp) (A.B.C.D/M|A.B.C.D
A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any) ((icmp-type
ICMP-TYPE|label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
no access-list swos WORD (deny|permit) ( tcp) (A.B.C.D/M|A.B.C.D
A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>)
(A.B.C.D/M|A.B.C.D A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>) ((label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
no access-list swos WORD (deny|permit)
(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>)
(A.B.C.D/M|A.B.C.D A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
((label(1-65535)|precedence<0-7>)|tos (0-255) |range <0-255>
<0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

Swos WORD: configure a character ACL.

(deny|permit) : ACL action, deny, permit.

(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>):

A.B.C.D A.B.C.D: represents the source IP address and mask. The mask adopts the anti-code mechanism, such as 192.168.1.1 0.0.0.0 means only match 192.168.1.1 source IP message.

host A.B.C.D: indicates that the source IP address is A.B.C.D 0.0.0.0.

any: indicates that the source IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

Label: configure priority.

Precedence: configure priority.

Tos: configure priority.

Pkt-size: configure message length

Interface[IFNAME] : install port number.

Description

The access-list command is used to create a standard filter rule group. A group can support up to 32 rules. No is to delete a rule group. When the message matches the corresponding rule, the action will be executed. For example, the configuration rule is as follows: access-list swos AA deny ip 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0. When the message from 192.168.1.1 is received and sent to 192.168.2.1, the action performed is discard. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list swos AA deny ip 192.168.1.1 0.0.0.0
192.168.2.1 0.0.0.0
```

24.9 Configure character type ACL based on IPV6 addresses

Command

```
ipv6 access-list swos WORD (deny|permit)
(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>)
(X:X::X:X/M|X:X::X:X |any) (X:X::X:X/M|X:X::X:X |any)
((label(1-65535)|precedence<0-7>) | tos (0-255) |range <0-255>
<0-255> | pkt-size ((lt|gt) <0-65535> | range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
ipv6 access-list swos WORD (deny|permit) (icmp)
(X:X::X:X/M|X:X::X:X |any) (X:X::X:X/M|X:X::X:X |any) ((icmp-type
ICMP-TYPE|label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
ipv6 access-list swos WORD (deny|permit) (udp)
(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>) (X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne)
<0-65535> | range <0-65535> <0-65535>)
((label(1-65535)|precedence<0-7>) | tos (0-255) |range <0-255>
```

```
<0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
        ipv6 access-list swos WORD (deny|permit) (tcp)
(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>)(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne)
<0-65535> | range <0-65535>
<0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
no ipv6 access-list swos WORD
(deny|permit) (udp) (X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne)
<0-65535> | range <0-65535> <0-65535>)(X:X::X:X/M|X:X::X:X |any)
((eq|lt|gt|ne) <0-65535> | range <0-65535>
<0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
no ipv6 access-list swos WORD (deny|permit)
 icmp) (X:X::X:X/M|X:X::X:X |any) (X:X::X:X/M|X:X::X:X |any)
((icmp-type ICMP-TYPE|label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
no ipv6 access-list swos WORD
(deny|permit) ( tcp) (X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne)
<0-65535> | range <0-65535> <0-65535>)(X:X::X:X/M|X:X::X:X |any)
((eq|lt|gt|ne) <0-65535> | range <0-65535>
<0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

```
no ipv6 access-list swos WORD (deny|permit)
(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>)( X:X::X:X/M
|X:X::X:X |any) (X:X::X:X/M|X:X::X:X |any)
((label(1-65535)|precedence<0-7>)|tos (0-255) |range <0-255>
<0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

Swos WORD: configure a character ACL.

(deny|permit) : ACL action, deny, permit.

(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>):

X:X::X:X/M|X:X::X:X |any: Represents the source IP address and mask, and the mask adopts the anti-code mechanism, such as: fe80::01 :: represents only messages matching fe80::01 source IP.

any: indicates that the source IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

Label: configure priority.

Precedence: configure priority.

Tos: configure priority.

Pkt-size: configure message length

Interface[IFNAME] : install port number.

Description

The access-list command is used to create a standard filter rule group. A group can support up to 32 rules. No is to delete a rule group. When the message matches the corresponding rule, the action will be executed. For example, the configuration rule is as follows: ipv6 access-list swos qwer deny any fe80::01 :: fe80::02 :: then when receiving the message from fe80::01 ::, to fe80::02 ::, the action executed is discard. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#ipv6 access-list swos qwer deny any fe80::01 ::
fe80::02 ::
```

24.10View All Configured ACL

Command

show access-list

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

-

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#show access-list
```

24.11 Configure time-range

Command

```
time-range NAME
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

Name.

