



Зелакс ZES

Справочник команд

ZES-20xx

ZES-21xx

ZES-30xx

Декларация о соответствии: Д-СПД-2592

© 1998 — 2011 Zelax. Все права защищены.

Редакция 02 от 13.09.2011 г.
ПО 6.1.72.28

Россия, 124681 Москва, г. Зеленоград, ул. Заводская, дом 1Б, строение 2
Телефон: +7 (495) 748-71-78 (многоканальный) <http://www.zelax.ru>
Отдел технической поддержки: tech@zelax.ru Отдел продаж: sales@zelax.ru

Оглавление

1	Базовая настройка коммутатора.....	16
1.1	Команды базовой настройки коммутатора.....	16
1.1.1	authentication line.....	16
1.1.2	banner.....	17
1.1.3	clock set.....	17
1.1.4	config.....	17
1.1.5	debug ssh-server.....	17
1.1.6	enable.....	18
1.1.7	enable password.....	18
1.1.8	end.....	18
1.1.9	exec-timeout.....	18
1.1.10	exit.....	19
1.1.11	help.....	19
1.1.12	hostname.....	19
1.1.13	ip host.....	20
1.1.14	ipv6 host.....	20
1.1.15	ip http server.....	21
1.1.16	login.....	21
1.1.17	password.....	21
1.1.18	reload.....	21
1.1.19	service password-encryption.....	21
1.1.20	service terminal-length.....	22
1.1.21	set default.....	22
1.1.22	setup.....	22
1.1.23	show clock.....	23
1.1.24	show cpu usage.....	23
1.1.25	show memory usage.....	23
1.1.26	show tech-support.....	23
1.1.27	show version.....	24
1.1.28	sysContact.....	24
1.1.29	sysLocation.....	24
1.1.30	username.....	24
1.1.31	write.....	25
1.2	Команды Telnet и SSH.....	25
1.2.1	authentication ip access-class.....	25
1.2.2	authentication ipv6 access-class.....	26
1.2.3	authentication line login.....	26
1.2.4	authentication securityip.....	27
1.2.5	authentication securityipv6.....	27
1.2.6	authorization.....	27
1.2.7	terminal length.....	28
1.2.8	terminal monitor.....	28
1.2.9	telnet.....	29
1.2.10	telnet-server enable.....	29
1.2.11	telnet-server max-connection.....	29
1.2.12	ssh-server authentication-retries.....	30
1.2.13	ssh-server enable.....	30
1.2.14	ssh-server host-key create rsa.....	30
1.2.15	ssh-server max-connection.....	31
1.2.16	ssh-server timeout.....	31
1.2.17	show ssh-server.....	31
1.2.18	show telnet login.....	31
1.3	Команды для настройки IP-адресов коммутатора.....	32
1.3.1	interface vlan.....	32
1.3.2	ip address.....	32
1.3.3	ipv6 address.....	32
1.3.4	ip bootp-client enable.....	33
1.3.5	ip dhcp-client enable.....	33
1.4	Команды для настройки протокола SNMP.....	34
1.4.1	debug snmp mib.....	34

1.4.2	debug snmp kernel.....	34
1.4.3	rmon enable	34
1.4.4	show private-mib oid	34
1.4.5	show snmp	35
1.4.6	show snmp engineid	36
1.4.7	show snmp group.....	36
1.4.8	show snmp mib	36
1.4.9	show snmp status	36
1.4.10	show snmp user	37
1.4.11	show snmp view.....	37
1.4.12	snmp-server community.....	38
1.4.13	snmp-server enable	38
1.4.14	snmp-server enable traps	38
1.4.15	snmp-server engineid.....	39
1.4.16	snmp-server group.....	39
1.4.17	snmp-server host	39
1.4.18	snmp-server securityip	40
1.4.19	snmp-server securityip enable	40
1.4.20	snmp-server trap-source.....	41
1.4.21	snmp-server view	41
1.4.22	snmp-server user	41
1.5	Команды для обновления ПО коммутатора	42
1.5.1	copy (FTP)	42
1.5.2	copy (TFTP)	43
1.5.3	ftp-dir	43
1.5.4	ftp-server enable	44
1.5.5	ftp-server timeout	44
1.5.6	ip ftp.....	44
1.5.7	show ftp.....	45
1.5.8	show tftp.....	45
1.5.9	tftp-server enable	45
1.5.10	tftp-server retransmission-number	45
1.5.11	tftp-server transmission-timeout.....	45
2	Команды для настройки стекирования	47
2.1.1	clear cluster nodes	47
2.1.2	cluster auto-add	47
2.1.3	cluster commander.....	47
2.1.4	cluster ip-pool.....	48
2.1.5	cluster keepalive interval.....	48
2.1.6	cluster keepalive loss-count.....	49
2.1.7	cluster member	49
2.1.8	cluster member auto-to-user	50
2.1.9	cluster reset member	50
2.1.10	cluster run	51
2.1.11	cluster update member	51
2.1.12	debug cluster.....	52
2.1.13	debug cluster packets	52
2.1.14	show cluster	52
2.1.15	show cluster members	53
2.1.16	show cluster candidates.....	53
2.1.17	show cluster topology.....	54
2.1.18	rcommand commander	54
2.1.19	rcommand member	55
3	Команды для настройки портов.....	56
3.1	Команды для настройки Ethernet-порта.....	56
3.1.1	bandwidth.....	56
3.1.2	clear counters interface.....	56
3.1.3	flow control	56
3.1.4	interface ethernet	57
3.1.5	loopback.....	57
3.1.6	mdi.....	57
3.1.7	name	58
3.1.8	negotiation.....	58

3.1.9	port-rate-statistics interval	58
3.1.10	port-scan-mode.....	59
3.1.11	rate-suppression	59
3.1.12	rate-violation	60
3.1.13	rate-violation control	60
3.1.14	show interface.....	60
3.1.15	shutdown	61
3.1.16	speed-duplex	62
3.1.17	combo-forced-mode.....	63
3.1.18	virtual-cable-test	63
3.2	Команды для настройки изоляции портов	64
3.2.1	isolate-port group.....	64
3.2.2	isolate-port group switchport interface.....	64
3.2.3	show isolate-port group	65
3.3	Команды для настройки обнаружения петель в портах	65
3.3.1	loopback-detection control.....	65
3.3.2	loopback-detection specified-vlan	66
3.3.3	loopback-detection interval-time.....	66
3.3.4	loopback-detection control-recovery timeout.....	67
3.3.5	show loopback-detection	67
3.3.6	debug loopback-detection	68
3.4	Команды для настройки функции ULDP	68
3.4.1	uldp enable	68
3.4.2	uldp disable.....	68
3.4.3	uldp hello-interval.....	68
3.4.4	uldp aggressive-mode	69
3.4.5	uldp manual-shutdown	69
3.4.6	uldp reset	69
3.4.7	uldp recovery-time	70
3.4.8	show uldp.....	70
3.4.9	debug uldp fsm interface ethernet	70
3.4.10	debug uldp error	71
3.4.11	debug uldp event	71
3.4.12	debug uldp packet	71
3.4.13	debug uldp	72
3.5	Команды для настройки LLDP	73
3.5.1	lldp enable	73
3.5.2	lldp enable (port).....	73
3.5.3	lldp mode	73
3.5.4	lldp tx-interval.....	74
3.5.5	lldp msgTxHold	74
3.5.6	lldp transmit delay.....	74
3.5.7	lldp notification interval	75
3.5.8	lldp trap	75
3.5.9	lldp transmit optional tlv	75
3.5.10	lldp neighbors max-num	76
3.5.11	lldp tooManyNeighbors.....	76
3.5.12	show lldp.....	76
3.5.13	show lldp traffic	77
3.5.14	show lldp interface ethernet.....	77
3.5.15	show lldp neighbors interface ethernet.....	77
3.5.16	show debugging lldp	78
3.5.17	debug lldp	78
3.5.18	debug lldp packets.....	79
3.5.19	clear lldp remote-table	79
4	Команды для настройки Port Channel.....	80
4.1.1	debug port-channel.....	80
4.1.2	interface port-channel	80
4.1.3	lACP port-priority	80
4.1.4	lACP system-priority.....	80
4.1.5	lACP timeout	81
4.1.6	load-balance	81
4.1.7	port-group	81

4.1.8	port-group mode.....	81
4.1.9	show port-group	82
5	Команды для настройки работы с Jumbo-кадрами.....	84
5.1.1	jumbo enable.....	84
6	Настройка VLAN.....	85
6.1	Команды для настройки VLAN.....	85
6.1.1	debug gvrp	85
6.1.2	dot1q-tunnel enable	85
6.1.3	dot1q-tunnel tpid	85
6.1.4	gvrp	86
6.1.5	garp timer hold	86
6.1.6	garp timer join	86
6.1.7	garp timer leave	87
6.1.8	garp timer leaveall.....	87
6.1.9	name	87
6.1.10	private-vlan.....	88
6.1.11	private-vlan association.....	88
6.1.12	show dot1q-tunnel.....	89
6.1.13	show garp.....	89
6.1.14	show gvrp.....	89
6.1.15	show vlan	89
6.1.16	show vlan-translation	90
6.1.17	switchport dot1q-tunnel.....	90
6.1.18	switchport access vlan	91
6.1.19	switchport hybrid allowed vlan	91
6.1.20	switchport hybrid native vlan.....	92
6.1.21	switchport interface	92
6.1.22	switchport mode.....	92
6.1.23	switchport trunk allowed vlan	93
6.1.24	switchport trunk native vlan.....	93
6.1.25	vlan.....	94
6.1.26	vlan-translation.....	94
6.1.27	vlan-translation enable.....	94
6.1.28	vlan-translation miss drop	95
6.1.29	vlan ingress enable	95
6.2	Команды для настройки динамических VLAN	96
6.2.1	protocol-vlan mode.....	96
6.2.2	show protocol-vlan	96
7	Команды для настройки selective QinQ.....	97
7.1.1	match	97
7.1.2	service-policy	97
7.1.3	set.....	97
8	Команды для работы с таблицей MAC-адресов.....	99
8.1	Команды для настройки таблицы MAC-адресов.....	99
8.1.1	clear mac-address-table dynamic.....	99
8.1.2	mac-address-table aging-time	99
8.1.3	mac-address-table static blackhole.....	99
8.1.4	show mac-address-table.....	100
8.2	Команды для настройки привязки MAC-адресов.....	100
8.2.1	clear port-security dynamic.....	100
8.2.2	show port-security.....	101
8.2.3	show port-security address	101
8.2.4	show port-security interface	102
8.2.5	switchport port-security	102
8.2.6	switchport port-security convert	103
8.2.7	switchport port-security lock.....	103
8.2.8	switchport port-security mac-address	103
8.2.9	switchport port-security maximum	103
8.2.10	switchport port-security timeout	104
8.2.11	switchport port-security violation.....	104
9	Команды для настройки протокола MSTP.....	105
9.1	Команды работы с протоколом MSTP.....	105
9.1.1	show	105

9.1.2	abort.....	105
9.1.3	exit	105
9.1.4	instance vlan	105
9.1.5	name	106
9.1.6	no	106
9.1.7	revision-level	107
9.1.8	spanning-tree.....	107
9.1.9	spanning-tree forward-time.....	107
9.1.10	spanning-tree hello-time	108
9.1.11	spanning-tree cost	108
9.1.12	spanning-tree link-type p2p	109
9.1.13	spanning-tree maxage	109
9.1.14	spanning-tree max-hop.....	109
9.1.15	spanning-tree mcheck	110
9.1.16	spanning-tree mode.....	110
9.1.17	spanning-tree mst configuration	110
9.1.18	spanning-tree mst cost	111
9.1.19	spanning-tree mst loopguard	111
9.1.20	spanning-tree mst port-priority.....	112
9.1.21	spanning-tree mst priority	112
9.1.22	spanning-tree mst rootguard	112
9.1.23	spanning-tree port-priority	113
9.1.24	spanning-tree rootguard	113
9.1.25	spanning-tree portfast.....	114
9.1.26	spanning-tree priority	114
9.1.27	spanning-tree format.....	114
9.1.28	spanning-tree digest-snooping	115
9.1.29	spanning-tree tcf flush (глобальный режим конфигурирования).....	115
9.1.30	spanning-tree tcf flush (режим настройки интерфейсов)	116
9.2	Команды мониторинга и отладки MSTP	117
9.2.1	show spanning-tree	117
9.2.2	show spanning-tree mst config.....	118
9.2.3	show mst-pending.....	118
9.2.4	debug spanning-tree.....	119
10	Команды для настройки качества обслуживания (QoS)	120
10.1.1	class.....	120
10.1.2	class-map	120
10.1.3	match	120
10.1.4	mls qos	121
10.1.5	mls qos cos.....	121
10.1.6	mls qos aggregate-policy.....	122
10.1.7	mls qos trust	122
10.1.8	mls qos dscp-mutation.....	123
10.1.9	mls qos map	123
10.1.10	policy.....	125
10.1.11	policy aggregate	125
10.1.12	policy-map	126
10.1.13	priority-queue out.....	126
10.1.14	set	126
10.1.15	service-policy	127
10.1.16	show class-map	127
10.1.17	show policy-map.....	128
10.1.18	show mls qos aggregate-policy	128
10.1.19	show mls qos interface	128
10.1.20	show mls qos maps	129
10.1.21	show mls-qos.....	130
10.1.22	wrr-queue cos-map.....	130
11	Команды для настройки перенаправления на основе потоков.....	132
11.1.1	access-group redirect to interface ethernet.....	132
11.1.2	show flow-based-redirect.....	132
12	Команды для настройки управления уровня 3	133
12.1	Команды для настройки интерфейса уровня 3	133
12.1.1	shutdown	133

12.1.2	interface vlan	133
12.2	Команды для настройки протоколов IPv4/v6	133
12.2.1	clear ipv6 neighbor	133
12.2.2	debug ip packet	134
12.2.3	debug ipv6 packet	134
12.2.4	debug ipv6 icmp	134
12.2.5	debug ipv6 nd	135
12.2.6	ip address	135
12.2.7	ip default-gateway	136
12.2.8	ipv6 address	136
12.2.9	ipv6 default-gateway	136
12.2.10	ipv6 nd dad attempts	137
12.2.11	ipv6 nd ns-interval	137
12.2.12	ipv6 neighbor	137
12.2.13	show ip interface	138
12.2.14	show ip traffic	138
12.2.15	show ipv6 interface	139
12.2.16	show ipv6 route	140
12.2.17	show ipv6 neighbors	141
12.2.18	show ipv6 traffic	141
12.3	Команды для настройки ARP	142
12.3.1	arp	142
12.3.2	clear arp-cache	142
12.3.3	clear arp traffic	143
12.3.4	debug arp	143
12.3.5	show arp	143
12.3.6	show arp traffic	144
12.4	Команды для настройки защиты от ARP-сканирования	144
12.4.1	anti-arpscan enable	144
12.4.2	anti-arpscan port-based threshold	145
12.4.3	anti-arpscan ip-based threshold	145
12.4.4	anti-arpscan trust	146
12.4.5	anti-arpscan trust ip	146
12.4.6	anti-arpscan recovery enable	146
12.4.7	anti-arpscan recovery time	147
12.4.8	anti-arpscan log enable	147
12.4.9	anti-arpscan trap enable	147
12.4.10	show anti-arpscan	148
12.4.11	debug anti-arpscan	148
12.5	Команды для настройки защиты от подмены протоколов (ARP, ND spoofing)	149
12.5.1	ip arp-security updateprotect	149
12.5.2	ipv6 nd-security updateprotect	149
12.5.3	ip arp-security learnprotect	150
12.5.4	ipv6 nd-security learnprotect	150
12.5.5	ip arp-security convert	150
12.5.6	ipv6 nd-security convert	151
12.5.7	clear ip arp dynamic	151
12.5.8	clear ipv6 nd dynamic	151
12.6	Команды для настройки защиты ARP (ARP Guard)	151
12.6.1	arp-guard ip	151
12.7	Команды для настройки самообращенных запросов (Gratuitous ARP)	152
12.7.1	ip gratuitous-arp	152
12.7.2	show ip gratuitous-arp	152
12.8	Команды для настройки ND snooping	153
12.8.1	clear ipv6 nd snooping binding	153
12.8.2	debug ipv6 nd snooping	153
12.8.3	Ipv6 nd snooping enable (Глобальный режим)	153
12.8.4	ipv6 nd snooping mac-binding-limit	153
12.8.5	ipv6 nd snooping max-dad-delay	154
12.8.6	ipv6 nd snooping max-dad-prepare-delay	154
12.8.7	ipv6 nd snooping max-sac-lifetime	154
12.8.8	ipv6 nd snooping policy	155
12.8.9	ipv6 nd snooping port-binding-limit	155

12.8.10	ipv6 nd snooping static-binding	155
12.8.11	ipv6 nd snooping trust	156
12.8.12	ipv6 nd snooping user-control	156
12.8.13	show ipv6 nd snooping binding	156
13	Команды для настройки протокола DHCP	158
13.1	Команды для настройки DHCP-сервера	158
13.1.1	bootfile	158
13.1.2	clear ip dhcp binding	158
13.1.3	clear ip dhcp conflict	158
13.1.4	clear ip dhcp server statistics	159
13.1.5	client-identifier	159
13.1.6	debug ip dhcp server	160
13.1.7	default-router	160
13.1.8	dns-server	160
13.1.9	domain-name	160
13.1.10	hardware-address	161
13.1.11	host	161
13.1.12	ip dhcp conflict logging	162
13.1.13	ip dhcp excluded-address	162
13.1.14	ip dhcp pool	162
13.1.15	ip dhcp conflict ping-detection enable	163
13.1.16	ip dhcp ping packets	163
13.1.17	ip dhcp ping timeout	164
13.1.18	lease	164
13.1.19	netbios-name-server	164
13.1.20	netbios-node-type	165
13.1.21	network-address	165
13.1.22	next-server	165
13.1.23	option	166
13.1.24	service dhcp	166
13.1.25	show ip dhcp binding	166
13.1.26	show ip dhcp conflict	167
13.1.27	show ip dhcp server statistics	167
13.2	Команды для настройки DHCP Relay	168
13.2.1	ip forward-protocol udp bootps	168
13.2.2	ip helper-address	168
13.3	Команды для настройки DHCPv6	169
13.3.1	clear ipv6 dhcp binding	169
13.3.2	clear ipv6 dhcp server statistics	169
13.3.3	debug ipv6 dhcp client packet	169
13.3.4	debug ipv6 dhcp detail	170
13.3.5	debug ipv6 dhcp detail	170
13.3.6	debug ipv6 dhcp server	170
13.3.7	dns-server	170
13.3.8	domain-name	170
13.3.9	excluded-address	171
13.3.10	ipv6 address	171
13.3.11	ipv6 dhcp client pd	171
13.3.12	ipv6 dhcp client pd hint	172
13.3.13	ipv6 dhcp pool	172
13.3.14	ipv6 dhcp relay destination	172
13.3.15	ipv6 dhcp server	172
13.3.16	ipv6 general-prefix	173
13.3.17	ipv6 local pool	173
13.3.18	lifetime	173
13.3.19	network-address	174
13.3.20	prefix-delegation	174
13.3.21	prefix-delegation pool	174
13.3.22	service dhcpv6	175
13.3.23	show ipv6 dhcp	175
13.3.24	show ipv6 dhcp binding	175
13.3.25	show ipv6 dhcp interface	176
13.3.26	show ipv6 dhcp local pool	176

13.3.27	show ipv6 dhcp pool.....	176
13.3.28	show ipv6 dhcp statistics	176
13.3.29	show ipv6 general-prefix	177
13.4	Команды для настройки протокола DHCP Snooping	177
13.4.1	debug ip dhcp snooping packet interface	177
13.4.2	debug ip dhcp snooping packet	177
13.4.3	debug ip dhcp snooping update	178
13.4.4	debug ip dhcp snooping event	178
13.4.5	debug ip dhcp snooping binding	178
13.4.6	ip dhcp snooping	178
13.4.7	ip dhcp snooping binding	179
13.4.8	ip dhcp snooping binding user	179
13.4.9	ip dhcp snooping binding arp	179
13.4.10	ip dhcp snooping binding dot1x	180
13.4.11	ip dhcp snooping binding user-control	180
13.4.12	ip dhcp snooping binding user-control max-user	181
13.4.13	ip dhcp snooping trust	181
13.4.14	ip dhcp snooping action	182
13.4.15	ip dhcp snooping action MaxNum	182
13.4.16	ip dhcp snooping limit-rate	182
13.4.17	ip dhcp snooping information enable	183
13.4.18	ip dhcp snooping information option	183
13.4.19	enable trustview key.....	184
13.4.20	ip user private packet version two.....	184
13.4.21	ip user helper-address	185
13.4.22	show trustview status	185
13.4.23	show ip dhcp snooping.....	186
13.4.24	show ip dhcp snooping binding all	188
14	Настройка Multicast-протокола IPv4	189
14.1	Команды настройки фильтров доступа (DCSCM).....	189
14.1.1	access-list (управление multicast-назначением).....	189
14.1.2	access-list (управление multicast-источником)	189
14.1.3	ip multicast destination-control.....	190
14.1.4	ip multicast destination-control access-group	190
14.1.5	ip multicast destination-control access-group (sip).....	191
14.1.6	ip multicast destination-control access-group (vmac).....	191
14.1.7	ip multicast policy	192
14.1.8	ip multicast source-control	192
14.1.9	ip multicast source-control access-group.....	192
14.1.10	multicast destination-control	193
14.1.11	show ip multicast destination-control	193
14.1.12	show ip multicast destination-control access-list	194
14.1.13	show ip multicast policy.....	194
14.1.14	show ip multicast source-control	194
14.1.15	show ip multicast source-control access-list.....	195
14.2	Команды настройки IGMP Snooping.....	195
14.2.1	clear ip igmp snooping vlan	195
14.2.2	clear ip igmp snooping vlan <1-4094> mrouter-port	195
14.2.3	debug igmp snooping {all packet event timer mfc}	196
14.2.4	ip igmp snooping	196
14.2.5	ip igmp snooping vlan	196
14.2.6	ip igmp snooping vlan immediate-leave	196
14.2.7	ip igmp snooping vlan l2-general-querier.....	197
14.2.8	ip igmp snooping vlan l2-general-querier-source.....	197
14.2.9	ip igmp snooping vlan l2-general-querier-version	197
14.2.10	ip igmp snooping vlan limit.....	198
14.2.11	ip igmp snooping vlan mrouter-port interface	198
14.2.12	ip igmp snooping vlan mrpt	199
14.2.13	ip igmp snooping vlan report source-address.....	199
14.2.14	ip igmp snooping vlan static-group	199
14.2.15	ip igmp snooping vlan query-interval	199
14.2.16	ip igmp snooping vlan query-mrsp	200
14.2.17	ip igmp snooping vlan query-robustness	200