Description

Time-range means to configure a period of time during which the action of the ACL is executed, and when the time is up, the action of the ACL is not executed, which acts as a timing function. Support 20 groups of time-range, each group supports two types of time absolute (absolute time) and inquire (cycle time), and each group supports the creation of up to 16 time rules. Absolute time means to select a period of time, cycle time means to select a period of time, the weekly cycle time is divided into day, workday, non-work, supporting the configuration of time as well.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#time-range ac // create a time-range called ac
```

```

Switch(config-time-range)#absolute start 12:00 1971-12-14 end 14:00 1971-12-15 // configure a period of time from 12:00
1971-12-14 to 14:00 1971-12-15.
Switch(config-time-range)#periodic 09:00 to 12:00 daily //
configure a weekly cycle time from 09:00 to 12:00 every morning
*Switch#show time-range // view the current configuration of
time-range
Current time: 10:52 1970-01-01
time-range ac (inactive)
    periodic 09:00 to 12:00 daily
    absolute start 12:00 1971-12-14 end 14:00 1971-12-15
Switch(config-time-range)#no periodic 09:00 to 12:00 // delete
the sub-items of configuration cycle time within the time-range
Switch(config-time-range)#no absolute start 12:00 1971-12-14 end
14:00 1971-12-15 //Delete the configuration absolute time
subitem in the time-range
Switch(config)#no time-range ac //delete time-range ac

```

24.12 Time-range binds to the ACL

Command

```

access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>)
time-range WORD

```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

Bind a time-range to an ACL and perform the ACL action within the setting time. An ACL can only bind one time-range, and one time-range can bind multiple ACL. When deleted, if the time-range is referenced, the time-range is not allowed to be deleted and its subitems are allowed to be modified.

Instance

```

Switch(config)#access-list 10 time-range ad // bind the standard
ACL numbered 10 to time-range ad.

```

```
Switch(config)#no access-list 10 time-range ad // unbind the
standard ACL numbered 10 to time-range ad.
```

24.13 Activate ACL

Command

```
ip-access-group (<1-199>|<1300-2699>) in
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

(<1-199>|<1300-2699>) in: ACL rule group ID, in represents the ingress direction.

Description

ACLS configured with time-range also need to be activated, meeting the rule of first activation first effect.

A port can only activate one IP address ACL and one MAC address ACL.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#ip-access-group 1 in
```

24.14 Configure ACL based on MAC address

Command

```
mac access-list <2000-2699> (deny|permit) MAC MASK MAC MASK
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) MAC MASK MAC MASK
(<1-65535>|NUM|)

mac access-list <2000-2699> (deny|permit) MAC MASK host MAC
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) MAC MASK host MAC
(<1-65535>|NUM|)
```

```
mac access-list <2000-2699> (deny|permit) MAC MASK any
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) MAC MASK any
(<1-65535>|NUM|)
```

```
mac access-list <2000-2699> (deny|permit) any host MAC
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) any host MAC
(<1-65535>|NUM|)
```

```
mac access-list <2000-2699> (deny|permit) any MAC MASK
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) any MAC MASK
<1-65535>|NUM|)
```

```
mac access-list <2000-2699> (deny|permit) host MAC MAC MASK
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) host MAC MAC MASK
(<1-65535>|NUM|)
```

```
mac access-list <2000-2699> (deny|permit) host MAC any
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) host MAC any
(<1-65535>|NUM|)
```

```
mac access-list <2000-2699> (deny|permit) host MAC host MAC
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) host MAC host MAC
(<1-65535>|NUM|)
```

```
mac access-list <2000-2699> (deny|permit) any any (<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) any any
(<1-65535>|NUM|)
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<2000-2699>: standard MAC ACL label range

MAC MASK MAC MASK: source MAC + MASK destination MAC+ MASK.

(<1-65535>|NUM|): Ethernet type. Hexadecimal/hexadecimal input.

Description

Configure an ACL based on MAC address to perform the configured action when the message matches the rule issued.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#mac access-list 2001 deny any any 0x8100 //
Configure a message ACL that dismisses a MAC address of type 0x8100
Ethernet Switch(config)#no mac access-list 2001 deny any any 0x8100
///// delete a message ACL that discards a MAC address of Ethernet
type 0x8100
```

24.15View All Configured MAC ACL

Command

```
show mac access-list
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

-

Instance

```
Switch> enable
Switch# show mac access-list
```

24.16Time-range and MAC ACL binding

Command

```
mac access-list <2000-2699> time-range WORD
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

Bind a time-range to an ACL and perform the MAC ACL action within the setting time. An MAC ACL can only bind one time-range, and one time-range can bind multiple MAC ACL. When deleted, if the time-range is referenced, the time-range is not allowed to be deleted and its subitems are allowed to be modified.

Instance

```
Switch(config)#mac access-list 2001 time-range ad // bind the
standard MAC ACL numbered 2001 to time-range ad.
Switch(config)#no mac access-list 2001 time-range ad // unbind the
standard MAC ACL numbered 2001 to time-range AD.
```

24.17 Activate MAC ACL

Command

```
mac-access-group <2000-2699> in
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

<2000-2699>: MAC ACL rule group ID
in: indicates the direction of ingress.

Description

ACLs configured with time-range also need to be activated, meeting the rule of first activation first effect.

A port can only activate one IP address ACL and one MAC address ACL.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#mac-access-group 2001 in
```

24.18 View all Activated ACL

Command

show access-group

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

View the currently activated ACL port .

Instance

Switch> **enable**

Switch#**show access-group**

25 802.1X Authentication Configuration

25.1 Global 802.1X Authentication Enablement

Command

```
[ no ] dot1x system-auth-ctrl
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

-

Description

dot1x system-auth-ctrl: command is used to enable global dot1x authentication function.

no dot1x system-auth-ctrl: command is used to disable global dot1x authentication function.

By default, global dot1x authentication function is disabled.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#dot1x system-auth-ctrl
```

25.2 802.1X authentication port authorization mode

Command

```
dot1x port-control (auto | force-authorized | force-unauthorized)
no dot1x port-control
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

auto: set port to enable 802.1x authentication mode and it is unauthorized mode by default.

force-authorized: set the port to forced authorized mode.

force-unauthorized: set the port to unauthorized forced mode

Description

dot1x port-control: command is used to set the access control mode of 802.1x on the specified port.

no dot1x port-control: the command is used to delete port 802.1x authentication function.

The port is not configured with 802.1x authentication by default.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x port-control auto
```

25.3 802.1X Authentication Port Controlled Direction

Command

```
dot1x port-control dir (both | in)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

both: the controlled direction is bi-directional

in: the controlled direction is ingress.

Description

dot1x port-control dir: command is used to configure port controlled directions.

By default, the controlled direction of the port is ingress.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface ge1
```

```
Switch(config-ge1)#dot1x port-control dir both
```

25.4 802.1X Authentication EAPOL Protocol Version

Command

```
dot1x protocol-version (1| 2)
```

```
no dot1x protocol-version
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

1: Configure EAPOL to 1

2: Configure EAPOL to 2

Description

dot1x protocol-version: command is used for the EAPOL protocol version of dot1x.

no dot1x protocol-version: command is used for the default EAPOL protocol version of dot1x.

By default, the EAPOL protocol message version is 2.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface ge1
```

```
Switch(config-ge1)#dot1x protocol-version 2
```

25.5 802.1X Authentication Port Silent Time

Command

```
dot1x quiet-period <1-65535>  
no dot1x quiet-period
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

1-65535: the silent time of the port, ranging from 1-65535 seconds, defaults to 60 seconds

Description

dot1x quiet-period: Command for the dot1x port's silence time.

no dot1x quiet-period: command is used for the default quiet time of the dot1x port.

By default, the silence time of the dot1x port is 60 seconds.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#interface ge1  
Switch(config-ge1)#dot1x quiet-period 120
```

25.6 802.1x Authorization Port Reauthentication Interval

Command

```
dot1x timeout re-authperiod <1-4294967295>  
no dot1x timeout re-authperiod
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

1-4294967295: re-authentication interval for port, the range is 1-4294967295 seconds, the default value is 3600 seconds.

Description

dot1x timeout re-authperiod: command is used for re-authentication intervals on the dot1x port.

no dot1x timeout re-authperiod: command is used for the default re-authentication interval of dot1x port.

By default, the re-authentication interval on dot1x port is 3600 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x timeout re-authperiod 1200
```

25.7 802.1X Authorization Server Timeout Time

Command

```
dot1x timeout server-timeout <1-65535>
no dot1x timeout server-timeout
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

1-65535: the server timeout of the port, ranging from 1- 65535 seconds, defaults to 30 seconds.

Description

dot1x timeout server-timeout: The command is used for the server timeout on the dot1x port.

no dot1x timeout server-timeout: command is for the default server timeout of the dot1x port.

By default, the server timeout on dot1x port is 30 seconds.

Instance

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x timeout server-timeout 60
```

25.8 802.1X Authorization Client Timeout Time

Command

```
dot1x timeout supp-timeout <1-65535>
no dot1x timeout supp-timeout
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

1-65535: the client timeout of the port, ranging from 1- 65535 seconds, defaults to 30 seconds

Description

dot1x timeout supp-timeout: command is used for the client timeout on the dot1x port.

no dot1x timeout supp-timeout: command is for the default client timeout of the dot1x port.

By default, the client timeout on dot1x port is 30 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x timeout supp-timeout 60
```

25.9 802.1X Authorization Message Retransmission Interval

Command

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```


View

Interface Mode

Default Level

2: Configuration level

Parameters

1-65535: the retransmission interval of the port, the range is 1-65535 seconds, the default is 30 seconds

Description

dot1x timeout tx-period: command is used for retransmission intervals on the dot1x port.

no dot1x timeout tx-period: command is used for the default retransmission interval of the dot1x port.

By default, the retransmission interval on dot1x port is 30 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x timeout tx-period 60
```

25.10 802.1X Authorization Message Retransmission Interval

Command

```
dot1x reauthMax <1-10>
no dot1x reauthMax
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

1-65535: the number of retransmission of request/id message of the port, ranging from 1 to 10 seconds, it is 3 times by default

Description

dot1x reauthMax: command is used for the times of retransmissions of the dot1x port.

no dot1x reauthMax: command is used for the default times of retransmissions
By default, the times of retransmissions on dot1x port is 3.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x reauthMax 4
```

25.11 802.1x authorization port reauthentication mode

Command

```
dot1x reauthentication
no dot1x reauthentication
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

dot1x reauthentication: command is used to enable re-authentication on the dot1x port.

no dot1x reauthentication: command is used to disable the re-authentication feature on the dot1x port.

By default, the re-authentication interval on dot1x port is 3600 seconds.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x reauthentication
```