14.2.18	ip igmp snooping vlan suppression-query-time	200
14.2.19	show ip igmp snooping	201
15	Настройка Multicast-протокола IPv6	203
15.1	Команды настройки DCSCM протокола IPv6	203
15.1.1	ipv6 access-list (управление multicast-источником с ipv6-адресом)	203
15.1.2	ipv6 access-list (управление назначением multicast-трафика)	203
15.1.3	ipv6 multicast destination-control access-group	204
15.1.4	ipv6 multicast destination-control access-group (sip)	204
15.1.5	ipv6 multicast destination-control access-group (vmas)	205
15.1.6	ipv6 multicast policy	205
15.1.7	ipv6 multicast source-control	205
15.1.8	ipv6 multicast source-control access-group	206
15.1.9	multicast destination-control	206
15.1.10	show ipv6 multicast destination-control	207
15.1.11	show ipv6 multicast destination-control access-list	207
15.1.12	show ipv6 multicast policy	208
15.1.13	show ipv6 multicast source-control	208
15.1.14	show ipv6 multicast source-control access-list	208
15.2	Команды для настройки MLD Snooping	209
15.2.1	clear ipv6 mld snooping vlan	209
15.2.2	clear ipv6 mld snooping vlan <1-4094> mrouter-port	209
15.2.3	debug mld snooping {all packet event timer mfc}	209
15.2.4	ipv6 mld snooping	209
15.2.5	ipv6 mld snooping vlan	210
15.2.6	ipv6 mld snooping vlan immediate-leave	210
15.2.7	ipv6 mld snooping vlan l2-general-querier	210
15.2.8	ipv6 mld snooping vlan limit	211
15.2.9	ipv6 mld snooping vlan mrouter-port interface	211
15.2.10	ipv6 mld snooping vlan mrpt	211
15.2.11	ipv6 mld snooping vlan query-interval	212
15.2.12	ipv6 mld snooping vlan query-mrsp	212
15.2.13	ipv6 mld snooping vlan query-robustness	212
15.2.14	ipv6 mld snooping vlan static-group	213
15.2.15	ipv6 mld snooping vlan suppression-query-time	213
15.2.16	show ipv6 mld snooping	214
16	Команды для настройки групповой VLAN (multicast vlan)	216
16.1.1	multicast-vlan	216
16.1.2	multicast-vlan association	216
17	Команды для настройки списков доступа (ACL)	217
17.1.1	absolute-periodic/periodic	217
17.1.2	absolute start	217
17.1.3	access-list (ip extended)	218
17.1.4	access-list (ip standard)	219
17.1.5	access-list (mac extended)	219
17.1.6	access-list (mac-ip extended)	220
17.1.7	access-list (mac standard)	222
17.1.8	clear access-group statistic	222
17.1.9	firewall	222
17.1.10	firewall default	223
17.1.11	ip access extended	223
17.1.12	ip access standard	223
17.1.13	ipv6 access-list	224
17.1.14	ipv6 access-list standard	225
17.1.15	ipv6 access-list extended	225
17.1.16	{ip ipv6 mac mac-ip} access-group	225
17.1.17	mac access extended	226
17.1.18	mac-ip access extended	226
17.1.19	permit deny (ip extended)	226
17.1.20	permit deny (ip standard)	227
17.1.21	permit deny (ipv6 extended)	228
17.1.22	permit deny (ipv6 standard)	229
17.1.23	permit deny (mac extended)	229
17.1.24	permit deny (mac-ip extended)	230

17.1.25	show access-lists	232
17.1.26	show access-group	232
17.1.27	show firewall.....	233
17.1.28	show ipv6 access-lists.....	233
17.1.29	show time-range.....	234
17.1.30	time-range	234
18	Команды для настройки 802.1x	235
18.1.1	debug dot1x detail.....	235
18.1.2	debug dot1x error.....	235
18.1.3	debug dot1x fsm.....	235
18.1.4	debug dot1x packet.....	236
18.1.5	dot1x accept-mac.....	236
18.1.6	dot1x eapw enable	237
18.1.7	dot1x enable.....	237
18.1.8	user-control limit.....	237
18.1.9	dot1x guest-vlan.....	238
18.1.10	dot1x macfilter enable	238
18.1.11	dot1x max-req	239
18.1.12	dot1x user free-resource.....	239
18.1.13	dot1x max-user macbased.....	239
18.1.14	dot1x max-user userbased	240
18.1.15	dot1x port-control	240
18.1.16	dot1x port-method.....	240
18.1.17	dot1x privateclient enable	241
18.1.18	dot1x re-authenticate	242
18.1.19	dot1x re-authentication.....	242
18.1.20	dot1x timeout quiet-period	242
18.1.21	dot1x timeout re-authperiod	242
18.1.22	dot1x timeout tx-period	243
18.1.23	dot1x unicast enable	243
18.1.24	show dot1x	243
19	Команды для настройки управления доступом (AM).....	245
19.1.1	am enable	245
19.1.2	am port.....	245
19.1.3	am ip-pool	245
19.1.4	am mac-ip-pool	246
19.1.5	no am all.....	246
19.1.6	show am.....	246
20	Команды для настройки протокола TACACS+	247
20.1.1	tacacs-server authentication host	247
20.1.2	tacacs-server key	247
20.1.3	tacacs-server nas-ipv4.....	247
20.1.4	tacacs-server timeout.....	248
20.1.5	debug tacacs-server.....	248
21	Команды для настройки протокола RADIUS	249
21.1.1	aaa enable	249
21.1.2	aaa-accounting enable.....	249
21.1.3	aaa-accounting update.....	249
21.1.4	debug aaa packet.....	250
21.1.5	debug aaa detail attribute	250
21.1.6	debug aaa detail connection	250
21.1.7	debug aaa detail event.....	251
21.1.8	debug aaa error.....	251
21.1.9	radius nas-ipv4.....	251
21.1.10	radius nas-ipv6.....	252
21.1.11	radius-server accounting host.....	252
21.1.12	radius-server authentication host.....	253
21.1.13	radius-server dead-time	253
21.1.14	radius-server key.....	254
21.1.15	radius-server retransmit	254
21.1.16	radius-server timeout	254
21.1.17	radius-server accounting-interim-update timeout	255
21.1.18	show aaa authenticated-user	255

21.1.19	show aaa authenticating-user.....	256
21.1.20	show aaa config.....	256
21.1.21	show radius count.....	256
22	Команды для настройки функции RA Security протокола IPv6.....	257
22.1.1	ipv6 security-ra enable.....	257
22.1.2	show ipv6 security-ra.....	257
22.1.3	debug ipv6 security-ra.....	257
23	Команды для настройки MAB.....	258
23.1.1	clear mac-authentication-bypass binding.....	258
23.1.2	debug mac-authentication-bypass.....	258
23.1.3	mac-authentication-bypass binding-limit.....	258
23.1.4	mac-authentication-bypass.....	258
23.1.5	mac-authentication-bypass guest-vlan.....	259
23.1.6	mac-authentication-bypass timeout linkup-period.....	259
23.1.7	mac-authentication-bypass timeout offline-detect.....	259
23.1.8	mac-authentication-bypass timeout quiet-period.....	259
23.1.9	mac-authentication-bypass timeout reauth-period.....	260
23.1.10	mac-authentication-bypass timeout stale-period.....	260
23.1.11	mac-authentication-bypass username-format.....	260
23.1.12	show mac-authentication-bypass.....	261
24	Команды для настройки MRPP.....	262
24.1.1	control-vlan.....	262
24.1.2	clear mrpp statistics.....	262
24.1.3	debug mrpp.....	262
24.1.4	enable.....	263
24.1.5	fail-timer.....	263
24.1.6	hello-timer.....	263
24.1.7	mrpp enable.....	264
24.1.8	mrpp poll-time.....	264
24.1.9	mrpp ring.....	264
24.1.10	mrpp ring primary-port.....	264
24.1.11	mrpp ring secondary-port.....	265
24.1.12	node-mode.....	265
24.1.13	show mrpp.....	265
24.1.14	show mrpp statistics.....	266
25	Команды для настройки ULPP.....	267
25.1.1	clear ulpp flush counter interface.....	267
25.1.2	control-vlan.....	267
25.1.3	debug ulpp error.....	267
25.1.4	debug ulpp event.....	267
25.1.5	debug ulpp flush content interface.....	268
25.1.6	debug ulpp flush {send receive} interface.....	268
25.1.7	description.....	268
25.1.8	flush disable arp.....	268
25.1.9	flush disable mac.....	269
25.1.10	flush enable arp.....	269
25.1.11	flush enable mac.....	269
25.1.12	preemption delay.....	269
25.1.13	preemption mode.....	270
25.1.14	protect vlan-reference-instance.....	270
25.1.15	show ulpp flush counter interface.....	270
25.1.16	show ulpp flush-receive-port.....	271
25.1.17	show ulpp group.....	271
25.1.18	ulpp control vlan.....	271
25.1.19	ulpp flush disable arp.....	271
25.1.20	ulpp flush disable mac.....	272
25.1.21	ulpp flush enable arp.....	272
25.1.22	ulpp flush enable mac.....	272
25.1.23	ulpp group.....	272
25.1.24	ulpp group master.....	273
25.1.25	ulpp group slave.....	273
26	Команды для настройки ULSP.....	274
26.1.1	debug ulsm event.....	274

26.1.2	show ulsm group	274
26.1.3	ulsm group	274
26.1.4	ulsm group {uplink downlink}	274
27	Команды для настройки PPPoE Intermediate Agent	276
27.1.1	debug pppoe-ia	276
27.1.2	pppoe intermediate-agent	276
27.1.3	pppoe intermediate-agent (для порта)	276
27.1.4	pppoe intermediate-agent access-node-id	276
27.1.5	pppoe intermediate-agent circuit-id	277
27.1.6	pppoe intermediate-agent identifier-string option delimiter	277
27.1.7	pppoe intermediate-agent trust	278
27.1.8	pppoe intermediate-agent vendor-tag strip	278
27.1.9	show pppoe intermediate-agent access-node-id	278
27.1.10	show pppoe intermediate-agent identifier-string option delimiter	278
27.1.11	show pppoe intermediate-agent info	279
28	Команды для настройки зеркалирования портов	280
28.1.1	monitor session source interface	280
28.1.2	monitor session source interface access-list	280
28.1.3	monitor session destination interface	281
28.1.4	show monitor	281
29	Команды для настройки SNTP	282
29.1.1	debug sntp	282
29.1.2	snmp server	282
29.1.3	snmp polltime	282
29.1.4	snmp timezone	282
29.1.5	show snmp	283
30	Команды для настройки NTP	284
30.1.1	ntp enable	284
30.1.2	ntp server	284
30.1.3	ntp broadcast server count	284
30.1.4	ntp timezone	285
30.1.5	ntp access-group	285
30.1.6	ntp authenticate	285
30.1.7	ntp authentication-key	285
30.1.8	ntp trusted-key	286
30.1.9	ntp disable	286
30.1.10	debug ntp authentication	286
30.1.11	debug ntp packet	286
30.1.12	debug ntp adjust	287
30.1.13	debug ntp sync	287
30.1.14	debug ntp events	287
30.1.15	show ntp status	288
30.1.16	show ntp session	288
31	Команды для настройки перехода на летнее/зимнее время	289
31.1.1	clock summer-time absolute	289
31.1.2	clock summer-time recurring	289
31.1.3	clock summer-time recurring	289
32	Команды для диагностики и контроля состояния устройства	291
32.1.1	clear logging	291
32.1.2	logging	291
32.1.3	logging loghost sequence-number	291
32.1.4	logging executed-commands	292
32.1.5	ping	292
32.1.6	ping6	293
32.1.7	show debugging	294
32.1.8	show flash	294
32.1.9	show history	295
32.1.10	show logging buffered	295
32.1.11	show logging source mstp	295
32.1.12	show memory	296
32.1.13	show running-config	296
32.1.14	show startup-config	296
32.1.15	show switchport interface	296

32.1.16	show tcp.....	297
32.1.17	show tcp ipv6.....	297
32.1.18	show telnet login.....	298
32.1.19	show tech-support.....	298
32.1.20	show udp.....	298
32.1.21	show udp ipv6.....	298
32.1.22	show version.....	299
32.1.23	traceroute.....	299
32.1.24	traceroute6.....	300
33	Перезагрузка коммутатора по истечении заданного времени.....	301
33.1.1	reload after.....	301
33.1.2	reload cancel.....	301
33.1.3	show reload.....	301
34	Команды для отладки и диагностики пакетов, принятых и посланных CPU.....	303
34.1.1	cpu-rx-ratelimit enhanced.....	303
34.1.2	cpu-rx-ratelimit total.....	303
34.1.3	cpu-rx-ratelimit protocol.....	303
34.1.4	clear cpu-rx-stat protocol.....	304
34.1.5	debug driver.....	304
34.1.6	show cpu-rx protocol.....	304
35	Команды для работы с PoE.....	306
35.1	Команды для настройка PoE.....	306
35.1.1	power inline enable (глобальный режим конфигурирования).....	306
35.1.2	power inline max (глобальный режим конфигурирования).....	306
35.1.3	power inline police.....	306
35.1.4	power inline legacy.....	307
35.1.5	power inline enable (режим настройки интерфейсов).....	307
35.1.6	power inline max (режим настройки интерфейсов).....	308
35.1.7	power inline priority.....	308
35.2	Команды для мониторинга и отладки PoE.....	308
35.2.1	show power inline.....	308
35.2.2	show power inline interface ethernet.....	309
35.2.3	debug power inline.....	310

1 Базовая настройка коммутатора

1.1 Команды базовой настройки коммутатора

1.1.1 authentication line

Синтаксис: `authentication line {console | vty | web} login {local | radius | tacacs}`
`no authentication line {console | vty | web} login`

Назначение: Позволяет сконфигурировать VTY (параметры для инициации сеанса Telnet и SSH), Web и Console, задать приоритет режима аутентификации при регистрации пользователей.

Значение по умолчанию: Настройка для метода входа с консоли не задана. По умолчанию для методов входа VTY и через Web-интерфейс включена локальная аутентификация.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Для методов регистрации пользователей на коммутаторе с порта Console, VTY и посредством Web-интерфейса может быть задан метод аутентификации. Может быть выбрана локальная аутентификация, аутентификация по протоколам RADIUS, TACACS, либо любая комбинация этих трех методов аутентификации. Если задана комбинация методов аутентификации, выбор предпочтительного метода выполняется слева направо. Если пользователь прошел аутентификацию по некоторому методу, следующие, менее предпочтительные методы аутентификации, игнорируются. Если пользователь получил ответ от соответствующего протокола (о том, что он допущен или отвергнут), то не будет предпринято попытки применения следующего метода (исключение из этого правила: если локальная аутентификация была безуспешна, будет предпринята попытка применить следующий метод аутентификации). Если ответ от протокола аутентификации не получен, будет предпринята попытка использовать следующий метод аутентификации. Для того, чтобы можно было использовать метод RADIUS, предварительно должны быть сконфигурированы функции AAA RADIUS-сервера. Для того, чтобы можно было использовать метод TACACS, предварительно должен быть сконфигурирован TACACS-сервер.

Команда **authentication line console login** используется только с командой **login**. Команда **authentication line console login** устанавливает на коммутаторе использование метода регистрации с порта Console. Команда **login** позволяет при регистрации с порта Console использовать пароли, заданные командой **password** для аутентификации.

Если задана локальная аутентификация, но локальных пользователей не сконфигурировано, то пользователи могут воспользоваться регистрацией на коммутаторе через порт Console.

Пример: Настроить регистрацию по Telnet и SSH с использованием метода аутентификации по протоколу RADIUS.

```
Switch(config)#authentication line vty login local radius
```

См. также:

Команда	Описание
aaa enable	Включает функцию аутентификации AAA на коммутаторе.
radius-server authentication host	Позволяет задать IP-адрес RADIUS-сервера, номер порта прослушивания, секретный ключ, является ли сервер первичным или нет, режим доступа
tacacs-server authentication host	Позволяет задать IP-адрес, номер порта прослушивания, значение таймера и строку ключа сервера TACACS+
tacacs-server key	Позволяет задать ключ сервера TACACS+

1.1.2 banner

Синтаксис: `banner motd <LINE>`

`no banner motd`

Назначение: Позволяет задать информацию, которая будет выводиться после успешной регистрации пользователя на коммутаторе через консоль или телнет.

Параметр: `<LINE>`: информацию, которая будет выводиться после успешной регистрации пользователя на коммутаторе.

Режим команды: Глобальный режим конфигурирования.

Значение по умолчанию: отсутствует.

Пример:

```
Switch(config)#banner motd ###Hello###
```

1.1.3 clock set

Синтаксис: `clock set <HH:MM:SS> <YYYY.MM.DD>`

Назначение: Установка даты и времени.

Параметр: `<HH:MM:SS>`: текущее время, **HH**: число в пределах 0 — 23, **MM** и **SS**: число в пределах 0 — 59; `<YYYY.MM.DD>`: текущий год/месяц/день, **YYYY**: число в пределах 1970 — 2038, **MON**: месяц, число в пределах 1 — 12, **DD**: день, число в пределах 1 — 31.

Режим команды: Привилегированный режим.

Значение по умолчанию: 0:0:0, 2006.1.1.

Руководство по применению: При выключении электропитания коммутатора его системные часы сбрасываются. После возобновления подачи электропитания с помощью этой команды необходимо установить дату и время.

Пример: Для установки системных часов на 23:00:00 и 1 августа 2002 г., необходимо ввести команду, приведенную ниже.

```
Switch#clock set 23:0:0 2002.8.1
```

1.1.4 config

Синтаксис: `config [terminal]`

Назначение: Переход из привилегированного режима в глобальный режим конфигурирования.

Параметр: `terminal` - конфигурирование терминала.

Режим команды: Привилегированный режим.

Пример:

```
Switch#config
```

1.1.5 debug ssh-server

Синтаксис: `debug ssh-server`

`no debug ssh-server`

Назначение: Выводит на дисплей отладочную информацию SSH-сервера. Отмена команды `"no debug ssh-server"` прекращает вывод на дисплей отладочной информации SSH-сервера.

Значение по умолчанию: Функция выключена.

Режим команды: Привилегированный режим.

Пример:

```
Switch#debug ssh-server
```

1.1.6 enable

Синтаксис: enable

disable

Назначение: Переход из пользовательского режима в привилегированный режим

Режим команды: Пользовательский режим / Привилегированный режим

Описание: При переходе из пользовательского режима в привилегированный режим, во избежание несанкционированного доступа к коммутатору пользователей, не являющимися администраторами, необходима аутентификация пользователей (требуется пароль пользователя с правами администратора). Если введен правильный пароль, выполняется переход в привилегированный режим. Если три последовательных попытки ввода пароля администратора были безуспешны, будет сохранен пользовательский режим. Установка пароля пользователя с правами администратора выполняется в глобальном режиме конфигурирования командой "enable password".

Пример:

```
Switch>enable  
Switch#
```

1.1.7 enable password

Синтаксис: enable password [0 | 7] <password>

no enable password

Назначение: Позволяет задать пароль, используемый для перехода из пользовательского режима в привилегированный режим. Отмена команды "**no enable password**" удаляет этот пароль.

Параметр: <password>: 0 – без шифрования, 7 – с шифрованием.

Режим команды: Глобальный режим конфигурирования.

Значение по умолчанию: Пароль не задан (имеет пустое значение).

Описание: Пароль задается для предотвращения перехода в привилегированный режим пользователей, не имеющих привилегий администратора. Пароль рекомендуется установить в начале конфигурирования коммутатора. Кроме того, если администратору на продолжительное время необходимо покинуть терминал, рекомендуется выйти из привилегированного режима (ввести команду "**exit**").

Пример: Установить для администратора пароль "admin".

```
Switch(config)#enable password 8 admin
```

1.1.8 end

Синтаксис: end

Назначение: Выход из текущего режима работы.

Режим команды: Любой режим за исключением пользовательского и привилегированного режимов.

Пример: Выход из режима настройки vlan.

```
Switch(config-vlan1)#end  
Switch#
```

1.1.9 exec-timeout

Синтаксис: exec-timeout <minutes> [<seconds>]

no exec-timeout

Назначение: Задаёт интервал времени, по истечении которого происходит выход из привилегированного режима. Отмена команды: "**no exec-timeout**" восстанавливает настройки, используемые по умолчанию.

Параметры: `<minute>` интервал времени в минутах (в пределах 0 — 35791). `<seconds>` интервал времени в секундах (в пределах 0 - 2147483).

Режим команды: Глобальный режим конфигурирования

Значение по умолчанию: 10 минут.

Описание: По соображениям безопасности время сеанса работы пользователя, имеющего привилегированный доступ, должно быть ограничено. Необходим таймер сеанса, который и задается с помощью этой команды. По истечении времени таймера сеанс привилегированного доступа будет автоматически прекращен. Для новой попытки привилегированного доступа потребуется повторно ввести имя пользователя и пароль. Если таймер установить на 0, он будет отключен.

Пример: Установить таймер выхода из привилегированного режима на 6 минут.
`Switch(config)#exec-timeout 6`

Установить таймер выхода из привилегированного режима на 5 минут 30 секунд.
`Switch(config)#exec-timeout 5 30`

1.1.10 exit

Синтаксис: `exit`

Назначение: Выход из текущего режима, возврат в предыдущий режим.

Режим команды: Все режимы.

Пример:

```
Switch(config)#exit
Switch#
```

1.1.11 help

Синтаксис: `help`

Назначение: Выводит на экран краткое описание команды, имеющееся в системе контекстной справки.