25.12 802.1X Authentication Port Initialization

Command

```
dot1x initialize
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

dot1x initialize: command is used to initialize and unauthorize the dot1x port and attempt to re-authenticate on the dot1x port.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x initialize
```

25.13 802.1X Authorization Key Encryption Function

Command

```
dot1x keytxenabled (enable | disable)
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

-

Description

dot1x keytxenabled enable: command is used to enable key encryption on the dot1x port (when clients interact with EPAOL messages).

dot1x keytxenabled disable: command is used to disable key encryption on the dot1x port.

Key encryption on the dot1x port is disabled by default.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x keytxenabled enable
```

25.14 Display 802.1X Authentication Global Information

Command

```
show dot1x
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show dot1x: command is used to display dot1x global information and radius client information.

Instance

```
Switch> enable
Switch#show dot1x
802.1X Port-Based Authentication Enabled
RADIUS client address: not configured
```

25.15 Display 802.1X Authentication Detailed Information

Command

```
show dot1x all
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show dot1x all: command is used to display dot1x global information and radius client information, as well as port information.

Instance

```
Switch> enable
Switch#show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS client address: not configured
802.1X info for interface ge4
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 90
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

25.16 Display 802.1X Authentication Port Information

Command

show dot1x interface <IFNAME>

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

lfname:specifies the port name

Description

show dot1x interface: command is used to display dot1x information for the specified port.

Instance

```
Switch> enable
Switch#show dot1x interface ge4
802.1X info for interface ge4
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 92
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

25.17 Display 802.1X Authentication Port Diagnosis Information

Command

show dot1x diagnostics interface <IFNAME>

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

lfname:specifies the port name

Description

show dot1x diagnostics interface: command is used to display dot1x diagnostics information for the specified port.

Instance

```
Switch> enable
Switch#show dot1x diagnostics interface ge4
802.1X Diagnostics for interface ge4
authEnterConnecting: 707
authEaplogoffWhileConnecting: 355
authEnterAuthenticating: 0
authSuccessWhileAuthenticating: 0
authTimeoutWhileAuthenticating: 0
authFailWhileAuthenticating: 0
authEapstartWhileAuthenticating: 0
authEaplogoggWhileAuthenticating: 0
authReauthsWhileAuthenticated: 0
authEapstartWhileAuthenticated: 0
authEaplogoffWhileAuthenticated: 0
BackendResponses: 0
BackendAccessChallenges: 0
BackendOtherrequestToSupplicant: 0
BackendAuthSuccess: 0
BackendAuthFails: 0
```

25.18 Display 802.1X Authentication Port Session Information

Command

show dot1x sessionstatistics interface <IFNAME>

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

lfname:specifies the port name

Description

show dot1x sessionstatistics interface: command is used to display dot1x sessionstatistics information for the specified port.

Instance

```
Switch> enable
Switch#show dot1x sessionstatistics interface ge4
802.1X session statistics for interface ge4
session authentication method: Local server
session time: 0 secs
session user name:
session terminate cause: Port failure
```

25.19 Display 802.1X Authentication Port Message Statistics

Command

show dot1x statistics interface <IFNAME>

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

lname:specifies the port name

Description

show dot1x statistics interface: command is used to display dot1x message for the specified port.

Instance

```
Switch> enable
Switch#show dot1x statistics interface ge4
802.1X statistics for interface ge4
EAPOL Frames Rx: 0 - EAPOL Frames Tx: 0
EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
EAP Rsp/Id Frames Rx: 0 - EAP Response Frames Rx: 0
EAP Req/Id Frames Tx: 719 - EAP Request Frames Tx: 0
Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
```



```
EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src:
0000.0000.0000
```

25.20 RADIUS Server Regeneration Interval

Command

```
radius-server deadtime <0-1440>
no radius-server deadtime
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

0-1440: regeneration interval of RADIUS, ranging from 0-1440 minutes, defaults to 0

Description

radius-server deadtime: command is used to configure the interval between the radius unreachable is restored to reachable.

no radius-server deadtime: command is used to delete the interval.

By default, the regeneration interval is 0.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#radius-server deadtime 5
```

25.21 RADIUS Server

Command

```
radius-server host <HOSTNAME> {key STRING | auth-port PORTNO |
timeout SEC | retransmit RETRIES}
no radius-server host <HOSTNAME> (auth-port PORTNO | )
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

hostname: IP address or host name of RADIUS server

STRING: Shared key with RADIUS server

PORTNO: UDP port of RADIUS authentication, the value range is 0-65535

SEC: timeout interval of RADIUS server, value range is 1-1000, the default value is 5 seconds

RETRIES: the number of times the RADIUS server retransmits over the timeout, the value range is 1-100, which is 3 times by default

Description

radius-server host: command is used to configure the RADIUS server.

no radius-server host: command is used to configure the RADIUS server.

By default, the RADIUS server is not configured.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#radius-server host 192.168.1.100 key 123456
```

```
auth-port 1812
```

26 Alarm Configuration

26.1 Enable Port Alarm

Command

```
system alarm enable
```

View

```
ge (Gigabit Ethernet) port view
```

```
xe (10 Gigabit Ethernet) port view
```

Default Level

```
2: Configuration level
```

Parameters

```
-
```

Description

Enabling port up/down the alarm light on the panel will be lit immediately when the port down occurs. When the port up occurs, the alarm light on the panel will be turned off. By default, it is turned off. However, the warning light will also be turned on when the power alarm is enabled, so it is recommended not to turn them on at the same.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge 1
Switch(config-ge1)#system alarm enable
```

26.2 Disable Port Alarm

Command

```
system alarm disable
```

View

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

Default Level

2: Configuration level

Parameters

-

Description

Enabling port up/down the alarm light on the panel will be lit immediately when the port down occurs. When the port up occurs, the alarm light on the panel will be turned off. By default, it is turned off. However, the warning light will also be turned on when the power alarm is enabled, so it is recommended not to turn them on at the same.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge 1
Switch(config-ge1)#system alarm disable
```

26.3 Enable Power Alarm

Command

```
power <1-2> alarm enable
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<1-2>: means power supply 1, 2

Description

Enabling power<1-2>alarm, light on the panel will be lit immediately when the port is down. When power is specified to up, the alarm light on the panel will be turned off. By default, it is turned off. However, the warning light will also be turned on when the port alarm is enabled, so it is recommended not to turn them on at the same.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#power 1 alarm enable
```

26.4 Power off Warning

Command

```
power <1-2> alarm disable
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<1-2>: means power supply 1, 2

Description

Enabling power<1-2>alarm, light on the panel will be lit immediately when the port is down. When power is specified to up, the alarm light on the panel will be turned off. By default, it is turned off. However, the warning light will also be turned on when the port alarm is enabled, so it is recommended not to turn them on at the same.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#power 1 alarm disable
```

27 RMON Configuration

27.1 RMON Alarm Group

Command

```
rmon alarm <Index> <alarm-variable> interval <Seconds> {absolute  
| delta} rising-threshold <RISING_THRES> event <event_Index>  
falling-threshold <FALL_THRES> event <event_Index> ( owner  
<name>|)  
no rmon alarm <Index>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

Index: warning group index, the range is 1-65535.

alarm-variable: the format is etherStatsEntry.n.n

Seconds: sampling time interval ranging from 1-4294967295

Delta: sampling type is variable value (the current sample value of the selected variable relative to the last sample value)

absolute: the sampling type is absolute.

rising-threshold RISING_THRES: upper threshold, the value range is 0 ~ 2147483647.

event_Index: index of event groups corresponding to the upper threshold, the range is 1-65535.

falling -threshold FALL_THRES: lower threshold, the value range is 0 ~ 2147483647.

event_Index: index of event groups corresponding to the lower threshold, the range is 1-65535.

name: character string, creator of the row.

Description

rmon alarm: command is used to configure alarm group.

no rmon alarm: command is used to delete alarm group.

By default alarm group is not configured.

The alarm variable format support string format (not OID format), formats are etherStatsEntry. integer. instance or etherStatsString.instance, integer the range is 1-21, corresponding to the etherStatsString below respectively.

etherStatsString supports the following:

"etherStatsIndex"
"etherStatsDataSource"
"etherStatsDropEvents"
"etherStatsOctets"
"etherStatsPkts"
"etherStatsBroadcastPkts"
"etherStatsMulticastPkts"
"etherStatsCRCAlignErrors"
"etherStatsUndersizePkts"
"etherStatsOversizePkts"
"etherStatsFragments"
"etherStatsJabbers"
"etherStatsCollisions"
"etherStatsPkts64Octets"
"etherStatsPkts65to127Octets"
"etherStatsPkts128to255Octets"
"etherStatsPkts256to511Octets"
"etherStatsPkts512to1023Octets"
"etherStatsPkts1024to1518Octets"
"etherStatsOwner"
"etherStatsStatus"

Instance is an interface index.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#rmon alarm 1 etherStatsIndex.1 interval 20 delta
rising-threshold 200 event 1 falling-threshold 20 event 1
```

27.2 RMON Statistical Group

Command

```
rmon collection stats <INDEX>  
no rmon collection stats <INDEX>
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

INDEX: statistics group Index, the range is 1-65535.

Description

rmon collection stats: command is used to configure the port statistics group.
no rmon collection stats: command is used to cancel the port statistics group.
The port is not configured with statistics group by default.

Instance

```
Switch> enable  
Switch#configure terminal  
Switch(config)#interface ge1  
Switch(config-ge1)#rmon collection stats 1
```

27.3 RMON History Group

Command

```
rmon collection history <INDEX> {buckets <NUMBER> | interval  
<SECONDS> | owner <NAME> | }  
no rmon collection history <INDEX>
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

INDEX: statistics group index, the range is 1-65535.

NUMBER: set the historical table capacity corresponding to the history group, ranging from 1-65535.

SECONDS: set the historical group statistical cycle value in the range of 1-3600

Seconds.

NAME: creator of the row

Description

rmon collection history: command is used to configure the port history group.

no rmon collection stats: command is used to delete the port statistics group.

The port is not configured with history group by default.