Режим команды: Все режимы.

Описание: Выводит на экран сообщение онлайн-справки, имеющейся в коммутаторе. По команде `help` отображается информация всей справочной системы, а также ее разделы. Для получения контекстной справки в любой момент можно на клавиатуре нажать клавишу `?`.

Пример:

```
switch(config)#help
```

Командный интерфейс (CLI) обеспечивает расширенный режим работы контекстной справки. Для получения контекстной справки в любой момент нажмите на клавиатуре клавишу `?`.

Если согласований не обнаружено, список, выведенный, системой контекстной справки, будет пустым. Еще раз введите команду, по которой Вы хотите получить справку, затем введите `'?'`, будут показаны опции команды. Поддерживаются два стиля вывода справки:

1. Если Вы знаете имя команды и желаете правильно ввести аргумент (например, ввели `'show ?'`), выводится полный текст справки и описание возможных аргументов команды.
2. Если аргумент введен в сокращенном виде из-за того, что Вы не знаете его точного значения (например, `'show ve?'`), то выводится сокращенная справка.

1.1.12 hostname

Синтаксис: `hostname <hostname>`

`no hostname`

Назначение: Устанавливает строку приглашения командного интерфейса. Отмена команды `"no hostname"` отменяет настройку.

Параметр: `<hostname>`: строка, которая будет выводиться в качестве приглашения, допустимая длина – не более 30 символов.

Режим команды: Глобальный режим конфигурирования.

Значение по умолчанию: Switch.

Описание: Используя эту команду, пользователь может задать строку приглашения командного интерфейса (CLI) в соответствии со своими предпочтениями.

Пример: Установить строку приглашения "Test".

```
Switch(config)#hostname Test
Test(config)#
```

1.1.13 ip host

Синтаксис: ip host <hostname> <ip_addr>

no ip host {<hostname>|all}

Назначение: Задаёт соответствие между хостом и IP-адресом. Отмена команды **no ip host** удаляет соответствие между хостом и IP-адресом.

Параметр: <hostname>: имя хоста, допустимая длина — не более 15 символов.

<ip_addr>: IP-адрес, соответствующий имени хоста; <all>: все имена хостов.

Режим команды: Глобальный режим конфигурирования.

Описание: Соответствие между именем хоста, установленное этой командой, можно использовать в таких командах, как "**ping <host>**".

Пример: Установить IP-адрес 200.121.1.1 для хоста с именем zelax.

```
Switch(config)#ip host zelax 200.121.1.1
```

См. также:

Команда	Описание
telnet	Подключение к удалённому хосту по Telnet
ping	Проверка связи с удалённым клиентским устройством
traceroute	Тестирование шлюзов, через которые пакеты проходят на маршруте от отправившего их оборудования до оборудования назначения

1.1.14 ipv6 host

Синтаксис: ipv6 host <hostname> <ipv6_addr> no ipv6 host {<hostname>|all}

Назначение: Задаёт соответствие между хостом и IPv6-адресом.

Отмена команды "no ipv6 host <hostname>" удаляет соответствие между хостом и IPv6-адресом.

Параметр: <hostname>: имя хоста, допустимая длина — не более 15 символов; <ipv6_addr>: IPv6-адрес, соответствующий имени хоста, <all> все адреса хостов.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Соответствие между именем хоста и IPv6-адресом, установленное этой командой, можно использовать в таких командах, как "traceroute6 <host>" и т. п.

Пример: Установить IPv6-адрес 2001:1:2:3::1 для хоста с именем zelax.

```
Switch(config)#ipv6 host zelax 2001:1:2:3::1
```

См. также:

Команда	Описание
Ping6	Проверка связи с удалённым клиентским устройством
Traceroute6	Тестирование шлюзов, через которые пакеты проходят на маршруте от отправившего их оборудования до оборудования назначения

1.1.15 ip http server

Синтаксис: ip http server

no ip http server

Назначение: Включает доступ к коммутатору по Web.

Режим команды: Глобальный режим конфигурирования.

Описание: С помощью этой команды можно использовать для настройки коммутатора графический web-интерфейс, значительно облегчающий конфигурирование.

Пример: Включить функцию web-сервера и настройку с помощью web-интерфейса.
Switch(config)#ip http server

1.1.16 login

Синтаксис: login

no login

Назначение: Команда **login** включает аутентификацию паролей. “no login” отменяет настройку, выполненную по команде **login**.

Режим команды: Глобальный режим конфигурирования

Значение по умолчанию: Аутентификация паролей выключена

Описание: При применении данной команды, пользователи должны ввести пароль, установленный командой password, на вход в пользовательский режим с консоли.

Пример: Включить пароль.
Switch(config)#login

1.1.17 password

Синтаксис: password [0 | 7] <password>

no password

Назначение: Позволяет ввести пароль на вход в пользовательский режим с консоли. Отмена команды “no password” удаляет этот пароль.

Параметр: <password>: 0 – без шифрования, 7 – с шифрованием..

Режим команды: Глобальный режим конфигурирования.

Значение по умолчанию: Пароль не задан (имеет пустое значение).

Описание: Когда задан пароль и выполнена команда login, пользователи должны будут ввести пароль, заданный командой password, чтобы с консоли войти в пользовательский режим.

Пример:
Switch(config)#password 0 test
Switch(config)#login

1.1.18 reload

Синтаксис: reload

Назначение: Перезагрузка коммутатора.

Режим команды: Привилегированный режим.

Описание: Используя эту команду, можно перезагрузить коммутатор, не выключая электропитание.

1.1.19 service password-encryption

Синтаксис: service password-encryption

no service password-encryption

Назначение: Позволяет зашифровать пароли в системе. Отмена команды “**no service password-encryption**” отменяет шифрование.

Режим команды: Глобальный режим конфигурирования

Значение по умолчанию: Шифрование паролей в системе выключено.

Описание: При вводе этой команды ранее незашифрованные пароли (в том числе введенные с помощью команды **password**, **enable password** и **username**) будут зашифрованы. Отмена команды “**no service password-encryption**”отменяет эту функцию, однако уже зашифрованные пароли останутся зашифрованными.

Пример: Зашифровать пароли в системе.

```
Switch(config)#service password-encryption
```

1.1.20 service terminal-length

Синтаксис: **service terminal-length <0-512>**

no service terminal-length

Назначение: Позволяет настроить число строк, в которых будут отображаться символы на терминале (vty). Отмена команды “**no service terminal-length**” отменяет изменение выводимого на экран числа символов.

Параметр: Число строк символов, отображаемых на экране терминалов vty, в пределах 0-512.

Режим команды: Глобальный режим конфигурирования

Описание: Позволяет задать число строк, отображаемых на экране терминала. Указанное число строк будет отображаться на экранах терминалов telnet- и ssh-клиентов и на консоли.

Пример: Задать число строк на экране vty равным 20.

```
Switch(config)#service terminal-length 20
```

1.1.21 set default

Синтаксис: **set default**

Назначение: Восстанавливает на коммутаторе заводские настройки.

Режим конфигурирования: Привилегированный режим.

Описание: После этой команды на коммутаторе будут восстановлены заводские настройки. Все настройки, сделанные пользователем, будут стерты. После перезагрузки коммутатора, приглашение командной строки примет вид, который был при первом включении питания коммутатора.

Примечание: Для сохранения результатов после применения этой команды следует ввести команду **write**.

Пример:

```
Switch#set default
Are you sure? [Y/N] = y
Switch#write
Switch#reload
```

1.1.22 setup

Синтаксис: **setup**

Назначение: Вход в режим настройки коммутатора.

Режим конфигурирования: Привилегированный режим.

Описание: После входа с помощью этой команды в режим настройки коммутатора может быть выполнено конфигурирование IP-адресов и т. п.

1.1.23 show clock

Синтаксис: show clock

Назначение: Выводит на дисплей показания системных часов.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Описание: Если показания системных часов не соответствуют текущему времени, пользователь с помощью другой команды может установить время и дату.

Пример:

```
Switch#show clock
Current time is TUE AUG 22 11:00:01 2002
```

См. также:

```
clock set
```

1.1.24 show cpu usage

Синтаксис: show cpu usage

Назначение: Выводит на дисплей текущую загрузку процессора.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Описание: Отображение загрузки процессора за последние 5 сек., 30 сек., 5 мин. и с момента старта устройства. Обратите внимание, что выводятся значения свободной процессорной емкости.

Пример:

```
Switch#show cpu usage

Last 5 second CPU IDLE: 87%
Last 30 second CPU IDLE: 88%
Last 5 minute CPU IDLE: 88%
From running CPU IDLE: 92%
```

1.1.25 show memory usage

Синтаксис: show memory usage

Назначение: Выводит на дисплей информацию о использовании оперативной памяти.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Описание: Отображение загрузки процессора за последние 5 сек., 30 сек., 5 мин. и с момента старта устройства. Обратите внимание, что выводятся значения свободной процессорной емкости.

Пример:

```
Switch#show memory usage

The memory total 64 MB , free 17639284 bytes , usage is 73.72%
```

1.1.26 show tech-support

Синтаксис: show tech-support [no-more]

Назначение: Позволяет вывести на дисплей информацию о работе коммутатора, информацию о состоянии задач. Персонал службы технической поддержки может использовать эту команду для контроля правильности работы коммутатора.

Параметр: no-more: позволяет вывести всю необходимую информацию на дисплей сразу же, не ожидая нажатия клавиши пользователем.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Описание: Эта команда используется для сбора соответствующей информации, когда коммутатор работает неправильно.

Пример:

```
Switch#show tech-support
```

1.1.27 show version

Синтаксис: show version

Назначение: Отображает текущую версию аппаратных и программных средств коммутатора.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Описание: Выводит на дисплей информацию об аппаратных и программных функциях коммутатора.

Пример:

```
Switch#show version
```

1.1.28 sysContact

Синтаксис: sysContact <LINE>

no sysContact

Назначение: Задаёт контактную информацию производителя устройства.

Режим конфигурирования: Режим конфигурирования.

Описание: Позволяет указать контактную информацию производителя устройства.

Пример:

```
Switch(config)#sysContact +7 495 7487178
```

1.1.29 sysLocation

Синтаксис: sysLocation <LINE>

no sysContact

Назначение: Задаёт адрес производителя устройства.

Режим конфигурирования: Режим конфигурирования.

Описание: Позволяет указать адрес производителя устройства.

Пример:

```
Switch(config)#sysLocation Russia, 124681, Moscow, Zelenograd,  
Zavodskaya st., 1B, bldg 2
```

1.1.30 username

Синтаксис: username <username> [privilege <privilege>] [password <0|7> <password>]

no username <username>

Назначение: Позволяет локально установить имя пользователя для регистрации и пароль для соответствующего уровня привилегий.

Параметр: <username>: имя пользователя.

<privilege>: максимальный уровень привилегий для доступа к командам, определяющий те из них, которые разрешено выполнять пользователю (1 или 15, по умолчанию установлен уровень 1).

<password>: пароль пользователя. Если при установке пароля ввести опцию 7, то пароль будет зашифрован. Если ввести опцию 0, пароль шифроваться не будет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Коммутатор поддерживает два варианта выбора уровней привилегий для доступа командам (уровень 1 и уровень 15). Уровень 1 используется для доступа к командам в пользовательском режиме. Уровень 15 используется для доступа к командам других режимов (не пользовательского режима). С помощью этой команды может быть сконфигурировано не более 16 локальных пользователей, длина паролей должна быть не более 32 символов.

Примечание: После того, как команды сконфигурированы и пользователь регистрируется на коммутаторе с именем и паролем, определяющим уровень привилегий, до ввода строки с командой аутентификации локального входа с консоли, необходимо удостовериться, что имеется хотя бы один пользователь с уровнем привилегий 15 - это необходимо для внесения изменений в настройки в привилегированном режиме и в глобальном режиме конфигурирования. Если локальных пользователей с уровнем привилегий 15 не зарегистрировано, то на коммутатор можно войти без аутентификации только в том случае, если для входа с консоли установлена локальная аутентификация. Если для регистрации на коммутаторе используется метод HTTP, то зарегистрироваться на нем смогут только пользователи с уровнем привилегий 15. Пользователи с меньшим уровнем привилегий будут отвергаться.

Пример: Требуется создать учетную запись с именем admin и уровнем привилегий 15.

Кроме того, требуется создать двух обычных пользователей с уровнем привилегий 1. После этого требуется включить локальную аутентификацию.

При таких настройках только администратор сможет регистрироваться на коммутаторе в привилегированном режиме, используя методы входа по Telnet и с консоли. Пользователи user1 и user2 смогут регистрироваться на коммутаторе при доступе по Telnet и с консоли только в пользовательском режиме.

При регистрации по HTTP, аутентификацию сможет пройти только администратор, пользователи user1 и user2 будут отвергнуты.

```
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)#username user1 privilege 1 password 7 user1
Switch(config)#username user2 password 0 user2
Switch(config)#authentication line console login local
```

1.1.31 write

Синтаксис: write

Назначение: Сохраняет текущие настроенные параметры во флэш-памяти.

Режим конфигурирования: Привилегированный режим.

Описание: С помощью этой команды, изменения, внесенные в конфигурацию, могут быть сохранены во флэш-памяти. После перезагрузки системы может быть восстановлена ранее сохраненная конфигурация. Эта команда эквивалентна команде **copy running-config startup-config**.

1.2 Команды Telnet и SSH

1.2.1 authentication ip access-class

Синтаксис: authentication ip access-class {<num-std> | <name>}

no authentication ip access-class

Назначение: Ограничивает доступ к коммутатору по telnet/SSH/Web с помощью стандартного ACL.

Параметр: <num-std>: номер стандартного ACL в диапазоне от 1 до 99. <name>: наименование стандартного ACL.

Значение по умолчанию: Доступ не ограничен.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример:

```
Switch(config)#authentication ip access-class 1 in
```

1.2.2 authentication ipv6 access-class

Синтаксис: `authentication ipv6 access-class {<num-std> | <name>}`

`no authentication ipv6 access-class`

Назначение: Ограничивает доступ к коммутатору по telnet/SSH/Web с помощью стандартного IPv6 ACL.

Параметр: `<num-std>`: номер стандартного IPv6 ACL в диапазоне от 500 до 599. `<name>`: наименование стандартного IPv6 ACL.

Значение по умолчанию: Доступ не ограничен.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример:

```
Switch(config)#authentication ipv6 access-class 500 in
```

1.2.3 authentication line login

Синтаксис: `authentication line {console | vty | web} login {local | radius | tacacs}`

`no authentication line {console | vty | web} login`

Назначение: Позволяет сконфигурировать VTY (параметры для инициации сеанса Telnet и SSH), Web и Console, задать приоритет режима аутентификации при регистрации пользователей. Отмена команды `"no authentication line {console | vty | web} login"` восстанавливает режим аутентификации, используемый по умолчанию.

Значение по умолчанию: Настройки для метода входа в консоль не заданы. По умолчанию для методов входа VTY и через Web-интерфейс включена локальная аутентификация.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Для методов регистрации пользователей на коммутаторе с порта Console, VTY и посредством Web-интерфейса может быть задан метод аутентификации. Может быть выбрана локальная аутентификация, аутентификация по протоколам RADIUS, TACACS, либо любая комбинация этих трех методов аутентификации.

Если задана комбинация методов аутентификации, выбор предпочтительного метода выполняется слева направо. Если пользователь прошел аутентификацию по некоторому методу, следующие, менее предпочтительные методы аутентификации, игнорируются.

Если пользователь получил ответ от соответствующего протокола (о том, что он допущен или отвергнут), то не будет предпринято попытки применения следующего метода (исключение из этого правила: если локальная аутентификация была безуспешна, будет предпринята попытка применить следующий метод аутентификации). Если ответ от протокола аутентификации не получен, будет предпринята попытка использовать следующий метод аутентификации.

Для того, чтобы можно было использовать метод RADIUS, предварительно должны быть сконфигурированы функции AAA RADIUS-сервера.

Для того, чтобы можно было использовать метод TACACS, предварительно должен быть сконфигурирован TACACS-сервер.

Команда `authentication line console login` используется только с командой `login`. Команда `authentication line console login` устанавливает на коммутаторе использование метода регистрации с порта Console.

Команда `login` позволяет при регистрации с порта Console использовать пароли, заданные командой `password` для аутентификации.

Если задана локальная аутентификация, но локальных пользователей не сконфигурировано, то пользователи могут воспользоваться регистрацией на коммутаторе через порт Console.

Пример: Установить для сеансов удаленного доступа режим аутентификации radius.
`Switch(config)#authentication login radius`

См. также:

Команда	Описание
<code>aaa enable</code>	Включает функцию аутентификации AAA на

	коммутаторе.
radius-server authentication host	Позволяет задать IP-адрес RADIUS-сервера, номер порта прослушивания, секретный ключ, является ли сервер первичным или нет, режим доступа
tacacs-server authentication host	Позволяет задать IP-адрес, номер порта прослушивания, значение таймера и строку ключа сервера TACACS+
tacacs-server key	Позволяет задать ключ сервера TACACS+

1.2.4 authentication securityip

Синтаксис: `authentication securityip <ip-addr>`

no authentication securityip <ip-addr>

Назначение: Позволяет установить безопасный IP-адрес для методов регистрации Telnet и HTTP. Отмена команды “**no authentication securityip <ip-addr>**” удаляет установленный безопасный IP-адрес.

Параметры: `<ip-addr>`: безопасный IP-адрес соответствующего клиента для регистрации на коммутаторе.

Значение по умолчанию: Безопасный IP-адрес не установлен.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Пока безопасный IP-адрес не установлен, на IP-адрес клиента, который может быть зарегистрирован на коммутаторе, не накладывается никаких ограничений.

После того, как безопасный IP-адрес установлен, только клиенты с безопасными IP-адресами могут регистрироваться на коммутаторе.

На коммутаторе может быть сконфигурировано не более 32 безопасных IP-адресов.

Пример: Установить в качестве безопасного IP-адреса 192.168.1.21.

```
Switch(config)#authentication securityip 192.168.1.21
```

1.2.5 authentication securityipv6

Синтаксис: `authentication securityipv6 <ipv6-addr>`

no authentication securityipv6 <ipv6-addr>

Назначение: Позволяет установить безопасный IPv6-адрес для методов регистрации Telnet и HTTP. Отмена команды “**no authentication securityipv6 <ipv6-addr>**” удаляет установленный безопасный IPv6-адрес.

Параметры: `<ipv6-addr>`: безопасный IPv6-адрес, который может использоваться для регистрации на коммутаторе.

Значение по умолчанию: Безопасный IPv6-адрес не установлен.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Пока безопасный IP-адрес не установлен, на IPv6-адрес клиента, который может быть зарегистрирован на коммутаторе, не накладывается никаких ограничений. После того, как безопасный IPv6-адрес установлен, только клиенты с безопасными IPv6-адресами могут регистрироваться на коммутаторе. На коммутаторе может быть сконфигурировано не более 32 безопасных IPv6-адресов.

Пример: Установить безопасный IPv6-адрес 2001:da8:123:1::1.

```
Switch(config)#authentication securityipv6 2001:da8:123:1::1
```

1.2.6 authorization

Синтаксис: `authorization line {console | vty | web} exec {local | radius | tacacs}`

no authorization line {console | vty | web} exec

Назначение: Позволяет сконфигурировать VTY (параметры для инициации сеанса Telnet и SSH), Web и Console, задать приоритет режима авторизации при регистрации пользователей.

Значение по умолчанию: Не задано.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Для методов регистрации пользователей на коммутаторе с порта Console, VTY и посредством Web-интерфейса может быть задан метод авторизации. Может быть выбрана локальная авторизация, авторизация по протоколам RADIUS, TACACS, либо любая комбинация этих трех методов авторизации.

Если задана комбинация методов авторизации, выбор предпочтительного метода выполняется слева направо. Если пользователь прошел авторизацию по некоторому методу, следующие, менее предпочтительные методы авторизации, игнорируются.

Если пользователь получил ответ от соответствующего протокола (о том, что он допущен или отвергнут), то не будет предпринято попытки применения следующего метода (исключение из этого правила: если локальная авторизация была безуспешна, будет предпринята попытка применить следующий метод авторизации). Если ответ от протокола авторизации не получен, будет предпринята попытка использовать следующий метод авторизации.

Для того, чтобы можно было использовать метод RADIUS, предварительно должны быть сконфигурированы функции AAA RADIUS-сервера. Для того, чтобы можно было использовать метод TACACS, предварительно должен быть сконфигурирован TACACS-сервер.

Пример:

```
Switch(config)#authorization line vty exec radius
```

1.2.7 terminal length

Синтаксис: `terminal length <0-512>`

`terminal no length`

Назначение: Позволяет задать число символов, отображаемых на экране терминала. Отмена команды **“terminal no length”** отменяет операцию переключения экрана и восстанавливает отображение всего контента.

Параметр: Число строк, отображаемых на экране, в пределах от 0 до 512 (0 соответствует безостановочному отображению символов).

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: 25 строк.

Описание: Позволяет задать число строк, отображаемых на терминале, если имеются еще данные для отображения, не уместившиеся на экране, будет выведено сообщение More... (Еще...). Для вывода на экран последующей информации нажмите любую клавишу

Пример: Установить вывод по 20 строк на экране.

```
Switch#terminal length 20
```

1.2.8 terminal monitor

Синтаксис: `terminal monitor`

`terminal no monitor`

Назначение: Позволяет скопировать сообщения отладки на текущий терминал. Отмена команды **“terminal no monitor”** восстанавливает режим, заданный по умолчанию.

Режим конфигурирования: Привилегированный режим.

Описание: Позволяет задать дополнительные направления вывода сообщений отладки, отображаемых на текущем терминале. Если команда вводится через telnet или SSH-клиент, сообщения отладки будут посылаться этому клиенту. По умолчанию сообщения отладки выводятся на консоль.

Пример:

```
Switch#terminal monitor
```

1.2.9 telnet

Синтаксис: `telnet {<ip-addr> | <ipv6-addr> | host <hostname>} [<port>]`

Назначение: Подключение к удаленному хосту по Telnet.