Instance

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface ge1
```

```
Switch(config-ge1)#rmon collection history 1 buckets 10 interval  
60
```

27.4 RMON Event Group

Command

```
rmon event <INDEX> {description <STRING> | log | trap <COMMUNITY>}  
(owner <NAME> | )  
no rmon event <INDEX>
```

View

Interface Mode

Default Level

2: Configuration level

Parameters

INDEX: event group index, the range is 1-65535.

Log: log events. When events are triggered, the system logs them.

STRING: event description.

COMMUNITY: Trap event. When the event is triggered, the system will send it with community as the group name.

NAME: creator of the row

Description

rmon event: command is used to configure the event group.

no rmon event: command is used to cancel the event group.

The port is not configured with event group by default.

Instance

```
Switch> enable
Switch#configure terminal
Switch(config)#rmon event 2 log
```

27.5 Display RMON Alarm Group Information

Command

```
show rmon alarm
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show rmon alarm: command is used to display alarm group information.

Instance

```
Switch> enable
Switch#show rmon alarm
alarm Index = 1
alarm status = VALID
    alarm Interval = 20
    alarm Type is Delta
    alarm Value = 0
    alarm Rising Threshold = 200
    alarm Rising Event = 1
    alarm Falling Threshold = 20
    alarm Falling Event = 1
    alarm Owner is RMON_SNMP

alarm Index = 2
alarm status = VALID
    alarm Interval = 20
    alarm Type is Delta
    alarm Value = 0
    alarm Rising Threshold = 200
    alarm Rising Event = 1
```

```
alarm Falling Threshold = 20
alarm Falling Event = 1
alarm Owner is RMON_SNMP
```

27.6 Display RMON Statistics Information

Command

```
show rmon statistics
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show rmon statistics: command is used to display statistics group information.

Instance

```
Switch> enable
Switch#show rmon statistics
    rmon collection index 1
    stats->ifindex = 5002
    input packets 00, bytes 00, dropped 00, multicast packets 00
    output packets 00, bytes 3406566434058944, multicast packets
00 broadcast packets 00
```

27.7 Display RMON History Group Information

Command

```
show rmon history
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show rmon history: command is used to display history group information.

Instance

```
Switch> enable
Switch#show rmon history
    history index = 1
    data source ifindex = 5002
    buckets requested = 50
    buckets granted = 50
    Interval = 1800
    Owner RMON_SNMP
```

27.8 Display RMON Event Group Information

Command

show rmon event

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show rmon event: command is used to display event group information.

Instance

```
Switch> enable
Switch#show rmon event
    event Index = 1
    Description RMON_SNMP
    Event type Log
    Last Time Sent = 07:43:20
    Owner RMON_SNMP
```

28 Log Configuration

28.1 Log File Size Limit

Command

```
log file size <10-10000>
no log file size
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

<10-10000>: log file size, the unit is KB.

Description

log file size: the command is used to set the maximum size of logfile in KB.

no log file size: the command is used to delete the setting of logfile size and restore it to the default size, namely 2M.

Instance

```
Configure the logfile size to 5M
Switch> enable
Switch#configure terminal
Switch(config)#log file size 5000
```

```
Delete settings of logfile size
Switch> enable
Switch#configure terminal
Switch(config)#no log file size
```

28.2 Log stdout Display

Command

```
log stdout
no log stdout
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

No.

Description

log stdout: the command is used to open the switch and display the log information in stdout.

no log stdout: the command is used to close the switch and not to display the log information in stdout.

Instance

Configure to open the log information displayed in stdout

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#log stdout
```

close the log information displayed in stdout

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#no log stdout
```

28.3 LogInformation Highest Display Level

Command

```
Log trap ( alerts | critical | debugging | emergencies | errors
| informational | notifications | warnings )
no log trap
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

No.

Description

log trap: the command sets the maximum display level of log information.

no log trap: the command is used to remove the settings for the highest display level of log information and restore it to the default level, which is the "debug" level.

Instance

```
# set the log information for the highest level "informational"
Switch> enable
Switch#configure terminal
Switch(config)#log trap informational
```

Delete the highest level Settings for log information

```
Switch> enable
Switch#configure terminal
Switch(config)#no log trap
```

28.4 Log Level Record Display

Command

log record-priority
no log record-priority

View

Configure Mode

Default Level

2: Configuration level

Parameters

No.

Description

log record-priority: the command is used to open the level of log information, that is, to display the information according to the level of log information.

no log record-priority: the command is used to close the level of log information, and all log information is unified as debug level.

Instance

Configure to open log information record-priority

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#log record-priority
```

Close log information record-priority

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#no log record-priority
```

28.5 Syslog Server Download Log

Command

```
log syslog server <A.B.C.D> [<PORT>]
```

```
no log syslog server
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: syslog server IP address

PORT: The port used by the syslog server.

Description

log syslog server: the command is used to set the IP address of the remote syslog server. After executing the command, the log information of the system will be sent to the syslog server with the specified IP address for processing remotely. The parameter A.B.C.D specifies the IP address used by the syslog server, and the parameter PORT specifies the port used by the syslog server.

no log syslog server: the command is used to delete the configuration of the remote syslog server. After executing the command, the system will no longer send log information to any remote syslog server, but only save the log information locally.

Instance

```
# configuration sends log information to syslog server 192.168.1.1  
on port 8848
```

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#log syslog server 192.168.1.1 8848
```

```
#Disable the log sending function to the remote syslog server
```

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#no log syslog
```

29 NTP Configuration

29.1 NTP server

Command

```
ntp server <A.B.C.D>  
no ntp server <A.B.C.D | all>
```

View

Configure Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: ntp server IP address.

Description

ntp server <A.B.C.D>: used to configure the IP address of ntp server and start the ntp service. The default ntp service is not enabled. Only one ntp server is currently supported.

no ntp server <A.B.C.D/all> : delete the configured ntp server IP address and disable the ntp service. A.B.C.D is the address of the NTP server that need to be deleted. Since the system currently supports at most one ntp server IP configuration, the two forms of this command achieve the same effect: delete all ntp server IP addresses and disable the ntp service.

Instance

```
# Enable ntp service and configure ntp server ip to 192.168.1.1  
Switch> enable  
Switch#configure terminal  
Switch(config)#ntp server 192.168.1.1
```

Delete all configured ntp server IP and disable the ntp service
(1)

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#no ntp server 192.168.1.1
```

Delete all configured ntp server IP and disable the ntp service
(2)

```
Switch> enable
```

```
Switch#configure terminal
```

```
Switch(config)#no ntp server all
```

30 Network Diagnose Configuration

30.1 Ping Test

Command

```
ping WORD
ping ip WORD
ping ipv6 WORD
ping
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

WORD: the connected destination IP address that needs to be checked.

Ipv6: supported ipv6.

Description

-

Instance

```
Switch> enable
Switch#ping 192.168.1.188
PING 192.168.1.188 (192.168.1.188): 56 data bytes
64 bytes from 192.168.1.188: seq=0 ttl=128 time=1.493 ms
64 bytes from 192.168.1.188: seq=1 ttl=128 time=13.077 ms

--- 192.168.1.188 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 1.493/7.285/13.077 ms
```

```
*Switch#ping ipv6 fe80::01 (Ipv6 address needs to be configured
to fe80::02/64)
Output Interface: vlanif1
PING fe80::01 (fe80::1): 56 data bytes
64 bytes from fe80::1: seq=0 ttl=128 time=0.536 ms
64 bytes from fe80::1: seq=1 ttl=128 time=0.483 ms

--- fe80::01 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.483/0.509/0.536 ms
```

30.2 TracerouteTest

Command

```
traceroute ip WORD
traceroute ipv6 WORD
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

WORD: the connected destination IP address that needs to be checked.

Ipv6: supported ipv6.

Description

-

Instance

```
Switch> enable
Switch#traceroute ip 192.168.1.254
traceroute to 192.168.1.254 (192.168.1.254), 30 hops max, 38 byte
packets
 1 192.168.1.254 (192.168.1.254) 0.036 ms 0.033 ms 0.013 ms

*Switch#traceroute ipv6 fe80::01 (Ipv6 address needs to be
configured to fe80::02/64 )
Output Interface: vlanif1
traceroute to fe80::01 (fe80::1), 30 hops max, 16 byte packets
 1 fe80::1 (fe80::1) 1.144 ms 0.440 ms 0.346 ms
```

30.3 Port Loopback

Command

```
loopback IFNAME internal mac
loopback IFNAME internal phy
no loopback IFNAME internal
```

View

Privileged Exec Mode

Default Level

1: View level

Parameters

IFNAME: Specify the name of test port.

Internal: represents an internal ring test.

mac/phy: the loop need to test is in the MAC layer or phy layer

Description

When the port loopback test is enabled, the port link light will be on, no execution will cancel the test, and the port link light will be off.

Instance

```
Switch> enable
Switch#loopback ge1 internal mac
Switch#no loopback ge1 internal
```

31 System Management

31.1 Device Information Display

31.1.1 Display System Version

Command

show version

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

-

Description

show version: the command displays the current system version information.

Instance

```
# Display System Current Version Information
Switch> enable
Switch#show version
```

31.1.2 Display Product Information

Command

show product-info [<NAME>]

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

NAME: product information name, no parameters by default.

Description

show product-info [**<NAME>**]: the command is used to display the product information value of the given name, and all product information will be displayed when no parameters are provided.

Instance

```
# Display Product Information:
Switch> enable
Switch(config)#show product-info
```

31.2 System Software Upgrade

Command

copy tftp package <A.B.C.D> <WORD>

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

A.B.C.D:tftp server ip address.

WORD: the name of the upgrade file

Description

copy tftp package: the command is used to upgrade the system software, in which the parameter A.B.C.D is the IP address of the tftp server, and WORD is the file name of “xxx.bin” for upgrade.

When files are uploaded and downloaded, the tftpd32 software can be used as the tftp server on the PC. When a file is transferred, make sure the TFTP server is open and the file path is correct.

Instance

```
# Upgrade system WWW and product information
Switch> enable
Switch#copy tftp package 192.168.1.1 packetweb.bin

# Upgrade System Software
Switch> enable
Switch#copy tftp package 192.168.1.1 packetapp.bin
```

31.3 Configuration File Import and Export

31.3.1 Import Configuration File

Command

```
copy tftp startup-config <A.B.C.D> <WORD>
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: tftp server ip address

WORD: the name of the upgraded configuration file

Description

copy tftp startup-config: the command is used to upgrade the system configuration file, in which the parameter A.B.C.D is the IP address of the tftp server, and WORD is the name of the configuration file used for the upgrade.