Параметр: `<ip-addr>`: IP-адрес удаленного хоста;

`<ipv6-addr>`: IPv6-адрес удаленного хоста;

`<hostname>`: имя удаленного хоста, допустимая длина — не более 30 символов;

`<port>`: номер порта, в пределах 0~65535.

Режим конфигурирования: Привилегированный режим.

Описание: Эта команда используется, когда коммутатор работает как Telnet-клиент, используя команду `telnet` в привилегированном режиме, пользователь может регистрироваться на других удаленных хостах для их настройки. Когда коммутатор работает как Telnet-клиент, он может устанавливать TCP-соединение только с одним удаленным хостом. Если требуется соединение с другим удаленным хостом, текущее TCP-соединение должно быть сброшено «горячей» командой `CTRL+ \`. Для доступа по telnet необходимо предварительно установить соответствие между именем хоста и IP/IPv6-адресом. Требующиеся для этого команды: `ip host`, `ipv6 host` (см. соответствующие разделы). Если хост имеет как IPv4-адрес, так и IPv6-адрес, для доступа по telnet следует использовать IPv6-адрес.

Пример: Установить связь с хостом с IP-адресом 20.1.1.1 путем доступа по Telnet.

```
Switch#telnet 20.1.1.1
Connecting Host 20.1.1.1 Port 23...
Service port is 23
Connected to 20.1.1.1
login:admin
password:*****
Switch_2>
```

1.2.10 telnet-server enable

Синтаксис: `telnet-server enable`

`no telnet-server enable`

Назначение: Включает функцию Telnet-сервера на коммутаторе. Отмена команды `no telnet-server enable` выключает функцию Telnet-сервера.

Значение по умолчанию: Telnet-сервер включен.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Эта команда может быть выполнена только через порт Console. Этой командой можно разрешить или запретить сеансы удаленного доступа к коммутатору по Telnet.

Пример: Выключить сервер telnet для коммутатора.

```
Switch(config)#no telnet-server enable
```

1.2.11 telnet-server max-connection

Синтаксис: `telnet-server max-connection {<max-connection-number> | default}`

Назначение: Позволяет задать максимальное число соединений Telnet, поддерживаемых коммутатором.

Параметры: `<max-connection-number>`: максимальное число поддерживаемых Telnet-соединений, в пределах от 5 до 16.

Опция `default` восстанавливает настройки, заданные по умолчанию.

Значение по умолчанию: Установлено максимальное число соединений, равное 5.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Задать максимальное число соединений Telnet, поддерживаемых коммутатором, равным 10.

```
Switch(config)#telnet-server max-connection 10
```

1.2.12 ssh-server authentication-retries

Синтаксис: `ssh-server authentication-retries <authentication-retries>`

`no ssh-server authentication-retries`

Назначение: Задаёт число попыток аутентификации SSH. Отмена команды “`no ssh-server authentication-retries`” восстанавливает число попыток аутентификации SSH, используемое по умолчанию.

Параметр: `<authentication-retries>`: число попыток аутентификации, диапазон значений - от 1 до 10.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Задано число попыток аутентификации SSH равное 3.

Пример: Установить число попыток аутентификации SSH-клиентов равное 5.

```
Switch(config)#ssh-server authentication-retries 5
```

1.2.13 ssh-server enable

Синтаксис: `ssh-server enable`

`no ssh-server enable`

Назначение: Включает функцию SSH-сервера на коммутаторе. Отмена команды “`no ssh-server enable`” выключает функцию SSH-сервера.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: По умолчанию функция SSH-сервера выключена.

Описание: До соединения SSH-клиентов с коммутатором должны быть сконфигурированы пользователи и SSH-сервер.

Пример: Включить SSH-сервер на коммутаторе.

```
Switch(config)#ssh-server enable
```

1.2.14 ssh-server host-key create rsa

Синтаксис: `ssh-server host-key create rsa [modulus < modulus >]`

Назначение: Генерирует новый ключ хоста RSA.

Параметр: `modulus` – модуль, который будет использован для вычисления ключа хоста; диапазон значений - от 768 до 2048. Значение по умолчанию: 1024.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Система использует ключ, который ssh-сервер сгенерировал при первом запуске.

Описание: Эта команда используется для создания новых ключей безопасности для хоста. Когда SSH-клиент регистрируется на сервере, новый ключ хоста используется для аутентификации. После того как ключ создан, SSH-клиенты смогут использовать его для связи с хостом. Если конфигурация при новом ключе была сохранена командой `write`, система будет постоянно использовать этот ключ для аутентификации хоста. Шифрование и дешифрование ключа может занимать значительное время. Кроме того, некоторые клиенты могут не поддерживать ключи с модулем 2048 бит. Поэтому рекомендуется для обеспечения эффективности и совместимости использовать модули 1024 бит, заданные по умолчанию.

Пример: Создать для хоста новый ключ.

```
Switch(config)#ssh-server host-key create rsa
```

1.2.15 ssh-server max-connection

Синтаксис: `ssh-server max-connection {<max-connection-number> | default}`

Назначение: Позволяет задать максимальное число соединений SSH, поддерживаемых коммутатором.

Параметры: `<max-connection-number>`: максимальное число поддерживаемых SSH-соединений, в пределах от 5 до 16. Опция **default** восстанавливает настройки, заданные по умолчанию.

Значение по умолчанию: Установлено максимальное число соединений, равное 5.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Задать максимальное число соединений SSH, поддерживаемых коммутатором, равным 10.

```
Switch(config)#ssh-server max-connection 10
```

1.2.16 ssh-server timeout

Синтаксис: `ssh-server timeout <timeout>`

`no ssh-server timeout`

Назначение: Позволяет задать время таймера аутентификации SSH. Отмена команды **“no ssh-server timeout”** восстанавливает время таймера аутентификации SSH, используемое по умолчанию.

Параметр: `<timeout>`: значение времени таймера в диапазоне от 10 до 600 секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: По умолчанию установлено время таймера аутентификации SSH 180 с.

Пример: Установить время таймера аутентификации SSH 240 секунд.

```
Switch(config)#ssh-server timeout 240
```

1.2.17 show ssh-server

Синтаксис: `show ssh-server`

Назначение: Выводит на дисплей информацию о состоянии SSH-сервера и информацию о зарегистрированных пользователях.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show ssh-server
ssh-server is enabled
connection  version      state                user name
1           2.0          session started    test
```

1.2.18 show telnet login

Синтаксис: `show telnet login`

Назначение: Выводит на дисплей информацию о пользователе Telnet, подключенном к коммутатору.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Описание: Эта команда используется для восстановления информации о сеансах удаленного доступа telnet.

Пример:

```
Switch#show telnet login
Authenticate login by local
Login user: admin
```

1.3 Команды для настройки IP-адресов коммутатора

1.3.1 interface vlan

Синтаксис: `interface vlan <vlan-id>`

`no interface vlan <vlan-id>`

Назначение: Позволяет войти в режим настройки интерфейса VLAN. Отмена команды “`no interface vlan <vlan-id>`” удаляет существующий интерфейс VLAN.

Параметры: `<vlan-id>`: числовой идентификатор VLAN ID, присвоенный VLAN, в пределах от 1 до 4094.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Перед тем, как настраивать VLAN, необходимо убедиться, что он создан. Для выхода из режима настройки интерфейсов VLAN в глобальный режим конфигурирования используйте команду `exit`.

Пример: Войти в режим настройки интерфейса VLAN для VLAN1.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#
```

1.3.2 ip address

Синтаксис: `ip address <ip-address> <mask> [secondary]`

`no ip address [<ip-address> <mask>] [secondary]`

Назначение: Позволяет настроить IP-адрес и маску для коммутатора. Отмена команды “`no ip address <ip address> <mask> [secondary]`” удаляет сделанную настройку IP-адреса.

Параметр: `<ip-address>`: IP-адрес; `<mask>`: маска подсети; `[secondary]` указывает, что введенный IP-адрес является вторичным IP-адресом.

Значение по умолчанию: IP-адрес не задан.

Режим конфигурирования: Режим настройки интерфейса VLAN.

Описание: Перед тем, как присваивать IP-адрес коммутатору необходимо создать интерфейс VLAN.

Пример: Установить IP-адрес 10.1.128.1/24 для интерфейса VLAN1.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

См. также:

Команда	Описание
<code>ip bootp-client enable</code>	Конфигурирует коммутатор, как BootP-клиент
<code>ip dhcp-client enable</code>	Используется для настройки коммутатора для работы в качестве DHCP-клиента и получения IP-адресов для него и шлюза по протоколу DHCP

1.3.3 ipv6 address

Синтаксис: `ipv6 address <ipv6address | prefix-length> [eui-64]`

`no ipv6 address <ipv6address | prefix-length> [eui-64]`

Назначение: Позволяет задать для интерфейса агрегируемый глобальный unicast-адрес, unique local адрес и link local адрес.

Параметры: `<ipv6address>`: префикс IPv6-адреса; `<prefix-length>`: длина префикса IPv6-адреса, в пределах от 3 до 128; `eui-64` означает, что IPv6-адрес для интерфейса будет создан автоматически.

Режим конфигурирования: Режим настройки интерфейсов

Значение по умолчанию: Нет.

Описание: Префикс IPV6-адреса не должен быть multicast-адресом, либо IPV6-адресом другого специального типа. Разным интерфейсам VLAN уровня 3 запрещено совместно использовать один и тот же префикс адреса. Как и любой глобальный unicast-адрес, префикс должен быть в пределах от 2001:: до 3fff ::, при этом длина его должна быть не менее 3. Длина префикса адреса локального сайта или линии не должна быть менее 10.

Примеры: Задать IPV6-адрес интерфейса третьего уровня для VLAN1. Задать префикс 2001:3f:ed8::99, длина префикса 64.

```
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
```

1.3.4 ip bootp-client enable

Синтаксис: ip bootp-client enable

no ip bootp-client enable

Назначение: Конфигурирует коммутатор, как BootP-клиент. Посредством протокола BootP коммутатор может самостоятельно получить IP-адреса для себя и IP-адрес шлюза, по которым к нему можно будет обращаться. Отмена команды “no ip bootp-client enable” протокол BootP на коммутаторе.

Значение по умолчанию: BootP-клиент выключен.

Режим конфигурирования: Режим настройки интерфейса VLAN.

Описание: Существует три метода конфигурирования IP-адреса коммутатора: ручное конфигурирование, по протоколу BootP и по протоколу DHCP. Эти три метода взаимоисключающие. В одно и то же время может использоваться только один метод.

Для получения IP-адреса по BootP в сети должен функционировать DHCP-сервер или BootP-сервер.

Пример: Получить IP-адрес, используя протокол BootP.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip bootp-client enable
Switch (Config-if-Vlan1)#exit
Switch(config)#
```

См. также:

Команда	Описание
ip address	Позволяет задать для коммутатора IP-адрес и соответствующую маску адресов
ip dhcp-client enable	Используется для конфигурирования коммутатора, как DHCP-клиента и получения IP-адреса для него и IP-адреса шлюза по протоколу DHCP

1.3.5 ip dhcp-client enable

Синтаксис: ip dhcp-client enable

no ip dhcp-client enable

Назначение: Используется для настройки коммутатора для работы в качестве DHCP-клиента и получения IP-адресов для него и IP-адреса шлюза по протоколу DHCP. Отмена команды “no ip dhcp-client enable” выключает настройку для работы в качестве DHCP-клиента.

Примечание: Для восстановления IP-адреса по DHCP в сети должен функционировать DHCP-сервер.

Значение по умолчанию: конфигурирование с помощью DHCP-клиента выключено.

Режим конфигурирования: Режим настройки интерфейса VLAN.

Описание: Настройка IP-адреса вручную, настройка по DHCP – три взаимоисключающих метода конфигурирования. В одно и то же время может использоваться только один метод.

Пример: Сконфигурировать IP-адрес по протоколу DHCP.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

1.4 Команды для настройки протокола SNMP

1.4.1 debug snmp mib

Синтаксис: `debug snmp mib`

`no debug snmp mib`

Назначение: Включает отладку SNMP mib. Команда “`no debug snmp mib`” выключает отладку.

Режим конфигурирования: Привилегированный режим.

Описание: Если возникли неполадки с SNMP, команда отладки SNMP позволяет локализовать источники неполадок.

Пример:

```
Switch#debug snmp mib
```

1.4.2 debug snmp kernel

Синтаксис: `debug snmp kernel`

`no debug snmp kernel`

Назначение: Включает отладку ядра SNMP. Команда “`no debug snmp kernel`” выключает функцию отладки.

Режим конфигурирования: Привилегированный режим.

Описание: Если возникли неполадки с SNMP, команда отладки SNMP позволяет локализовать источники неполадок.

Пример:

```
Switch#debug snmp kernel
```

1.4.3 rmon enable

Синтаксис: `rmon enable`

`no rmon enable`

Назначение: Включает функции RMON. Команда “`no rmon enable`” выключает RMON.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: По умолчанию функции RMON выключены.

Пример: Включить функции RMON.

```
Switch(config)#rmon enable
```

Disable RMON.

```
Switch(config)#no rmon enable
```

1.4.4 show private-mib oid

Синтаксис: `show private-mib oid`

Назначение: Выводит цифровое значение oid для private MIB.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования.

Пример:

```
Switch#show private-mib oid
Private MIB OID:1.3.6.1.4.1.7840.2.1
```

1.4.5 show snmp

Синтаксис: show snmp

Назначение: Отображает всю информацию счетчиков SNMP.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Пример:

```
Switch#show snmp
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs 0 SNMP packets output
0 Too big errors (Max packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Get-response PDUs
  0 SNMP trap PDUs
```

Информация, отображаемая на дисплее	Описание
snmp packets input	Общее число входных пакетов SNMP.
bad snmp version errors	Число пакетов с ошибками в информации о номере версии протокола.
unknown community name	Число пакетов с ошибками в имени community.
illegal operation for community name supplied	Число пакетов с ошибками из-за прав доступа для имени community.
encoding errors	Число пакетов с ошибками кодирования.
number of requested variablest	Число переменных, запрошенных NMS.
number of altered variables	Число переменных, заданных NMS.
get-request PDUs	Число пакетов, принятых по запросам "get" (получить)
get-next PDUs	Число пакетов, принятых по запросам "getnext" (получить следующий)
set-request PDUs	Число пакетов, принятых по запросам "set" (установить)
snmp packets output	Общее число выходных пакетов SNMP.
too big errors	Объект не может уложить отклик в одно сообщение.
maximum packet size	Максимальная длина пакетов SNMP.
no such name errors	Число пакетов, запрашивающих несуществующие объекты MIB.
bad values errors	Число пакетов SNMP с ошибками "Bad_values" (Неправильные значения)
general errors	Число пакетов SNMP с ошибками "General_errors" (Ошибки общего характера)

response PDUs	Число посланных ответных пакетов.
trap PDUs	Число посланных пакетов Trap.

1.4.6 show snmp engineid

Синтаксис: show snmp engineid

Назначение: Выводит на дисплей ID вычислительной подсистемы и другие данные о ней.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Пример:

```
Switch#show snmp engineid SNMP
engineID:3138633303f1276c
Engine Boots is:1
```

Информация, отображаемая на дисплее	Описание
SNMP engineID	Номер вычислительной подсистемы
Engine Boots	Число загруженных вычислительных подсистем

1.4.7 show snmp group

Синтаксис: show snmp group

Назначение: Выводит на дисплей информацию о группе.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Пример:

```
Switch#show snmp group
Group Name:initial
Security Level:noAuthnoPriv
Read View:one
Write View:<no writeview specified>
Notify View:one
```

Информация, отображаемая на дисплее	Описание
Group Name	Имя группы
Security level	Уровень безопасности
Read View	Имя вида сводной информации, доступного только по чтению
Write View	Имя вида сводной информации, доступного по записи
Notify View	Имя вида уведомления сводной информации
<no writeview specified>	Имя вида сводной информации не задано пользователем

1.4.8 show snmp mib

Синтаксис: show snmp mib

Назначение: Выводит на дисплей все MIB, поддерживаемые коммутатором.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

1.4.9 show snmp status

Синтаксис: show snmp status

Назначение: Выводит на дисплей информацию о конфигурации SNMP.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Пример:

```
Switch#show snmp status
Trap enable
RMON enable
Community Information:
V1/V2c Trap Host Information:
V3 Trap Host Information:
Security IP Information:
```

Информация, отображаемая на дисплее	Описание
Community string	Строка Community
Community access	Разрешен ли доступ к Community
Trap-rec-address	IP-адрес, который используется для приема сообщений Trap.
Trap Host	Включена или выключена отправка сообщений Trap.
Security IP	IP-адрес NMS, которой разрешен доступ к Агенту

1.4.10 show snmp user

Синтаксис: show snmp user

Назначение: Выводит на дисплей информацию о пользователе.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Пример:

```
Switch#show snmp user
User name: zelax
Engine ID: 1234567890
Auth Protocol:MD5
Priv Protocol:DES-CBC
Row status:active
```

Информация, отображаемая на дисплее	Описание
User name	Имя пользователя
Engine ID	ID вычислительной подсистемы
Priv Protocol	Применяемый алгоритм шифрования
Auth Protocol	Применяемый алгоритм идентификации
Row status	Состояние пользователя

1.4.11 show snmp view

Синтаксис: show snmp view

Назначение: Выводит на дисплей информацию о виде сводной информации

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Пример:

```
Switch#show snmp view
View Name:readview
1. -Included active
1.3. Excluded active
```

Информация, отображаемая на дисплее	Описание
View Name	Имя вида сводной информации
1. и 1.3.	Номер OID
Included	Вид сводной информации включает суб-деревья, корнем которых является этот OID
Excluded	Вид сводной информации не включает суб-деревья, корнем которых является

	этот OID
active	Состояние

1.4.12 snmp-server community

Синтаксис: `snmp-server community {ro | rw} <string>`

`no snmp-server community <string>`

Назначение: Конфигурирует для коммутатора строку community. Отмена команды “`no snmp-server community <string>`” удаляет сконфигурированную строку community.

Параметр: `<string>`: строка community;

`ro | rw`: указывает права доступа к базе данных MIB,

`ro` задает доступ только по чтению, `rw` - доступ по чтению/записи.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Коммутатором поддерживаются не более 4 строк community.

Пример: Задать для строки community значение private и разрешить доступ по чтению/записи.

```
Switch(config)#snmp-server community private rw
```

Задать для строки community значение public и разрешить доступ только по чтению.

```
Switch(config)#snmp-server community public ro
```

Измените права доступа для private на «только чтение».

```
Switch(config)#snmp-server community private ro
```

Удалить строку community с именем private.

```
Switch(config)#no snmp-server community private
```

1.4.13 snmp-server enable

Синтаксис: `snmp-server enable`

`no snmp-server enable`

Назначение: Делает коммутатор доступным, как прокси-сервер SNMP. Отмена команды “`no snmp-server enable`” выключает прокси-сервер SNMP.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: прокси-сервер SNMP выключен.

Описание: Прокси-сервер SNMP должен быть включен этой командой до того, как станет возможным конфигурирование коммутатора программным обеспечением управления сетью.

Пример: Включить прокси-сервер SNMP.

```
Switch(config)#snmp-server enable
```

1.4.14 snmp-server enable traps

Синтаксис: `snmp-server enable traps no snmp-server enable traps`

Назначение: Включает на коммутаторе отправку сообщения Trap. Отмена команды “`no snmp-server enable traps`” удаляет сделанную настройку.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Отправка сообщений Trap выключена.

Описание: Когда отправка сообщений Trap включена, они будут отправляться при включении/выключении системы или интерфейсов.

Пример: Включить отставку сообщений Trap.

```
Switch(config)#snmp-server enable traps
```

Выключить отставку сообщений Trap.

```
Switch(config)#no snmp-server enable trap
```

1.4.15 snmp-server engineid

Синтаксис: `snmp-server engineid <engine-string>`

`no snmp-server engineid`

Назначение: Позволяет задать идентификатор id вычислительной подсистемы для SNMP-сервера. Отмена команды “`no snmp-server engineid`” удаляет настройку id вычислительной подсистемы.

Режим конфигурирования: Глобальный режим конфигурирования

Параметр: `<engine-string>`: id вычислительной подсистемы в шестнадцатеричной форме, длина от 1 до 32 символов.

Значение по умолчанию: ID компании + локальный MAC-адрес.

Пример: Задать в качестве id вычислительной подсистемы A66688999F
`Switch(config)#snmp-server engineid A66688999F`

Восстановить id вычислительной подсистемы, заданный по умолчанию.
`Switch(config)#no snmp-server engineid`

1.4.16 snmp-server group

Синтаксис: `snmp-server group <group-string> {NoauthNopriv | AuthNopriv | AuthPriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]]`

`no snmp-server group <group-string> {NoauthNopriv | AuthNopriv | AuthPriv}`

Назначение: Конфигурирует на коммутаторе новую группу. Отмена команды “`no snmp-server group <group-string> {NoauthNopriv|AuthNopriv|AuthPriv}`” удаляет соответствующую группу.

Режим конфигурирования: Глобальный режим конфигурирования

Параметры: `<group-string>`: имя группы, длина имени — от 1 до 32 символов.

NoauthNopriv Если задана эта опция, аутентификация и шифрование будут выключены.

AuthNopriv Если задана эта опция, аутентификация будет включена, но шифрование применяться не будет.

AuthPriv Будут включены и шифрование, и аутентификация

read-string Имя считываемого вида, длина имени - от 1 до 32 символов

write-string Имя записываемого вида, длина имени - от 1 до 32 символов

notify-string Имя вида, для которого посылается сообщение Trap, длина имени - от 1 до 32 символов

Описание: По умолчанию системой сконфигурирован вид сводной информации с именем v1defaultviewname. Рекомендуется использовать этот вид.

Если считываемый или записываемый виды не сконфигурированы, соответствующая операция работать не будет.

Пример: Создать вид сводной информации с именем CompanyGroup, с использованием аутентификации и шифрования, с доступом по чтению и именем readview, операция записи недоступна.

```
Switch(config)#snmp-server group CompanyGroup AuthPriv read readview
```

Удалить вид.

```
Switch(config)#no snmp-server group CompanyGroup AuthPriv
```

1.4.17 snmp-server host

Синтаксис: `snmp-server host {<host-ipv4-address> | <host-ipv6-address>} {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>`

no snmp-server host {<host-ipv4-address> | <host-ipv6-address>} {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>

Назначение: В версиях протокола SNMP v1 и v2c эта команда конфигурирует строку Trap community и IP-адрес станции управления SNMP, которая будет принимать сообщения Trap.

В версии протокола SNMP v3 этой командой следует конфигурировать IP-адрес SNMP-сервера, имя пользователя и уровень безопасности. Отмена команды “**no snmp-server host {<host-ipv4-address> | <host-ipv6-address>} {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>**” удаляет соответствующую настройку.

Режим конфигурирования: Глобальный режим конфигурирования

Параметры: <host-ipv4-addr> | <host-ipv6-addr>: IP-адрес рабочей станции NMS, которая принимает сообщения Trap. v1 | v2c | v3: номер версии протокола, используемый для сообщений Trap.

NoauthNopriv|AuthNopriv|AuthPriv: уровень безопасности при сообщениях Trap версии v3 (соответственно: без аутентификации и без шифрования; с аутентификацией, безшифрования; с аутентификацией и шифрованием.).

<user-string>: строка community для сообщений Trap в версиях протокола v1/v2c. В версии v3 эта строка является именем пользователя.

Описание: Строка community для сообщений Trap, сконфигурированная этой командой, используется в качестве строки community, заданной по умолчанию для сообщений RMON.

Если для событий RMON строк community не сконфигурировано, будет использована строка community, сконфигурированная этой командой. В остальных случаях для сообщений RMON Trap будет использоваться строка RMON.

Эта команда позволяет задать IP-адрес сетевой станции управления, принимающей сообщения SNMP Trap, однако всего может быть задано не более 8 IP-адресов.

Пример: Сконфигурировать IP-адрес для получения сообщений Trap
Switch(config)#snmp-server host 1.1.1.5 v1 usertrap

1.4.18 snmp-server securityip

Синтаксис: snmp-server securityip {<ipv4-address> | <ipv6-address>}

no snmp-server securityip {<ipv4-address> | <ipv6-address>}

Назначение: Конфигурирует права доступа с безопасного IPv4- или IPv6-адреса станции NMS административного управления коммутатором. Отмена команды “**no snmp-server securityip {<ipv4-address> | <ipv6-address>}**” удаляет сконфигурированный безопасный IPv4- или IPv6-адрес.

Режим конфигурирования: Глобальный режим конфигурирования

Параметры: <ipv4-address>: безопасный IP-адрес NMS.

<ipv6-address>: безопасный IPv6-адрес NMS.

Описание: Так как эта команда влияет только на IPv4- или IPv6-адрес станции администрирования NMS и безопасный IPv4- или IPv6-адрес, сконфигурированный этой командой, в результате чего пакеты SNMP, посылаемые станцией могут обрабатываться коммутатором, то эта команда применима только в версиях протокола SNMPv1 и SNMPv2c.

Эта команда позволяет задать IPv4- или IPv6-адрес сетевой станции управления, принимающей сообщения SNMP Trap, однако всего может быть задано не более 6 IP-адресов.

Пример: Сконфигурировать безопасный IP-адрес станции администрирования NMS.
Switch(config)#snmp-server securityip 1.1.1.5

Удалить безопасный IPv6-адрес.

Switch(config)#no snmp-server securityip 2001::1

1.4.19 snmp-server securityip enable

Синтаксис: snmp-server securityip enable

snmp-server securityip disable

Назначение: Включает или выключает функцию проверки безопасного IP-адреса NMS.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: По умолчанию функция проверки безопасного IP-адреса включена.

Пример: Выключить функцию проверки безопасного IP-адреса.

```
Switch(config)#snmp-server securityip disable
```

1.4.20 snmp-server trap-source

Синтаксис: snmp-server trap-source {<ipv4-address> | <ipv6-address>}

no snmp-server trap-source {<ipv4-address> | <ipv6-address>}

Назначение: Устанавливает IP-адреса источника для отправки trap-сообщений.

Режим конфигурирования: Глобальный режим конфигурирования

Параметры: <ipv4-address>: IPv4-адрес для отправки trap-сообщений, <ipv6-address>: IPv6-адрес для отправки trap-сообщений

Пример:

```
Switch(config)#snmp-server trap-source 192.168.0.24
```

1.4.21 snmp-server view

Синтаксис: snmp-server view <view-string> <oid-string> {include | exclude}

no snmp-server view <view-string>

Назначение: С помощью этой команды создаются или обновляются сконфигурированные виды сводной информации. Отмена команды “no snmp-server view <view-string>” удаляет соответствующий сконфигурированный вид.

Режим конфигурирования: Глобальный режим конфигурирования

Параметры: <view-string>: имя вида, длина имени – в диапазоне 1-32 символа;

<oid-string>: номер OID или имя соответствующего узла, длина имени 1-255 символов.

include | exclude, — включает или исключает этот OID.

Описание: Команда поддерживает не только ввод символьной строки переменной OID в качестве параметра, она также поддерживает ввод, при котором в качестве параметра используется имя узла.

Пример:

Создать вид сводной информации с именем readview, в который включен узел iso и исключен узел iso.3.

```
Switch (config)#snmp-server view readview iso include
```

```
Switch (config)#snmp-server view readview iso.3 exclude
```

Удалить вид.

```
Switch (config)#no snmp-server view readview
```

1.4.22 snmp-server user

Синтаксис: snmp-server user <use-string> <group-string> (encrypted | noencrypted) auth (md5 | sha) <word>

no snmp-server user <user-string>

Назначение: Добавляет пользователя в существующую группу. Отмена команды “no snmp-server user <user-string> <group-string>” удаляет пользователя.

Режим конфигурирования: Глобальный режим конфигурирования

Параметры: <view-string>: имя пользователя, длина имени от 1 до 32 символов;

<group-string>: имя группы, в которую добавляется пользователь, длина имени от 1 до 32 символов;

Если задано **encrypted**, пароль пользователя будет зашифрован по алгоритму DES.

Если задано **auth**, будет проверена контрольная сумма пакетов snmp.

Если задано **md5**, будет использован алгоритм HMAC MD5.

Если задано **sha**, будет использован алгоритм HMAC SHA.

<word>: пароль для пользователя, длина пароля от 8 до 32 символов.

Описание: Если шифрование и аутентификация не сконфигурированы, то по умолчанию они выключены.

Если шифрование включено, то и аутентификация также будет включена.

При удалении пользователя: если введенное имя пользователя распознано (обработано правильно), то имя группы игнорируется.

Пример: Добавить пользователя с именем tester в группу с именем UserGroup. Должно быть включено шифрование, при аутентификации должен использоваться алгоритм HMAC md5 и пароль hello.

```
Switch (config)#snmp-server user tester UserGroup encrypted auth md5 hello
```

Удалить пользователя.

```
Switch (config)#no snmp-server user tester
```

1.5 Команды для обновления ПО коммутатора

1.5.1 copy (FTP)

Синтаксис: `copy <source-url> <destination-url> [ascii | binary]`

Назначение: Загружает файлы в FTP-клиент.

Параметры: **<source-url>**: местонахождение исходных файлов или каталогов, которые требуется скопировать;

<destination-url>: адрес назначения, в которое требуется скопировать исходные файлы или каталоги;

вид полей **<source-url>** и **<destination-url>** сильно изменяется в зависимости от конкретного расположения файлов или каталогов.

ascii указывает, что следует использовать стандарт ASCII;

binary указывает, что при передаче файла следует использовать двоичную систему (метод передачи, используемый по умолчанию).

Когда URL соответствует FTP-адресу, форма команды следующая: Ошибка! Недопустимый объект гиперссылки.>, где **<username>** является именем пользователя FTP, **<password>**: пароль пользователя FTP, **<ipaddress>**: IP-адрес FTP сервера/клиента, **<filename>**: имя файла, выгружаемого или загружаемого по FTP.

Специальные ключевые слова для имени файла:

Ключевые слова	Адреса источника или назначения
running-config	Файлы текущей рабочей конфигурирования
startup-config	Файлы конфигурации начальной загрузки
nos.img	Системные файлы
nos.rom	Системные файлы начальной загрузки

Режим конфигурирования: Привилегированный режим

Примеры: Сохранить файлы образа системы во флэш-памяти, используя FTP-сервер с адресом 10.1.1.1, имя пользователя Switch, пароль superuser.

```
Switch#copy nos.img ftp://Switch:superuser@10.1.1.1/nos.img
```

Получить с FTP-сервера с адресом 10.1.1.1 файл nos.img, используя имя пользователя Switch и пароль superuser.

```
Switch#copy ftp://Switch:superuser@10.1.1.1/nos.img nos.img
```

Сохранить файлы рабочей конфигурации.

```
Switch#copy running-config startup-config
```

См. также:

Команда	Описание
write	Сохраняет текущие настройки параметров во флэш-памяти

1.5.2 copy (TFTP)

Синтаксис: copy <source-url> <destination-url> [ascii | binary]

Назначение: Загружает файлы в TFTP-клиент.

Параметры: <source-url>: местонахождение исходных файлов или каталогов, которые требуется скопировать;

<destination-url>: адрес назначения, в которое требуется скопировать исходные файлы или каталоги;

вид полей <source-url> и <destination-url> сильно изменяется в зависимости от конкретного расположения файлов или каталогов.

ascii указывает, что следует использовать стандарт ASCII;

binary указывает, что при передаче файла следует использовать двоичную систему (метод передачи, используемый по умолчанию).

Когда URL соответствует TFTP-адресу, форма команды следующая: **tftp://<ipaddress>/<filename>**, где <ipaddress>: IP-адрес клиента/сервера TFTP, <filename>: имя файла, загружаемого или выгружаемого по TFTP.

Специальные ключевые слова для имени файла:

Ключевые слова	Адреса источника или назначения
running-config	Файлы текущей рабочей конфигурации
startup-config	Файлы конфигурации начальной загрузки
nos.img	Системные файлы
nos.rom	Системные файлы начальной загрузки

Режим конфигурирования: Привилегированный режим

Примеры: Скопировать образ системы из флэш-памяти на TFTP-сервер с адресом 10.1.1.1.

```
Switch#copy nos.img tftp://10.1.1.1/nos.img
```

Скопировать образ с именем nos.img с TFTP-сервера с адресом 10.1.1.1.

```
Switch#copy tftp://10.1.1.1/nos.img nos.img
```

Сохранить файлы рабочей конфигурации

```
Switch#copy running-config startup-config
```

См. также:

Команда	Описание
write	Сохраняет текущие настройки параметров во флэш-памяти

1.5.3 ftp-dir

Синтаксис: ftp-dir <ftp-server-url>

Назначение: Просмотр содержимого директории на FTP-сервере.

Режим конфигурирования: Привилегированный режим.

Параметры: <ftp-server-url>: параметры подключения к FTP-серверу. Параметр <ftp-server-url> имеет формат ftp://<username>:<password>@<ipaddress>, где <username> - имя пользователя для подключения к FTP-серверу, <password> - пароль, <ipaddress> - IP-адрес FTP-сервера.

Пример:

```
Switch#ftp-dir ftp://TestUser:test@192.168.0.105
220-FileZilla Server version 0.9.34 beta
331 Password required for TestUser
230 Logged on
```

```

200 Port command successful
150 Opening data channel for directory list.
226 Transfer OK
Recv total 102 bytes
nos.img
test.cfg
Switch#Close ftp client.

```

1.5.4 ftp-server enable

Синтаксис: `ftp-server enable`

`no ftp-server enable`

Назначение: Запускает FTP-сервер. Отмена команды “`no ftp-server enable`” выключает FTP-сервер и прекращает регистрацию пользователей по FTP.

Значение по умолчанию: FTP-сервер по умолчанию не запущен.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Когда функция FTP-сервера включена, коммутатор может выполнять функции ftp-клиента.

FTP-сервер по умолчанию не запущен.

Пример: Включить FTP-сервер.

```
Switch(config)#ftp-server enable
```

См. также:

Команда	Описание
<code>ip ftp</code>	Позволяет задать имя пользователя и пароль для доступа по ftp

1.5.5 ftp-server timeout

Синтаксис: `ftp-server timeout <seconds>`

Назначение: Устанавливает время простоя соединения

Параметры: `<seconds>`: пороговое время простоя (в секундах) для FTP-соединения, диапазон значений - от 5 до 3600.

Значение по умолчанию: По умолчанию системой установлено 600 секунд.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Когда время простоя соединения передачи данных по FTP превысит это предельное значение, FTP-соединение будет отключено.

Пример: Задать пороговое время простоя 100 секунд.

```
Switch(config)#ftp-server timeout 100
```

1.5.6 ip ftp

Синтаксис: `ip ftp username <username> password [type {0 | 7}] <password>`

Назначение: Позволяет задать имя пользователя и пароль для доступа по ftp. Отмена команды `no ip ftp username <username>` удаляет соответствующие имя пользователя и пароль.

Параметры: `<user-name>`: имя пользователя для FTP-доступа, длина имени — не более 16 символов. Параметр `0 | 7`, если выбран `0` — пароли не будут шифроваться, если выбрано `7` — будет применяться шифрование паролей.

`<password>`: пароль для FTP-доступа, длина пароля — не более 16 символов.

Настройки по умолчанию: Используется анонимный доступ по FTP.

Режим конфигурирования: Глобальный режим конфигурирования

Примеры: Сконфигурировать имя пользователя Switch для FTP-доступа, пароль superuser.

```
Switch(config)#ip ftp username Switch password 0 superuser
```

1.5.7 show ftp

Синтаксис: show ftp

Назначение: Выводит на дисплей параметры конфигурирования FTP-сервера.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Не задействовано.

Пример:

```
Switch#show ftp
timeout :600 seconds
```

Параметры	Описание
timeout	Время таймера

1.5.8 show tftp

Синтаксис: show tftp

Назначение: Выводит на дисплей параметры конфигурирования TFTP-сервера.

Значение по умолчанию: Не задействовано.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch#show tftp
timeout : 600 seconds
Retry Times : 5
```

Параметры	Описание
Timeout	Время таймера
Retry Times	Число попыток

1.5.9 tftp-server enable

Синтаксис: tftp-server enable

no tftp-server enable

Назначение: Запускает TFTP-сервер. Отмена команды “no ftp-server enable” выключает TFTP-сервер.

Значение по умолчанию: По умолчанию TFTP-сервер не включен.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Когда TFTP-сервер включен, коммутатор может также использоваться и как TFTP-клиент.

Пример: Включить TFTP-сервер.

```
Switch(config)#tftp-server enable
```

1.5.10 tftp-server retransmission-number

Синтаксис: tftp-server retransmission-number <number>

Назначение: Позволяет задать предельное число попыток передачи данных по протоколу TFTP.

Параметры: <number>: максимальное число попыток, от 1 до 20.

Значение по умолчанию: Установлено число попыток, равное 5.

Режим конфигурирования: Глобальный режим конфигурирования

Пример: Установить предельное число попыток равным 10.

```
Switch(config)#tftp-server retransmission-number 10
```

1.5.11 tftp-server transmission-timeout

Синтаксис: tftp-server transmission-timeout <seconds>

Назначение: Позволяет задать время таймера для передачи данных по протоколу TFTP.

Параметры: <seconds>: значение времени таймера в секундах, в пределах от 5 до 3600 секунд.

Значение по умолчанию: 600 секунд.

Режим конфигурирования: Глобальный режим конфигурирования

Пример: Установить время таймера равным 60 секундам.

```
Switch(config)#tftp-server transmission-timeout 60
```

2 Команды для настройки стекирования

2.1.1 clear cluster nodes

Синтаксис: `clear cluster nodes [nodes-sn <candidate-sn-list> | mac-address<mac-addr>]`

Назначение: Очищает узлы в списке коммутаторов-кандидатов, обнаруженных управляющим коммутатором.

Параметры: **<candidate-sn-list>**: номера коммутаторов-кандидатов, в пределах от 1 до 256. Может быть указано несколько коммутаторов-кандидатов (более одного).

<mac-address>: mac-адрес коммутаторов (в том числе всех коммутаторов-кандидатов, коммутаторов-членов и других коммутаторов).

Значение по умолчанию: При вводе команды без параметров будет очищена информация о всех коммутаторах.

Режим конфигурирования: Привилегированный режим

Описание: После выполнения этой команды, информация о соответствующем узле удаляется из списка, хранящегося на управляющем коммутаторе. Через 30 секунд коммутатор обновит топологию стека и вновь добавит этот узел. Однако после того, как узел будет добавлен, идентификатор коммутатора-кандидата может измениться. Команда может быть выполнена только на управляющем коммутаторе.

Пример: Очистить все списки коммутаторов, обнаруженных управляющим коммутатором.
`Switch#clear cluster nodes`

2.1.2 cluster auto-add

Синтаксис: `cluster auto-add`

`no cluster auto-add`

Назначение: После выполнения этой команды на управляющем коммутаторе, новые обнаруженные коммутаторы-кандидаты будут автоматически добавлены в стек, как коммутаторы-члены стека. Отмена команды "**no cluster auto-add**" выключает эту функцию.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: Функция выключена.

Это означает, что коммутаторы-кандидаты не будут автоматически добавляться в стек.

Описание: После выполнения этой команды на управляющем коммутаторе, управляющий коммутатор будет автоматически добавлять коммутаторы-кандидаты в стек в качестве коммутаторов-членов стека.

Пример: Включить на управляющем коммутаторе функцию автоматического добавления.
`Switch(config)#cluster auto-add`

2.1.3 cluster commander

Синтаксис: `cluster commander [<cluster-name>]`

`no cluster commander`

Назначение: Позволяет включить управляющий коммутатор, создать стек, изменить имя стека. Отмена команды "**no cluster commander**" позволяет удалить стек.

Параметры: **<cluster-name>**: имя стека, длина не более 32 символов.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: Управляющий коммутатор не задан, имя стека не задано.

Описание: Команда позволяет задать коммутатор, как управляющий, и создать стек, состоящий из коммутаторов, не являющихся управляющими. После того, как коммутатор задан, как управляющий, имя стека не может быть изменено. Для того, чтобы стало возможно изменить имя стека, необходимо сначала ввести команду "**no cluster commander**".

Пример: Установить коммутатор в качестве управляющего. Идентификатор стека ZES:
`Switch(config)#cluster commander zes`

2.1.4 cluster ip-pool

Синтаксис: `cluster ip-pool <commander-ip>`

`no cluster ip-pool`

Назначение: Позволяет настроить частный IP-адрес пула коммутаторов-членов стека.

Параметры: `<commander-ip>`: головной IP-адрес адресного пула управляющего коммутатора стека, имеет формат 10.x.x.x; пул адресов должен быть достаточно большим (он должен поддерживать 128 коммутаторов-членов). Это требование означает, что последний байт адресов пула должен быть меньше 126 ($254 - 128 = 126$).

После конфигурирования управляющего коммутатора, изменять IP-адрес пула не следует.

Изменить этот адрес можно только после выполнения команды `"no cluster commander"`.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: Задан адрес пула 10.254.254.1.

Описание: Когда коммутаторы-кандидаты становятся членами стека, управляющий коммутатор назначает каждому из них частный IP-адрес для связи в стеке. Управляющий коммутатор использует этот адрес для управления и обслуживания коммутаторов-членов. Команда может быть выполнена только не на управляющем коммутаторе. После того, как стек сконфигурирован, пользователи не смогут изменить IP-адрес пула адресов.

Пример: Установить частный IP-адрес пула, используемый коммутаторами-членами стека равным 10.254.254.10.

```
Switch(config)#cluster ip-pool 10.254.254.10
```

2.1.5 cluster keepalive interval

Синтаксис: `cluster keepalive interval <second>`

`no cluster keepalive interval`

Назначение: Позволяет установить интервал времени передачи сообщений keepalive внутри стека.

Параметры: `<second>`: значение интервала времени передачи сообщений keepalive внутри стека, в пределах от 3 до 30 с.

Значение по умолчанию: 30 секунд.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Введенная с управляющего коммутатора, эта команда позволяет установить интервал времени, через который передаются сообщения keepalive внутри стека. Эта информация по TCP-протоколу передается на все коммутаторы-члены стека. Если команда введена не для управляющего коммутатора, введенное значение интервала времени передачи сообщений будет сохранено, но не будет использоваться до тех пор, пока этот коммутатор не станет управляющим. До наступления этого события будет использоваться интервал передачи сообщений keepalive внутри стека, установленный действующим управляющим коммутатором. В течение каждого интервала передачи сообщений keepalive внутри стека, управляющий коммутатор будет рассылать по стеку сообщения DP. Коммутаторы-члены будут отвечать на принятые сообщения DP сообщениями DR. Отмена команды `"no cluster keepalive interval"` будет восстанавливать значение интервала передачи сообщений поддержки работы стека, заданное по умолчанию.

Пример: Установить интервал передачи сообщений keepalive внутри стека равным 10 с.

```
Switch(config)#cluster keepalive interval 10
```

2.1.6 cluster keepalive loss-count

Синтаксис: `cluster keepalive loss-count <loss-count>`

`no cluster keepalive loss-count`

Назначение: Позволяет задать предельно допустимое число сообщений keepalive внутри стека, которые могут быть потеряны.

Параметры: `<loss-count>`: предельно допустимое число сообщений keepalive внутри стека, которые могут быть потеряны, в пределах от 1 до 10.

Значение по умолчанию: 3.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Введенная с управляющего коммутатора, эта команда позволяет распространить установленное предельно допустимое число сообщений keepalive внутри стека, которые могут быть потеряны, на все коммутаторы-члены, подключенные к управляющему коммутатору.

Если команда введена не для управляющего коммутатора, введенное значение будет сохранено, но не будет использоваться до тех пор, пока этот коммутатор не станет управляющим. До наступления этого события будет использоваться предельно допустимое число сообщений keepalive внутри стека, которые могут быть потеряны, установленное действующим управляющим коммутатором. Управляющий коммутатор после отправки каждого сообщения DP увеличивает счетчик потерянных сообщений каждого коммутатора на 1, а после того, как примет от этого коммутатора сообщение DR, очищает счетчик.