Instance

```
# Upgrade System Configuration File
Switch> enable
Switch#copy tftp startup-config 192.168.1.1 SWOS.conf
```

31.3.2 Configure File Export

Command

```
copy flash startup-config <A.B.C.D> (WORD| )
```

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: : tftp server ip address.

WORD: The name of the upgraded configuration file.

Description

copy tftp startup-config: the command is used to download starp-config files to the tftp server, in which the parameter A.B.C.D is the IP address of the tftp server, and WORD is the file name used when saving to the tftp server.

Instance

```
# upload startup-config to tftp server "192.168.1.1" and name it
"SWOS.conf"
Switch> enable
Switch#copy flash startup-config 192.168.1.1 SWOS.conf
```

31.4 Log File Export

Command

copy flash logfile <A.B.C.D> (WORD|)

View

Privileged Exec Mode

Default Level

2: Configuration level

Parameters

A.B.C.D: tftp server ip address.

WORD: the name of the upgraded configuration file.

Description

copy flash logfile: the command is used to download logfile to the tftp server, in which the parameter A.B.C.D is the IP address of the tftp server, and WORD is the file name used when saving to the tftp server.

Instance

```
# download logfile to tftp server "192.168.1.1" and name it
"message.log"
Switch> enable
Switch#copy flash logfile 192.168.1.1 message.log
```

31.5 Save Configuration

Command

```
copy running-config startup-config
write
do write
```

View

Privileged Exec Mode
Any

Default Level

2: Configuration level

Parameters

No.

Description

copy running-config startup-config: the command is used to cover the startup-config file with running-config, that is, to save running-config. Running-config is the configuration file that is currently running, and startup-config is the configuration file that is currently saved. copy running-config startup-config is to execute a "write" and save the configuration file.

do write: command can perform the save configuration in any mode (except Privileged Exec Mode).

Instance

```
# Save running-config
Switch> enable
Switch#copy running-config startup-config
#or
Switch> enable
*Switch#configure terminal
Switch(config)#do write
Building Configuration...
```

[OK]

31.6 Reboot the Device.

Command

reboot

View

Privileged Exec Mode

Default Level

1: View level

Parameters

-

Description

Reboot the device

Instance

```
Switch> enable
Switch#reboot
reboot system? (y/n): y
```

31.7 Restore Factory Settings

Command

erase startup-config
rm startup-config

View

Privileged Exec Mode

Default Level

1: Configuration level

Parameters

-

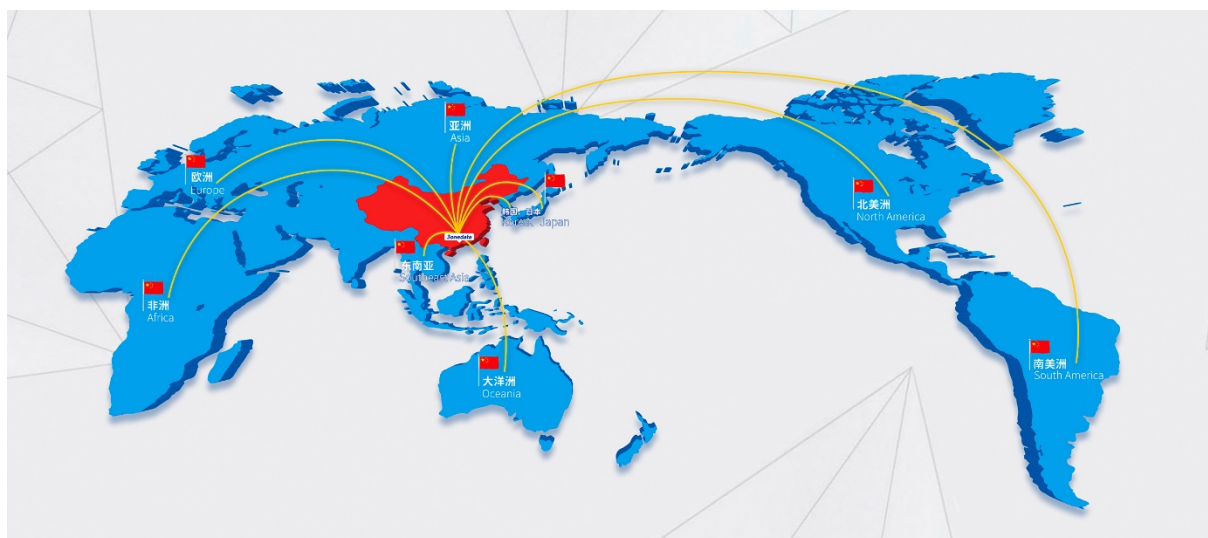
Description

Delete current configuration file.

Instance

```
Switch> enable
```

```
Switch#erase startup-config  
erase startup-config ? (y/n): y  
Switch#reboot
```



3onedata Co., Ltd.

Headquarter address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen

Technology support: tech-support@3onedata.com

Service hotline: +86-400-880-4496

Official Website: <http://www.3onedata.com>