Когда счетчик потерянных сообщений достигает установленного значения (по умолчанию 3) т. е. сообщения DR не приняты, управляющий коммутатор удаляет коммутатор из списка кандидатов. Если в течение некоторого времени коммутатор-член стека не мог принять сообщения DP от управляющего коммутатора и число не принятых сообщений DP превысило предельно допустимое число потерянных сообщений, коммутатор-член станет коммутатором-кандидатом.

Отмена команды "`no cluster keepalive loss-count`" восстанавливает значение предельно допустимое число потерянных сообщений, заданное по умолчанию.

Пример: Установить значение предельно допустимое число потерянных сообщений keepalive внутри стека равным 5.

```
Switch(config)#cluster keepalive loss-count 5
```

2.1.7 cluster member

Синтаксис: `cluster member {nodes-sn <candidate-sn-list> | mac-address <mac-addr> [id <member-id>]}`

`no cluster member {id <member-id> | mac-address <mac-addr>}`

Назначение: На управляющем коммутаторе добавляет коммутаторы-кандидаты в стек. Отмена команды "`no cluster member {id <member-id> | mac-address <mac-addr>}`" удаляет указанный коммутатор-член из стека и делает его коммутатором-кандидатом.

Параметры: `nodes-sn`: все коммутаторы-члены стека, имеющиеся в списке; каждому коммутатору-члену назначен номер узла, информацию о котором можно просмотреть, введя команду "`show cluster candidates`".

Одновременно могут быть добавлены один или несколько коммутаторов-кандидатов.

Значение `<candidate-sn-list>` должно быть в пределах от 1 до 256.

`mac-address`: MAC-адрес коммутатора-кандидата;

`<member-id>`: идентификатор (ID) коммутатора-кандидата, становящегося коммутатором-членом, в пределах от 1 до 128;

`nodes-sn` является автоматически создаваемым номером узла; после того, как коммутатор-кандидат станет коммутатором-членом стека, `nodes-sn` может измениться.

Коммутаторы-члены, добавленные этой командой, имеют те же свойства, что и добавленные в режиме добавления по mac-адресам (они имеют одинаковые конфигурационные файлы).

Если в качестве коммутатора-члена добавляется несколько коммутаторов, указание member-id запрещено. Это же правило действует и в режиме nodes-sn.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: После выполнения этой команды, (управляющий) коммутатор добавит коммутаторы, указанные в <nodes-sn> или в <mac-address> в стек. В одной команде можно указать несколько коммутаторов (используя символы-разделители '-' или ';'). В стеке коммутатор может быть только либо коммутатором-членом, либо управляющим коммутатором. При выполнении команды не на управляющем коммутаторе будет выведено сообщение об ошибке.

Пример: На управляющем коммутаторе добавить в стек коммутатор-кандидат с номером в списке 1. На управляющем коммутаторе добавить в стек коммутатор-кандидат с mac-адресом 11-22-33-44-55-66 (сделать его коммутатором-членом), присвоить ему member-id 5.

```
Switch(config)#cluster member nodes-sn 1
```

```
Switch(config)#cluster member mac-address 11-22-33-44-55-66 id 5
```

2.1.8 cluster member auto-to-user

Синтаксис: cluster member auto-to-user

Назначение: После ввода команды "no cluster auto-add" все коммутаторы-члены будут удалены. Чтобы сохранить их, пользователям необходимо сделать автоматически добавленные коммутаторы, коммутаторами, добавленными вручную.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: После выполнения этой команды, автоматически добавленные коммутаторы будут считаться коммутаторами, добавленными вручную.

Пример: Сделать автоматически добавленные коммутаторы-члены, коммутаторами-членами, добавленными вручную.

```
Switch(config)#cluster member auto-to-user
```

2.1.9 cluster reset member

Синтаксис: cluster reset member [id <member-id> | mac-address <mac-addr>]

Назначение: Введенная для управляющего коммутатора, эта команда позволяет перезагрузить коммутатор-член.

Параметры: <member-id>: идентификатор (ID) коммутатора-члена в стеке, в пределах от 1 до 128.

Для задания коммутаторов-членов в <member-id> можно использовать символы "-" или ";". Если значение опущено, будут перезагружены все коммутаторы.

Значение по умолчанию: Перезагрузка всех коммутаторов.

Режим конфигурирования: Привилегированный режим

Описание: Находясь на управляющем коммутаторе, пользователи могут использовать эту команду для перезагрузки коммутаторов-членов.

Если команда введена для коммутатора, не являющегося управляющим, на дисплей будет выведено сообщение об ошибке.

Пример: С управляющего коммутатора перезагрузить коммутатор-член стека с номером 1.

```
Switch#cluster reset member id 1
```

2.1.10 cluster run

Синтаксис: `cluster run [key <WORD>][vid <VID>]`

`no cluster run`

Назначение: Включает режим стекирования. Отмена команды “**no cluster run**” выключает режим стекирования

Параметры: **key:** Все ключи одного стека должны быть одинаковыми, длина – не более 16 символов.

vid: идентификатор vlan стека, в пределах 1-4094.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: Стекирование выключено, значение key: NULL(0) vid: 1.

Описание: Эта команда используется для начальной работы со стеками.

Необходимо включить стекирование, перед тем как вводить команды настройки стека..

Рекомендуется выделять для стека отдельный vlan (например, vlan 100).

Примечание: Если задан vlan стека, то протоколы маршрутизации должны быть выключены на интерфейсах 3-го уровня, во избежание передачи маршрутов внутри стека.

Пример: Выключить поддержку стеков на локальном коммутаторе.
Switch (config)#no cluster run

2.1.11 cluster update member

Синтаксис: `cluster update member <member-id> <src-url> <dst-filename> [ascii |binary]`

Назначение: Введенная с управляющего коммутатора, эта команда позволяет удаленно обновить коммутатор-член стека.

Параметры: **<member-id>:** идентификатор (ID) коммутатора-члена в стеке, в пределах от 1 до 128. Для задания коммутаторов-членов в **<member-id>** можно использовать символы “-” или “;”.

<src-url>: местонахождение файла-источника, который требуется скопировать;

<dst-filename>: путь к месту назначения копируемого файла во флэш-памяти коммутатора;

ascii: файл будет передан в формате ASCII;

binary: файл будет передан в двоичном формате.

Если **<src-url>** является адресом FTP, формат его подобен следующему: `ftp://<username>:<password>@<ipaddress>/<filename>`. Здесь **<username>**: имя пользователя FTP, **<password>** пароль на доступ к FTP, **<ipaddress>**: IP-адрес FTP-сервера, **<filename>**: имя файла.

Если **<src-url>** является адресом TFTP, формат его подобен следующему: `tftp://<ipaddress>/<filename>`. Здесь **<ipaddress>**: IP-адрес TFTP-сервера **<filename>**: имя файла.

Специальные ключевые слова для имени файла:

Ключевое слово	Адреса источника или назначения
startup-config	Файл конфигурирования начальной загрузки
nos.img	Системный файл

Режим конфигурирования: Привилегированный режим

Описание: Управляющий коммутатор посылает по удаленному доступу (через TCP-соединение) на коммутатор-член команду обновления. Коммутатор-член выполняет обновление и перезагружается. Если команда введена в коммутатор, не являющийся управляющим, на дисплей будет выведено сообщение об ошибке. Если пользователям необходимо обновить несколько коммутаторов, необходимо, чтобы все эти коммутаторы были одного типа, в противном случае может быть сбой из-за попытки загрузки в них неподходящих файлов IMG.

Пример: С управляющего коммутатора послать по удаленному доступу на коммутатор-член стека с идентификатором 1 команду обновления, используя в качестве **src-url** `ftp://admin:admin@192.168.1.1/nos.img` и в качестве **dst-url** `nos.img`.
Switch#cluster update member 1 ftp://admin:admin@192.168.1.1/nos.img nos.img

2.1.12 debug cluster

Синтаксис: `debug cluster {application | statemachine | tcp}`

`no debug cluster {application | statemachine | tcp}`

Назначение: Выводит на дисплей отладочные сообщения кластера.

касающиеся передачи данных между коммутаторами, когда они являются коммутаторами-членами стека, либо управляющим коммутатором. Отмена команды “**no debug cluster application**” прекращает вывод отладочных сообщений.

Параметры: **application:** вывод отладочной информации о конфигурировании кластера посредством SNMP и WEB;

statemachine: вывод отладочной информации при изменении статуса коммутатора;

tcp: вывод отладочной информации о tcp-соединениях между членами кластера.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch#debug cluster statemachine
```

2.1.13 debug cluster packets

Синтаксис: `debug cluster packets {DP | DR | CP} {receive | send}`

`no debug cluster packets {DP | DR | CP} {receive | send}`

Назначение: Включает для администратора стека вывод отладочных сообщений о приеме и отправке пакетов. Отмена команды “**no debug cluster packets {DP | DR | CP} {receive | send}**” прекращает вывод соответствующих сообщений.

Параметры: **DP:** Сообщения обнаружения.

DR: Ответные сообщения.

CP: Командные сообщения.

receive: Принятые сообщения.

send: Переданные сообщения.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Включает вывод отладочной информации о сообщениях стека.

Если включена классификация, все сообщения DP, DR и CP (принятые и переданные в стеке) будут выведены на дисплей.

Пример: Включить вывод отладочной информации о принятых сообщениях DP.

```
Switch#debug cluster packets DP receive
```

2.1.14 show cluster

Синтаксис: `show cluster`

Назначение: Используется для отображения информации о стеке.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Пример: Выполнить эту команду на коммутаторах, играющих разные роли.

На управляющем коммутаторе.

```
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: commander
IP pool: 10.254.254.1
Cluster name: zelax
Keepalive interval: 30
Keepalive loss-count: 3
```

```
Auto add: Disabled
Number of Members: 0
Number of Candidates: 3
```

На коммутаторе-члене стека.

```
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: Member
Commander Ip Address: 10.254.254.1
Internal Ip Address: 10.254.254.2
Commamder Mac Address: 00-1a-81-00-18-9d
```

На коммутаторе-кандидате.

```
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: Candidate
```

На коммутаторе с выключенным стекированием.

```
Switch#show cluster
Status: Disabled
```

2.1.15 show cluster members

Синтаксис: `show cluster members [id <member-id> | mac-address <mac-addr>]`

Назначение: Выводит на дисплей информацию о коммутаторах-членах стека.

Эта команда может быть выполнена только на управляющих коммутаторах.

Параметры: **<member-id>**: Идентификатор коммутатора-члена.

<mac-addr>: MAC-адрес CPU коммутатора-члена.

Значение по умолчанию: При вводе команды без параметров будет выведена информация о всех коммутаторах-членах.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Описание: При выполнении этой команды на управляющем коммутаторе будет отображена информация о всех коммутаторах-членах стека.

Пример: Выполнить команду на управляющем коммутаторе, чтобы вывести на дисплей информацию о всех коммутаторах-членах стека.

```
Switch#show cluster members
Member From: User config(U); Auto member(A)
ID      From  Status  Mac Address          Hostname          Description          Internal IP
-----
1       A     Active  00-1a-81-00-1a-ff   Switch            Zelax ZES-2026C Switch10.0.0.2
```

```
Switch#show cluster members id 1
Cluster Members:
ID: 1
Member status: Active(Auto add)
IP Address: 10.0.0.2
Mac Address: 00-1a-81-00-1a-ff
Description: Zelax ZES-2026C Switch
Hostname: Switch
```

2.1.16 show cluster candidates

Синтаксис: `show cluster candidates [nodes-sn <candidate-sn-list> | mac-address<mac-addr>]`

Назначение: Выводит на дисплей статистическую информацию о коммутаторах-кандидатах, зарегистрированных управляющим коммутатором стека.

Параметры: **<candidate-sn-list>**: номер коммутаторов-кандидатов, в пределах от 1 до 256.

Может быть указано несколько коммутаторов-кандидатов (более одного).

<mac-addr>: MAC-адрес коммутатора-члена.

Значение по умолчанию: При вводе команды без параметров будет выведена информация о всех коммутаторах-членах.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Описание: При вводе этой команды для коммутатора на дисплей будет выведена информация о коммутаторах-кандидатах.

Пример: Вывести на дисплей информацию о всех коммутаторах-кандидатах стека.

```
Switch#show cluster candidates
```

```
SN      Mac Address      Description      Hostname
```

2.1.17 show cluster topology

Синтаксис: `show cluster topology [root-sn <starting-node-sn> | nodes-sn<node-sn-list> | mac-address <mac-addr>]`

Назначение: Выводит информацию о топологии стека. Эта команда может быть выполнена только на управляющих коммутаторах.

Параметры: `<starting-node-sn>`: Начальный узел.

`<node-sn-list>`: Sn узла коммутатора.

`<mac-addr>`: MAC-адрес CPU коммутатора.

При вводе команды без параметров на дисплее отображается общая информация о топологии стека.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Описание: При выполнении этой команды для управляющего коммутатора на дисплей будет выведена информация о топологии начиная с указанного начального узла.

Пример: Выполнить команду для управляющего коммутатора для отображения топологии.

```
Switch#show cluster topology
```

```
Role: Commander(CM); Member(M); Candidate(CA); Other Commander(OC); Other Member(OM); NULL(NULL)
```

Level	SN	Description	Hostname	Role	MAC Address	Upstream Localport	Upstream Remoteport	Leaf Node
1	-	Zelax ZES-2026C Switch	Switch	CM	00-1a-81-00-18-9e	-root-	-root-	-
	1	Zelax ZES-2026C Switch	Switch1	M	00-1a-81-00-1a-ff	Eth0/0/24	Eth0/0/24	Y

```
Switch#show cluster topology nodes-sn 1
```

```
Topology role: M
```

```
Member status: active member (auto-add)
```

```
SN: 1
```

```
Mac address: 00-1a-81-00-1a-ff
```

```
Description: Zelax ZES-2026C Switch
```

```
Hostname: Switch
```

```
Upstream local-port: Eth0/0/24
```

```
Upstream node: 00-1a-81-00-18-9e
```

```
Upstream remote-port: Eth0/0/24
```

```
Upstream speed: 100full
```

2.1.18 rcommand commander

Синтаксис: `rcommand commander`

Назначение: Находясь на коммутаторе-члене стека, используйте эту команду для удаленного управления и настройки управляющего коммутатора.

Режим конфигурирования: Привилегированный режим

Описание: Эта команда используется для удаленного конфигурирования управляющего коммутатора. Пройдя аутентификацию, пользователи должны связаться с управляющим коммутатором по telnet. Для выхода из интерфейса настройки коммутатора используйте команду `exit`. Эта команда может быть выполнена только на коммутаторе-члене стека.

Пример: С коммутатора-члена стека войти в интерфейс настройки управляющего коммутатора.

```
Switch#rcommand commander
```

2.1.19 rcommand member

Синтаксис: rcommand member <mem-id>

Назначение: Введенная для управляющего коммутатора, эта команда позволяет удаленно управлять коммутаторами-членами стека.

Параметры: <mem-id>: идентификатор (ID) коммутатора-члена, в пределах от 1 до 128.

Режим конфигурирования: Привилегированный режим

Описание: Войдите на коммутаторе-члене стека в привилегированный режим и настройте этот коммутатор, используя удаленный доступ.

Для выхода из режима настройки коммутатора-члена стека используйте команду "exit".

Так как используется внутренний частный IP-адрес, telnet-аутентификации на коммутаторах-членах не потребуется. Команда может быть выполнена только на управляющем коммутаторе.

Пример: С управляющего коммутатора войти в режим настройки коммутатора-члена с идентификатором 1.

```
Switch#rcommand member 1
```

3 Команды для настройки портов

3.1 Команды для настройки Ethernet-порта

3.1.1 bandwidth

Синтаксис: `bandwidth control <bandwidth> {transmit | receive | both}`
`no bandwidth control`

Назначение: Включает на порту функцию управления скоростью. Отмена команды `no bandwidth control` выключает эту функцию.

Параметры: `<bandwidth>`: скорость в Кбит/с в пределах от 62 до 1000000;

`transmit`: ограничение скорости при передаче данных портом;

`receive`: ограничение скорости при приеме данных портом; когда заданы обе опции, скорость будет ограничиваться и во время передачи, и во время приема данных.

Режим конфигурирования: Режим настройки портов.

Значение по умолчанию: Управление скоростью выключено.

Описание: Если управление скоростью включено и задано ограничение скорости, максимальная скорость интерфейса будет ограничена до значения, установленного этой командой (не более, чем 10/100М).

Пример: Установить скорость передачи 40000 Кбит/с для портов 0/0/1-8.

```
Switch(config)#interface ethernet 0/0/1-8
Switch(Config-If-Port-Range)#bandwidth control 40000 both
```

3.1.2 clear counters interface

Синтаксис: `clear counters interface [{ethernet <interface-list> | vlan <vlan-id> | port-channel <port-channel-number> | <interface-name>}]`

Назначение: Очищает на Ethernet-интерфейсе информацию счетчиков.

Параметры: `<interface-list>`: номер Ethernet-порта;

`<vlan-id>`: номер интерфейса VLAN;

`<port-channel-number>`: номер магистрального интерфейса;

`<interface-name>`: имя интерфейса, например, port-channel 1.

Режим конфигурирования: Привилегированный режим

Значение по умолчанию: Информация счетчиков на Ethernet-интерфейсе не удаляется.

Описание: Если порт не указан, будет очищена статистика всех портов.

Пример: Очистить статистику Ethernet-порта 0/0/1.

```
Switch#clear counters interface ethernet 0/0/1
```

3.1.3 flow control

Синтаксис: `flow control`

`no flow control`

Назначение: Активирует для порта функцию управления потоком. Отмена команды `no flow control` выключает функцию управления потоком для порта.

Режим конфигурирования: Режим настройки портов.

Значение по умолчанию: Управление потоком выключено.

Описание: После того, как функция управления потоком будет включена, порт будет уведомлять передающее устройство о необходимости снизить скорость передачи во избежание потери пакетов, когда принимаемый трафик превышает пропускную способность кэша порта.

Порты коммутатора поддерживают управление потоком IEEE802.3X; порты, работающие в режиме полудуплекса, поддерживают управление потоком методом обратного давления (backpressure). Если управление потоком приводит к серьезной блокировке, коммутатор автоматически начнет управлять HOL (будет отбрасывать некоторые пакеты в очередях COS, которые могут привести к блокировке), чтобы предотвратить значительное снижение производительности сети.

Примечание: Управление потоком использовать не рекомендуется, если пользователем необходима низкоскоростная сеть с малой производительностью, но с малыми потерями пакетов. Когда функция управления потоком включена, скорость и режим дуплекса на обоих концах должны быть одинаковыми.

Пример: Включить функцию управления потоком в портах 0/0/1-8.
Switch(config)#interface ethernet 0/0/1-8
Switch(Config-Port-Range)#flow control

3.1.4 interface ethernet

Синтаксис: interface ethernet <interface-list>

Назначение: Включает режим настройки Ethernet-интерфейса из глобального режима конфигурирования.

Параметры: <interface-list>: номер порта.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Для выхода из режима настройки Ethernet-интерфейса в глобальный режим конфигурирования, введите команду **exit**.

Пример: Включить режим настройки Ethernet-интерфейса для портов 0/0/4-5.
Switch(config)#interface ethernet 0/0/4-5
Switch(Config-Port-Range)#

3.1.5 loopback

Синтаксис: loopback

no loopback

Назначение: Включает тестовую функцию петли для Ethernet-порта. Отмена команды **no loopback** выключает тестирование Ethernet-порта.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Тестовая петля для Ethernet-порта выключена.

Описание: Тестовая петля может использоваться для проверки правильности работы Ethernet-порта. После того, как тестовая петля будет включена, порт установит соединение с самим собой, при этом весь трафик, посылаемый портом, будет приниматься этим же самым портом.

Пример: Включить тестовую петлю для Ethernet-портов 0/0/1-8.
Switch(config)#interface ethernet 0/0/1-8
Switch(Config-If-Port-Range)#loopback

3.1.6 mdi

Синтаксис: mdi {auto | across | normal}

no mdi

Назначение: Позволяет задать типы кабелей, поддерживаемые Ethernet-портом. Отмена команды **no mdi** задает тип кабеля для автоматической идентификации.

Параметры: **auto:** указывает, что следует применять автоматическую идентификацию типа кабеля;

across: указывает, что поддерживаются только кабели с перекрещивающимися парами;

normal: указывает, что поддерживаются только кабели прямого типа.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Задана автоматическая идентификация типа кабеля.

Описание: Рекомендуется использовать автоматическую идентификацию.

Обычно прямой кабель используется для подключения коммутатора к PC, а кабель с перекрещивающимися парами – для соединения двух коммутаторов между собой.

Пример: Для Ethernet -портов 0/0/1-8 задать поддержку кабелей только кроссового типа.

```
Switch(config)#interface ethernet 0/0/1-8
Switch(Config-Port-Range)#mdi across
```

3.1.7 name

Синтаксис: name <string>

no name

Назначение: Позволяет задать имя для указанного порта. Отмена команды **no name** отменяет эту настройку.

Параметр: <string>: символьная строка длиной не более 32 символов.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Имя порта не задано.

Описание: Эта команда помогает в использовании коммутатора, так как пользователь с помощью нее может присвоить портам имена в соответствии с их применением. Например, можно присвоить имя «финансовый отдел» портам 0/0/1-2, так как они используются финансовым отделом, порту 0/0/9 - «технический отдел», так как он используется техническим отделом; имя «сервер» порту 0/0/12, так как он закреплен за сервером (подключен к нему).

В этом случае можно для удобства составить таблицу закрепления портов.

Пример: Для порта 0/0/1-2 задать имя financial

```
Switch(config)#interface ethernet 0/0/1-2
Switch(Config-If-Port-Range)#name financial
```

3.1.8 negotiation

Синтаксис: negotiation {on|off}

Назначение: Включает или выключает функцию автоматического определения параметров для порта 1000Base-FX.

Параметры: **on:** Включает функцию автоматического определения параметров; **off:** выключает функцию автоматического определения параметров.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Функция автоматического определения параметров по умолчанию включена..

Описание: Эта команда применима только к интерфейсу 1000Base-FX.

Команда **negotiation** неприменима к интерфейсам 1000Base-TX и 100Base-TX.

На комбо-порту эта команда применима только к порту 1000Base-FX и неприменима к порту 1000Base-TX.

Для изменения режима автоопределения параметров, скорости и режима дуплекса порта 1000Base-TX используйте вместо этой команды команду **speed-duplex**.

Пример: Порт 25 коммутатора Switch1 подключен к порту 25 коммутатора Switch1, требуется отключить автоопределение параметров на обоих портах.

```
Switch1(config)#interface ethernet0/0/25
Switch1(Config-If-Ethernet0/0/25)#negotiation off
Switch2(config)#interface ethernet0/0/25
Switch2(Config-If-Ethernet0/0/25)#negotiation off
```

3.1.9 port-rate-statistics interval

Синтаксис: port-rate-statistics interval [<interval-value>]

Назначение: Установка интервала сбора статистики скорости передачи данных через порт.

Параметры: **<interval-value>**: интервал сбора статистики, в секундах, в диапазоне от 5 до 600 сек., с шагом 5.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 5 сек. и 5 мин. для сбора статистики.

Пример:

```
Switch(config)#port-rate-statistics interval 20
```

3.1.10 port-scan-mode

Синтаксис: **port-scan-mode {interrupt | poll}**

no port-scan-mode

Назначение: Конфигурирование режима опроса порта.

Параметры: **interrupt**: режим прерывания; **poll**: режим опроса.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Режим опроса.

Описание: Существует два режима реагирования на события up/down порта Ethernet. В режиме прерывания происходит аппаратное прерывание для информирования о изменении состояния порта. В режим еопроса ПО коммутатора производит опрос состояния портов. Режим прерывания обеспечивает наибольшее быстродействия. Время схождения протокола MRPP в ремиже опроса составляет сотни миллисекунд, в режиме прерывания – менее 50 мс.

Пример:

```
Switch(config)#port-scan-mode interrupt
```

3.1.11 rate-suppression

Синтаксис: **rate-suppression {broadcast | brmc | brmcldf | all} <packets>**

no rate-suppression

Назначение: Позволяет задать поток данных, которому разрешено проходить через порт коммутатора. Отмена команды **no rate-suppression** разрешает проходить через порт всем потокам (на скорости работы линии).

Параметры: **broadcast**: broadcast-поток, **brmc**: broadcast- и multicast-потоки, **brmcldf**: broadcast-, multicast-, и DLF-потоки, **all**: все потоки.

<packets>: предельное число пакетов, от 1 до 1488905.

Единицей измерения потока пакетов является PPS (число пакетов/с).

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Разрешено прохождение всех потоков данных на скорости работы линии.

Описание: Эта команда дает пользователям возможность подавить потоки данных некоторых типов и уменьшить снижение производительности коммутатора, возникающее из-за обработки лишних данных. Если VLAN не сконфигурированы, все порты коммутатора работают в одном и том же broadcast-домене и это в значительной степени определяет производительность коммутатора. Используя эту команду с параметром **broadcast**, пользователи могут защитить коммутатор от broadcast-шторма. Выбор разрешенной скорости broadcast-потока 1000kps означает, что если скорость принимаемого потока больше этого значения, то за 1 секунду будет приниматься только 1000 кбит пакетных данных, остальные пакеты будут отброшены.

Пример: Разрешить для порта 1-8 прохождение broadcast-пакетов на скорости не более 1000 кбит/с.

```
Switch(config)#interface ethernet 0/0/1-8  
Switch(Config-If-Port-Range)#rate-suppression broadcast 1000
```

3.1.12 rate-violation

Синтаксис: `rate-violation [broadcast | multicast | unicast | all] <200-2000000>`

`no rate-violation`

Назначение: Включает функцию ограничения скорости приема пакетов, позволяет задать скорость приема пакетов/с. При превышении указанного количества пакетов в секунду порт переходит в состояния, указанное командой **rate-violation control**. Отмена команды **no rate-violation** выключает функцию ограничения скорости приема пакетов.

Параметры: **broadcast:** broadcast-пакеты, **multicast:** multicast-пакеты, **unicast:** unicast-пакеты, **all:** все потоки.

<200-2000000>: разрешенное количество пакетов в секунду.

Режим конфигурирования: Режим настройки интерфейсов

Значение по умолчанию: Скорость приема пакетов не ограничена.

Описание: Команда, в основном, используется для обнаружения прохождения через порт аномальных потоков данных. Например, если аномально большое число broadcast-сообщений обусловлено петлей, причем ухудшается выполнение других задач коммутатора, порт будет выключен, чтобы гарантировать выполнение других задач коммутатора.

Пример: Если пользователи задали для портов 8-10 коммутатора ограничение скорости 10000 пакетов/с и время восстановления порта (recovery time) 1200 с, то когда скорость приема пакетов превысит 10000 пакетов/с порт будет выключен. По истечении 1200 с порт будет включен снова (перейдет в состояние "UP").

```
Switch(config)#interface ethernet 0/0/8-10
Switch(Config-Port-Range)#rate-violation unicast 10000
Switch(Config-Port-Range)#rate-violation control shutdown recovery 1200
```

3.1.13 rate-violation control

Синтаксис: `rate-violation control [shutdown recovery <0-86400> | block]`

`no rate-violation control`

Назначение: Определяет состояние, в которое переходит порт при достижении ограничения, указанного командой **rate-violation**.

Параметры: **shutdown:** порт выключается; **block:** порт блокируется. Этот параметр является взаимоисключающим с функциями STP, MRPP, Loopback detection и ULPP.

<0-86400>: время восстановления после выключения, в секундах. Значение по-умолчанию 300 сек. 0 означает никогда не восстанавливать исходное состояние порта.

Значение по умолчанию: Действия не предусмотрены.

Пример:

```
Switch(config)#interface ethernet 0/0/8-10
Switch(Config-Port-Range)#rate-violation unicast 10000
Switch(Config-Port-Range)#rate-violation control shutdown recovery 1200
```

3.1.14 show interface

Синтаксис: `show interface [vlan <vlan-id> | ethernet <interface-number> | port-channel <port-channel-number> | <interface-name>] [detail]`

Назначение: Позволяет вывести на дисплей информацию для порта уровня 2 или 3.

Параметры: **<vlan-id>:** номер интерфейса VLAN, в пределах от 1 до 4094.

<interface-number>: номер Ethernet-порта.

<port-channel-number>: номер агрегированного интерфейса.

<interface-name>: имя интерфейса, например, port-channel1.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Описание: Для Ethernet-порта по этой команде будет выведена на дисплей информация о скорости работы порта, режиме дуплекса, состоянии порта (обусловленного управлением скоростью), ограничению скорости для борьбы с broadcast-штормом, статистике пакетов. Для интерфейсов vlan на дисплей будет выведена информация о MAC-адресе порта, его IP-адресе, статистики пакетов. Для агрегированного порта на дисплей будут выведены: скорость работы порта, режим дуплекса, состояние порта (обусловленное управлением скоростью), ограничение скорости для борьбы с broadcast-штормом, статистика пакетов.

Если порт не указан, будет выведена информация для всех портов коммутатора.

Пример: Вывести на дисплей информацию для интерфейса VLAN 1.

```
Switch#show interface vlan 1
Vlan1 is up, line protocol is up, dev index is 3001
Device flag 0x1003(UP BROADCAST MULTICAST)
IPv4 address is:
 192.168.2.24      255.255.255.0    (Primary)
 10.0.0.1         255.255.255.0    (Secondary)
VRF Bind: Not Bind
Hardware is EtherSVI, address is 00-1a-81-00-18-9d
MTU is 1500 bytes , BW is 0 Kbit
Encapsulation ARPA, loopback not set
5 minute input rate 5 bytes/sec, 0 packets/sec
5 minute output rate 130 bytes/sec, 1 packets/sec
The last 5 second input rate 27 bytes/sec, 0 packets/sec
The last 5 second output rate 171 bytes/sec, 2 packets/sec
Input packets statistics:
  Input queue 0/300, 0 drops
 26690505 packets input, 318871689 bytes, 0 no buffer
 0 input errors, 0 CRC, 0 oversize, 0 undersize
 0 jabber, 0 fragments
Output packets statistics:
 37085760 packets output, 2200230030 bytes, 0 underruns
 0 output errors, 0 collisions
```

Вывести на дисплей информацию для порта 0/0/1:

```
Switch#show interface ethernet 0/0/1
Ethernet0/0/1 is down, line protocol is down
Ethernet0/0/1 is layer 2 port, alias name is (null), index is 1
Hardware is Fast-Ethernet, address is 00-1a-81-00-18-9e
PVID is 1
MTU 1500 bytes, BW 100000 Kbit
Encapsulation ARPA, Loopback not set
Auto-duplex, Auto-speed
FlowControl is off, MDI type is auto
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
The last 5 second input rate 0 bytes/sec, 0 packets/sec
The last 5 second output rate 0 bytes/sec, 0 packets/sec
Input packets statistics:
 34091 input packets, 2829848 bytes, 0 no buffer
 34090 unicast packets, 0 multicast packets, 1 broadcast packets
 0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
 0 abort, 0 length error, 0 pause frame
Output packets statistics:
 33874 output packets, 2811802 bytes, 0 underruns
 33873 unicast packets, 0 multicast packets, 1 broadcast packets
 0 output errors, 0 collisions, 0 pause frame
```

3.1.15 shutdown

Синтаксис: shutdown

no shutdown

Назначение: Выключает указанный Ethernet-порт. Отмена команды **no shutdown** включает порт.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Ethernet-порт включен.

Описание: Когда Ethernet-порт выключен, кадры с данными не посылаются в порт, если пользователь введет команду **show interface**, то состояние порта, показанное на дисплее по этой команде, будет "down" (выключен).

Пример: Включить порты 0/0/1-8.

```
Switch(config)#interface ethernet0/0/1-8
Switch(Config-Port-Range)#no shutdown
```

3.1.16 speed-duplex

Синтаксис: **speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | force100-fx [module-type {auto-detected | no-phy-integrated | phy-integrated}] | {{force1g-half | force1g-full} [nonegotiate [master | slave]]}}**

no speed-duplex

Назначение: Позволяет настроить скорость и режим дуплекса портов 100Base-TX, 100Base-TX, 100Base-FX. Отмена команды **no speed-duplex** восстанавливает скорость и режима дуплекса, заданные по умолчанию, например автоматическое согласование параметров порта и режим дуплекса.

Параметры: **auto:** автоматическое согласование скорости;

force10-half: принудительная установка полудуплекса на порту 10Mbps;

force10-full: принудительная установка полного дуплекса на порту 10Mbps;

force100-half: принудительная установка полудуплекса на порту 100Mbps;

force100-full: принудительная установка полного дуплекса на порту 100Mbps;

force100-fx: принудительная установка полного дуплекса на порту 100Mbps;

module-type: тип модуля 100Base-FX;

auto-detected: автоматическое обнаружение;

no-phy-integrated: интегрированный модуль 100Base-TX отсутствует;

phy-integrated: интегрированный модуль 100Base-TX присутствует;

force1g-half: принудительная установка полудуплекса на порту 1000Mbps;

force1g-full: принудительная установка полного дуплекса на порту 1000Mbps;

nonegotiate: отключение автоматического согласования параметров для порта 1000 Mb;

master: принудительная установка для порта 1000Mb режима работы master;

slave: принудительная установка для порта 1000Mb режима работы slave.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Используются автоматическое согласование скорости и режим дуплекса, заданные по умолчанию.

Описание: При настройке скорости и режима дуплекса порта скорость и режим дуплекса должны быть совместимы с удаленным пиром. Если на удаленном порту задано автоматическое согласование, на локальном порту должно быть задано то же самое. Если на удаленном порту настройки заданы в принудительном режиме, именно этот принудительный режим должен использоваться и на локальном порту.

Если на порту 100Mbit/s принудительно задан режим оптического порта, автоматическое согласование не поддерживается и не используется в это же время для медного комбо-порта. 100Gb-порты по умолчанию работают в режиме master, nonegotiate (автоматическое согласование параметров не используется).

Если на одном устройстве установлен режим master, на другом устройстве должен быть задан режим slave. Режим force1g-half пока не поддерживается.

Пример: Соединить порт 1 коммутатора SwitchA с портом 1 коммутатора SwitchB; принудительно установить на них скорость 100 Мбит/с и режим полудуплекса.

```
SwitchA(config)#interface ethernet0/0/1
SwitchA(Config-If-Ethernet0/0/1)#speed-duplex force100-half
SwitchB(config)#interface ethernet0/0/1
SwitchB(Config-If-Ethernet0/0/1)#speed-duplex force100-half
```

3.1.17 combo-forced-mode

Синтаксис: `combo-forced-mode {copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto}`

Назначение: Устанавливает комбинированный режим работы порта (только для комбо-портов).

Параметры: **copper-forced:** принудительно устанавливает использование медного кабеля; **copper-preferred-auto:** при автоопределении типа кабеля приоритет имеет медный кабель; **sfp-forced:** принудительная установка использования оптического кабеля для порта; **sfp-preferred-auto:** при автоопределении типа кабеля приоритет имеет оптический кабель.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Комбинированный режим работы комбо-портов, приоритет имеет оптический кабель.

Описание: Комбинированный режим работы комбо-портов и соединение портов определяют активный комбо-порт. Комбо-порт состоит из одного оптического порта и одного медного порта. Для комбо-портов активным в одно и то же время может быть только один из них (медный или оптический) и только этот порт может нормально посылать или принимать данные. Следует отметить, что команды согласования скорости и режима дуплекса, примененные и для медного, и для оптического порта, не должны конфликтовать.

Пример: Принудительно установить порты 0/0/25, 0/0/26 как оптические.

```
Switch(config)#interface ethernet 0/0/25-26
Switch(Config-Port-Range)#combo-forced-mode sfp-forced
```

3.1.18 virtual-cable-test

Синтаксис: `virtual-cable-test`

Назначение: Позволяет протестировать физические соединения, в которых используются Ethernet-кабели. В результате выполнения этой команды, на дисплее может быть отображено состояние физических соединений, в том числе: `well` (нормальная работа), `short` (короткое замыкание в цепи), `open` (цепь разомкнута), `fail` (сбой теста). Если выдана информация о ненормальной работе соединения, будет указано и место отказа.

Режим конфигурирования: Режим настройки интерфейсов

Настройки по умолчанию: Тестирование физических соединений выключено.

Описание: Для соединений, выполненных кабелем «витая пара», разъемы RJ-45 должны соответствовать стандартам IEEE 802.3, в противном случае пары линий, отображаемые на дисплее, не будут соответствовать реально используемым физическим линиям. Для 100М-портов будут использованы только пары (1, 2) и (3, 6). Показанные результаты будут относиться только к этим двум парам. Если 1000М-порт подключен к 100М-порту, пары (4, 5) и (7, 8) не будут влиять на результирующую информацию. Результирующая информация будет изменяться в зависимости от типа линий витой пары, температуры окружающей среды, рабочего напряжения. Если температура окружающей среды 20 градусов Цельсия и напряжение поддерживается постоянным, длина витой пары ограничена 100 м. Допустимая погрешность +/-2.

Примечание: Следует отметить, что при тестировании интерфейса все соединения данных для указанного интерфейса будут разорваны. Они будут восстановлены и инициализированы спустя 5 — 10 секунд.

Для комбо-портов функция VCT доступна только в режиме медного порта.

Цвета проводов и разбивка кабеля по парам по стандарту EIA/TIA 568A: (1 — бело-зеленый, 2 — зеленый), (3 — бело-оранжевый, 6 — оранжевый), (4 — голубой, 5 — бело-голубой), (7 — бело-коричневый, 8 — коричневый). Цвета проводов и разбивка кабеля по парам по

стандарту EIA/TIA 568B: (1 — бело-оранжевый, 2 — оранжевый), (3 — бело-зеленый, 6 — зеленый), (4 — голубой, 5 — бело-голубой), (7 — бело-коричневый, 8 — коричневый).

Пример: Протестировать соединение «витая пара» 1000М-порта 0/0/25.

```
Switch(config)#interface ethernet 0/0/25
Switch(Config-If-Ethernet0/0/25)#virtual-cable-test
Switch(config-if-ethernet0/0/25)#virtual-cable-test
Interface Ethernet0/0/25:
```

```
-----
Cable pairs      Cable status      Error lenth (meters)
-----
(1, 2)           open              5
(3, 6)           open              5
(4, 5)           open              5
(7, 8)           open              5
```

3.2 Команды для настройки изоляции портов

3.2.1 isolate-port group

Синтаксис: `isolate-port group <WORD>`

`no isolate-port group <WORD>`

Назначение: Позволяет задать группу изолированных портов. Отмена команды `no isolate-port group <WORD>` удаляет группу изолированных портов и выводит из нее все порты.

Параметры: `<WORD>`: имя, идентифицирующее группу, длиной не более 32 символов.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: Нет.

Описание: Пользователи могут в соответствии со своими требованиями создавать различные группы изолированных портов. Например, если необходимо изолировать все downlink-порты в определенном vlan коммутатора, можно создать группу изолированных портов и добавить в нее все downlink-порты из этого vlan. Коммутатор поддерживает не более 16 групп изолированных портов. Если необходимо изменить настройки или конфигурацию группы изолированных портов, следует сначала удалить существующую группу командой отмены `no isolate-port group <WORD>`.

Пример: Создать группу изолированных портов с именем "test".

```
Switch(config)#isolate-port group test
```

3.2.2 isolate-port group switchport interface

Синтаксис: `isolate-port group <WORD> switchport interface [ethernet] <IFNAME>`

`no isolate-port group <WORD> switchport interface [ethernet] <IFNAME>`

Назначение: Добавляет один или несколько портов в группу изолированных портов. Каждый порт, входящий в группу изолированных портов, изолирован от остальных портов группы. Отмена команды `no isolate-port group <WORD> switchport interface [ethernet]` удаляет один или несколько портов из группы изолированных портов. В результате эти порты смогут связываться с остальными портами как обычно.

Если порты, удаленные из группы, продолжают принадлежать другой группе изолированных портов они остаются в той группе изолированными портами.

Если Ethernet-порт является членом агрегированной группы (convergence group), его не следует добавлять в группу изолированных портов и наоборот, порты, входящие в группы изолированных портов не следует добавлять в агрегированные группы портов.

Однако один и тот же порт может быть членом одной или более групп изолированных портов.

Параметры: `<WORD>`: имя, идентифицирующее группу, длиной не более 32 символов.

Если группы с указанным именем не существует, она будет создана. Опция `ethernet` означает, что изолированные порты будут Ethernet-портами. После этой опции можно перечислить

несколько Ethernet-портов, используя символы-разделители ";" и "-". Например, **ethernet 0/0/1;3;4-7;8**.

<IFNAME>: имя интерфейса, например, Ethernet 0/0/1.

Если указано имя интерфейса, параметр Ethernet указывать не требуется.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: Нет.

Описание: В соответствии со своими требованиями, пользователи могут добавлять или удалять Ethernet-порты из группы изолированных портов.

Когда Ethernet-порт является членом нескольких групп изолированных портов (более одной), он будет изолирован от всех остальных портов групп, которым он принадлежит.

Когда порты являются uplink-портами, может быть включена их изоляция. Это означает, что ни один порт, не являющийся uplink-портом, не сможет связаться с uplink-портами.

После того, как все uplink-порты удалены, изоляция портов будет автоматически выключена. В результате все порты смогут связываться друг с другом как обычно.

100M-порты обычно используются для подключения устройств (downlink), как uplink-порты они используются только в специальных случаях.

Пожалуйста, имейте в виду, что 8 из них функционируют, как полная группа. Это означает, что если порт ethernet 0/0/1 сконфигурирован, как uplink-порт, то все порты от ethernet 0/0/1 до ethernet 0/0/8 также будут uplink-портами и будут способны связываться с другими портами. Если порт ethernet 0/0/1 сконфигурирован, как downlink-порт, то порты ethernet 0/0/1 - ethernet 0/0/8 также будут downlink-портами.

Остальные порты также подчиняются этому правилу.

Пример: Добавить Ethernet-порты 0/0/1-2 и 0/0/5 в группу изолированных портов с именем "test".

```
Switch(config)#isolate-port group test switchport interface ethernet 0/0/1-2;  
0/0/5
```

3.2.3 show isolate-port group

Синтаксис: **show isolate-port group [<WORD>]**

Назначение: Выводит на дисплей информацию об изолированных портах, в том числе информацию по всем сконфигурированным группам изолированных портов, а также по всем Ethernet-портам в каждой группе.

Параметры: **<WORD>**: имя, идентифицирующее группу, длина имени – не более 32 символов. Если команда введена без параметров, на дисплей будет выведена конфигурация всех групп изолированных портов.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Значение по умолчанию: Вывод на дисплей информации для всех групп изолированных портов.

Описание: С помощью этой команды пользователи могут просматривать информацию о настройке изоляции портов.

Пример: Вывести на дисплей настройки изоляции портов для группы с именем "test".

```
Switch(config)#show isolate-port group test  
Isolate-port group test  
The isolate-port Ethernet0/0/5 The isolate-port Ethernet0/0/2
```

3.3 Команды для настройки обнаружения петель в портах

3.3.1 loopback-detection control

Синтаксис: **loopback-detection control {shutdown | block| learning}**

no loopback-detection control

Назначение: Позволяет включить функцию управления обнаружением петель на портах. Отмена команды **no loopback-detection control** выключает эту функцию.

Параметры: shutdown: задает в качестве метода управления выключение; это означает, что при обнаружении петли порт будет выключен.

block: задает в качестве метода управления блокирование; это означает, что через порт будет разрешена передача только сообщений bpdu, если обнаружена петля.

learning: выключает метод управления, состоящий в обучении MAC-адресам на порту, сбрасывает принятые сообщения и удаляет MAC-адрес порта.

Значение по умолчанию: Функция управления обнаружением петли выключена.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Если имеется какая-либо петля, операции управления будут выключены спустя некоторое время после включения порта. Если это время задано, то нормальное состояние портов будет восстановлено по истечении соответствующего таймера. Если в качестве метода управления выбрано блокирование, пользователями вручную должна быть установлена связь между объектом и идентификатором vlan.

Пример: Включить функцию обнаружения петель в режиме shutdown на порту ethernet 0/0/2.

```
Switch(config)#interface ethernet 0/0/2
Switch(Config-If-Ethernet0/0/2)#loopback-detection control shutdown
Switch(Config-If-Ethernet0/0/2)#no loopback-detection control
```

3.3.2 loopback-detection specified-vlan

Синтаксис: loopback-detection specified-vlan <vlan-list>

no loopback-detection specified-vlan [<vlan-list>]

Назначение: Позволяет включить функцию обнаружения петель на портах и задать VLAN, которые требуется проверить. Отмена команды **no loopback-detection specified-vlan [<vlan-list>]** выключает функцию обнаружения петель в портах или указанных VLAN.

Параметры: <vlan-list>: список VLAN, которым разрешено использовать порт.

Указанные vlan могут быть проверены на то, не является ли данный порт магистральным.

Эта команда используется для задания списка проверяемых vlan.

Значение по умолчанию: Функция обнаружения петель в портах выключена.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Порт может быть магистральным (trunk) для многих vlan, обнаружение петель может быть реализовано по принципу порт+vlan. Это означает, что объектами обнаружения могут быть указанные vlan в порту. Если порт является портом доступа (access), в порту будет проверяться только один vlan, несмотря на то, что может быть задано множество vlan. Эта функция не поддерживается для Port-channel.

Пример: Включить функцию обнаружения петель на порту ethernet 0/0/2.

```
Switch(config)#interface ethernet 0/0/2
Switch(Config-If-Ethernet0/0/2)#switchport mode trunk
Switch(Config-If-Ethernet0/0/2)#switchport trunk allowed vlan all
Switch(Config-If-Ethernet0/0/2)#loopback-detection specified-vlan 1;3;5-20
Switch(Config-If-Ethernet0/0/2)#no loopback-detection specified-vlan 1;3;5-20
```

3.3.3 loopback-detection interval-time

Синтаксис: loopback-detection interval-time <loopback> <no-loopback>

no loopback-detection interval-time

Назначение: Позволяет задать интервал обнаружения петли. Отмена команды **no loopback-detection interval-time** выключает интервал обнаружения петли.

Параметры: **<loopback>**: интервал обнаружения – время ожидания обнаружения петли обратной связи, в пределах от 5 до 300 секунд. **<no-loopback>**: интервал обнаружения, если петли нет - в пределах от 1 до 30 секунд.

Значение по умолчанию: 5 с, если предполагается, что петля существует, в противном случае – 3 с.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Если петля не обнаружена, интервал обнаружения может быть задан относительно небольшим. Если он слишком мал, то петля может быть не обнаружена, хотя на самом деле существует, что приведет в дальнейшем к неработоспособности сети. Поэтому рекомендуется выбирать достаточно большой интервал времени обнаружения петли, и предположение, что петля будет обнаружена.

Пример: Задать интервал обнаружения петли 35 с, 15 с.
Switch(config)#loopback-detection interval-time 35 15

3.3.4 loopback-detection control-recovery timeout

Синтаксис: loopback-detection control-recovery timeout <0-3600>

Назначение: Эта команда используется для восстановления неконтролируемого состояния по истечении специального интервала времени, когда в порту, находившемся в контролируемом состоянии, была обнаружена петля.

Параметры: **<0-3600>** секунд: время восстановления после контролируемого состояния, 0 – восстановление выполняться не будет.

Значение по умолчанию: Восстановление автоматически не выполняется.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Когда в порту обнаружена петля и он работает в контролируемом режиме, порт находится в этом режиме постоянно и восстановления не происходит. Порт не будет посылать пакеты для обнаружения режима выключения, однако он будет посылать пакеты обнаружения петли, чтобы установить в каком режиме работает петля – в режиме блокирования или в режиме обучения. Если задано время восстановления, то нормальное состояние портов будет восстановлено по истечении соответствующего таймера. Время восстановления является полезным параметром, позволяющим выключить режим контроля. Однако порт может продолжать обнаруживать петлю в других режимах, так что эту команду лучше не использовать.

Примеры: Включить автоматическое восстановление режима управления обнаружением петли по истечении 30 с.
Switch(config)#loopback-detection control-recovery timeout 30

3.3.5 show loopback-detection

Синтаксис: show loopback-detection [interface <interface-list>]

Назначение: Если команда введена без параметров, на дисплей будет выведена информация о состоянии обнаружения петель во всех портах. Если заданы параметры, будет выведена информация только для указанных портов.

Параметры: **<interface-list>**: список портов, при указании портов можно использовать символы-разделители ";", "-"; . Например, ethernet 0/0/1.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Описание: Позволяет вывести на дисплей состояние и результаты обнаружения петель в портах.

Пример: Показать состояние обнаружения петли в порту 4.
Switch(config)#show loopback-detection interface Ethernet 0/0/4
loopback detection config and state information in the switch!

PortName	Loopback Detection	Control Mode	Is Controlled
Ethernet0/0/4	Disable	No	No

3.3.6 debug loopback-detection

Синтаксис: debug loopback-detection

Назначение: Включает вывод отладочной информации обнаружения петли в порту – она будет формироваться при приеме и передаче сообщений и смене состояния.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим

Значение по умолчанию: Вывод отладочной информации выключен.

Описание: Выводит на дисплей информацию об отправке и приеме сообщений, об изменениях состояния.

Пример:

```
Switch#debug loopback-detection
%Jan 01 03:29:18 2006 Send loopback detection probe packet:dev
Ethernet0/0/10, vlan id 1
%Jan 01 03:29:18 2006 Send loopback detection probe packet:dev Ethernet
0/0/10, vlan id 2
```

3.4 Команды для настройки функции ULDP

3.4.1 uldp enable

Синтаксис: uldp enable

Назначение: Включает функцию ULDP. Введенная в глобальном режиме конфигурирования эта команда глобально включает функцию ULDP. Введенная в режиме настройки интерфейсов, эта команда включает функцию ULDP в порту.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Значение по умолчанию: Функция ULDP выключена.

Описание: Функцию ULDP можно включить в порту только в том случае, если она до этого включена в глобальном режиме конфигурирования. Если функция ULDP включена в глобальном режиме конфигурирования, она будет оказывать влияние на работу всех оптических портов. Для медных и оптических портов: после того, как функция ULDP включена в глобальном режиме конфигурирования, эту команду следует ввести и в режиме настройки интерфейсов. Только тогда функция ULDP будет работать в портах.

Пример: Включить функцию ULDP в глобальном режиме конфигурирования.

```
Switch(config)#uldp enable
```

3.4.2 uldp disable

Синтаксис: uldp disable

Назначение: Выключает функцию ULDP.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Значение по умолчанию: функция ULDP выключена.

Описание: Если функция ULDP выключена в глобальном режиме конфигурирования, она будет выключена и во всех портах.

Пример: Выключить функцию ULDP в глобальном режиме конфигурирования.

```
Switch(config)#uldp disable
```

3.4.3 uldp hello-interval

Синтаксис: uldp hello-interval <integer>

no uldp hello-interval

Назначение: Используется для задания интервала времени отправки сообщений hello функции ULDP. Отмена команды **no uldp hello-interval** восстанавливает интервал времени отправки сообщений hello, заданный по умолчанию.

Параметры: Интервал отправки сообщений hello, в пределах от 5 до 100 с, по умолчанию 10 с.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: 10 с.

Описание: Интервал отправки сообщений hello возможно задать только в том случае, когда функция ULDP включена в глобальном режиме конфигурирования. Значение интервала должно быть в пределах от 5 до 100 с.

Пример: Задать интервал отправки сообщений hello равным 12 с.
`Switch(config)#uldp hello-interval 12`

3.4.4 uldp aggressive-mode

Синтаксис: `uldp aggressive-mode`

no uldp aggressive-mode

Назначение: Позволяет настроить функцию ULDP для работы в агрессивном режиме. Отмена команды **no uldp aggressive-mode** восстанавливает настройки нормального режима работы.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Значение по умолчанию: Нормальный режим работы.

Описание: Режим работы функции ULDP можно задать только в том случае, если он включен в глобальном режиме конфигурирования. Когда в глобальном режиме конфигурирования включен агрессивный режим ULDP, все существующие оптические порты будут работать в агрессивном режиме. Для того, чтобы агрессивный режим ULDP был установлен в медных и оптических портах, он должен быть включен в режиме настройки интерфейсов.

Пример: Включить агрессивный режим ULDP в глобальном режиме конфигурирования.
`Switch(config)# uldp aggressive-mode`

3.4.5 uldp manual-shutdown

Синтаксис: `uldp manual-shutdown`

no uldp manual-shutdown

Назначение: Позволяет настроить функцию ULDP для работы в режиме выключения вручную. Отмена команды **no uldp manual-shutdown** восстанавливает автоматический режим работы функции ULDP.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: автоматический режим работы.

Описание: Эту команды следует использовать, если функция ULDP уже включена в глобальном режиме конфигурирования.

Пример: Включить в режиме выключения вручную в глобальном режиме конфигурирования.
`Switch(config)# uldp manual-shutdown`

3.4.6 uldp reset

Синтаксис: `uldp reset`

Назначение: Позволяет перезагрузить порт, выключенный функцией ULDP.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Значение по умолчанию: Нет.

Описание: Эта команда возымеет действие только в том случае, если указанный интерфейс выключен функцией ULDP.

Пример: Перезагрузить все порты, выключенные функцией ULDP.
`Switch(config)#uldp reset`

3.4.7 uldp recovery-time

Синтаксис: `uldp recovery-time<integer>`

`no uldp recovery-time`

Назначение: Позволяет задать для ULDP таймер восстановления. Отмена команды `no uldp recovery-time` восстанавливает настройки, заданные по умолчанию.

Параметры: Значение таймера восстановления ULDP. Должно находиться в пределах от 30 до 86400 с.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: 0 с, это означает, что восстановление выключено.

Описание: Если интерфейс выключен функцией ULDP, то по истечении таймера интерфейс будет автоматически включен. Если задан таймер восстановления 0 с, интерфейс включен не будет.

Пример: Установить таймер восстановления 600 с.
`Switch(config)#uldp recovery-time 600`

3.4.8 show uldp

Синтаксис: `show uldp [interface ethernet<interface-name>]`

Назначение: Позволяет вывести на дисплей настройки ULDP глобального режима конфигурирования и информацию о состоянии интерфейсов. Если задан параметр `<interface-name>`, на экран будут выведены настройки ULDP и состояние указанного интерфейса, а также состояния соседних для него интерфейсов.

Параметры: `<interface-name>`: имя интерфейса.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Значение по умолчанию: Нет.

Описание: Если команда введена без параметров, на дисплей будут выведены настройки ULDP для глобального режима конфигурирования. Если указано имя интерфейса, то наряду с настройками ULDP для глобального режима конфигурирования, будет отображена информация об указанном интерфейсе и интерфейсах, являющихся для него соседними.

Пример: Вывести на дисплей настройки ULDP для глобального режима конфигурирования.
`Switch(config)#show uldp`

3.4.9 debug uldp fsm interface ethernet

Синтаксис: `debug uldp fsm interface ethernet <IFname>`

`no debug uldp fsm interface ethernet <IFname>`

Назначение: Позволяет включить вывод отладочной информации ULDP для указанного интерфейса. Отмена команды `no debug uldp fsm interface ethernet <IFname>` прекращает вывод отладочной информации.

Параметры: `<IFname>`: имя интерфейса.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Вывод отладочной информации выключен.

Описание: Эту команду можно использовать для вывода на дисплей информации об изменениях состояний указанных в команде интерфейсов.

Пример: Вывести информацию об изменениях состояния интерфейса ethernet 0/0/1.
Switch#debug uldp fsm interface ethernet 0/0/1

3.4.10 debug uldp error

Синтаксис: debug uldp error

no debug uldp error

Назначение: Включает вывод на дисплей сообщений об ошибках функции ULDP. Отмена команды **no debug uldp error** выключает вывод на дисплей сообщений об ошибках.

Параметр: Нет.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Вывод на дисплей сообщений об ошибках функции ULDP выключен.

Описание: Команда используется для вывода на дисплей сообщений об ошибках функции ULDP.

Пример: Вывести на дисплей сообщения об ошибках.
Switch#debug uldp error

3.4.11 debug uldp event

Синтаксис: debug uldp event

no debug uldp event

Назначение: Позволяет включить вывод на дисплей отладочных сообщений о событиях ULDP. Отмена команды **no debug uldp event** выключает вывод на дисплей отладочных сообщений о событиях ULDP.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Вывод на дисплей отладочных сообщений о событиях ULDP выключен.

Описание: Эту команду можно использовать для вывода на дисплей информации о событиях ULDP всех типов.

Пример: Вывести на дисплей информацию о событиях ULDP.
Switch#debug uldp event

3.4.12 debug uldp packet

Синтаксис: debug uldp packet [receive|send]

no debug uldp packet [receive|send]

Назначение: Включает вывод отладочной информации о пакетах на прием и передачу. После этого выводит информацию о типе интерфейса, принявшего и передавшего пакеты на стороне клиента. Отмена команды **no debug uldp packet [receive|send]** выключает эту функцию.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим

Значение по умолчанию: функция выключена.

Описание: Эта команда используется для вывода на дисплей информации о пакетах, принятых и переданных каждым интерфейсом.
Switch#debug uldp packet receive

3.4.13 debug uldp

Синтаксис: `debug uldp {hello|probe|echo|unidir|all}[receive|send] interface ethernet <IFname>`

`no debug uldp {hello|probe|echo|unidir|all}[receive|send] interface ethernet <IFname>`

Назначение: Позволяет включить вывод на дисплей подробной информации о пакетах.

После включения отображает в интерфейсе терминала подробную информацию о пакетах некоторых типов.

Параметр: <IFname>: Имя интерфейса.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Функция выключена.

Описание: Эта команда используется для отображения подробной информации о пакетах hello, принятых в интерфейсе Ethernet 0/0/1.

```
Switch#debug uldp hello receive interface Ethernet 0/0/1
```

3.5 Команды для настройки LLDP

3.5.1 Ildp enable

Синтаксис: `Ildp enable`

`Ildp disable`

Назначение: Включает функцию LLDP в глобальном режиме конфигурирования. Отмена команды `Ildp disable` выключает функцию LLDP в глобальном режиме конфигурирования.

Параметры: Нет.

Значение по умолчанию: Функция LLDP выключена.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Если функция LLDP включена в глобальном режиме конфигурирования, она будет включена и на каждом порту.

Пример: Включить функцию LLDP коммутатора.
`Switch(config)#lldp enable`

3.5.2 Ildp enable (port)

Синтаксис: `Ildp enable`

`Ildp disable`

Назначение: Включает модуль LLDP в портах в глобальном режиме конфигурирования. Отмена команды `Ildp disable` выключает модуль LLDP в портах.

Параметры: Нет.

Значение по умолчанию: Модуль LLDP портов по умолчанию выключен в режиме настройки интерфейсов.

Режим конфигурирования: Режим настройки интерфейсов

Описание: Когда функция LLDP включена в глобальном режиме конфигурирования, она включена и на каждом порту. Команда используется для выключения функции LLDP в порту, если она не является в нем необходимой.

Пример: Выключить функцию LLDP в порту ethernet 0/0/5 коммутатора.
`Switch(config)#interface ethernet 0/0/5`
`Switch(Config-if-ethernet 0/0/5)#lldp disable`

3.5.3 Ildp mode

Синтаксис: `Ildp mode {send | receive | both | disable}`

Назначение: Позволяет настроить режим работы функции LLDP в порту.

Параметры: **send:** LLDP будет только отправлять сообщения.

receive: LLDP будет только принимать сообщения.

both: LLDP будет и принимать, и отправлять сообщения.

disable: LLDP не будет ни отправлять, ни принимать сообщения.

Значение по умолчанию: Both (функция LLDP будет и принимать, и отправлять сообщения).

Режим конфигурирования: Режим настройки интерфейсов

Описание: Позволяет задать режим работы агента Ildp в порту.

Пример: Задать в порту ethernet 0/0/5 коммутатора состояние "receive".
`Switch(config)#interface ethernet 0/0/5`
`Switch(Config-if-Ethernet 0/0/5)#lldp mode receive`

3.5.4 Ildp tx-interval

Синтаксис: `lldp tx-interval {seconds}`

`no lldp tx-interval`

Назначение: Когда функция LLDP включена, позволяет задать интервал отправки сообщений обновления во все порты. Значение интервала должно быть в пределах от 5 до 32768 с., по умолчанию установлено 30 с.

Параметры: **seconds:** интервал отправки сообщений обновления, в пределах от 5 до 32768 секунд.

Значение по умолчанию: 30 секунд.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Когда задан интервал отправки сообщений LLDP, они могут быть приняты только по истечении этого интервала. Интервал должен быть меньше или равен времени жизни сообщений. Если интервал слишком большой, состояние успеет устареть, при этом слишком часто будут выполняться реконструкции состояния. Если интервал слишком мал, увеличится поток данных в сети и уменьшится пропускная способность порта. Значение времени жизни сообщений рассчитывается путем умножения множителя на интервал отправки сообщений. Максимальное время жизни сообщений составляет 65535 с. Когда используется интервал отправки (tx-interval), заданный по умолчанию и соответствующими командами задана задержка, интервал отправки будет в 4 раза больше задержки, а не тот, что задан по умолчанию (40 с.).

Пример: Установить интервал отправки сообщений 40 с.

```
Switch(config)#lldp tx-interval 40
```

3.5.5 Ildp msgTxHold

Синтаксис: `lldp msgTxHold {value}`

`no lldp msgTxHold`

Назначение: Позволяет задать значение множителя времени жизни сообщений обновления, посылаемых во все порты, когда включена функция LLDP. Значение множителя должно быть в пределах от 2 до 10.

Параметры: **value:** множитель времени жизни, в пределах от 2 до 10.

Значение по умолчанию: 4.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: После того, как задан множитель, время жизни сообщений определяется, как произведение множителя на интервал отправки сообщений. Максимальное значение времени жизни составляет 65535 с.

Пример: Задать множитель для времени жизни сообщений равным 6.

```
Switch(config)#lldp msgTxHold 6
```

3.5.6 Ildp transmit delay

Синтаксис: `lldp transmit delay {seconds}`

`no lldp transmit delay`

Назначение: Так как локальная информация может часто меняться вместе с изменениями условий работы сети, за короткое время может быть послано много сообщений обновления. Поэтому необходима задержка, гарантирующая точность статистик локальной информации. Когда используется задержка, заданная по умолчанию и соответствующими командами задан интервал отправки (tx-interval), задержка отправки будет составлять четвертую часть интервала отправки, она не будет равна той, которая задана по умолчанию (2 с.).

Параметры: **seconds:** задержка отправки, в пределах от 1 до 8192 с.

Значение по умолчанию: 2 с.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Когда постоянно посылаются сообщения, задержка отправки позволяет защитить удаленный хост от большого числа повторных обновлений информации, обусловленных отправкой большого числа сообщений обновления.

Пример: Установить задержку отправки сообщений 3 с.
Switch(config)#lldp transmit delay 3

3.5.7 lldp notification interval

Синтаксис: lldp notification interval {seconds}

no lldp notification interval

Назначение: По истечении интервала уведомления, система проверяет не была ли изменена удаленная таблица. Если таблица изменилась, система отправляет сообщение Trap в управление SNMP.

Параметры: seconds: интервал уведомления, в пределах от 5 до 3600 с.

Значение по умолчанию: 5 с.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: После того, как установлен интервал уведомления, всякий раз, когда обнаружено изменение удаленной таблицы, по истечении интервала уведомления будет посылаться сообщение "trap".

Пример: Установить интервал отправки сообщений Trap равным 20 с.
Switch(config)#lldp notification interval 20

3.5.8 lldp trap

Синтаксис: lldp trap {enable | disable}

Назначение: enable: включает отправку сообщений Trap в указанном порту; disable: выключает отправку сообщений Trap в указанном порту.

Параметры: Нет.

Значение по умолчанию: По умолчанию в портах коммутатора отправка сообщений Trap выключена.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Команда позволяет включить в порту отправку сообщений Trap.

Пример: Включить отправку сообщений Trap на порту ethernet 0/0/5 коммутатора.
Switch(config)#interface ethernet 0/0/5
Switch(Config-if-ethernet 0/0/5)#lldp trap enable

3.5.9 lldp transmit optional tlv

Синтаксис: lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]

no lldp transmit optional tlv

Назначение: Позволяет задать тип опции TLV порта.

Параметры: portDesc: описание порта; sysName: имя системы; sysDesc: описание системы; sysCap: функции системы.

Значение по умолчанию: Сообщения не содержат опции TLV.

Режим конфигурирования: Режим настройки интерфейсов

Описание: Когда задана опция TLV, то каждая опция TLV может присутствовать только единожды в сообщениях.

portDesc – опциональная информация TLV, имя локального порта;

sysName – опциональная информация TLV, имя локальной системы;

sysDesc – опциональная информация TLV, описание локальной системы;

sysCap – опциональная информация TLV, функции локальной системы.

Пример: Задать в порту ethernet 0/0/5 коммутатора отправку информации portDesc и sysCap TLV.

```
Switch(config)#interface ethernet 0/0/5
Switch(Config-if-ethernet 0/0/5)#lldp transmit optional tlv portDesc sysCap
```

3.5.10 lldp neighbors max-num

Синтаксис: lldp neighbors max-num {value}

no lldp neighbors max-num

Назначение: Позволяет задать максимальное число записей в удаленной MIB.

Параметры: value: предельное число записей, от 5 до 500.

Значение по умолчанию: максимальное число записей в удаленной MIB равно 100.

Режим конфигурирования: Режим настройки интерфейсов

Описание: Позволяет задать максимальное число записей, сохраняемых в удаленной MIB.

Пример: Задать для удаленной MIB в порту ethernet 0/0/5 коммутатора предельное число записей 200.

```
Switch(config)#interface ethernet 0/0/5
Switch(Config-if-ethernet 0/0/5)#lldp neighbors max-num 200
```

3.5.11 lldp tooManyNeighbors

Синтаксис: lldp tooManyNeighbors {discard | delete}

Назначение: Позволяет задать операцию, которая будет выполняться, когда удаленная таблица полностью заполнена.

Параметры: discard: Отбрасывает текущее сообщение.

Delete: Удаляет сообщение с наименьшим TTL в удаленной таблице.

Значение по умолчанию: Отбрасывает текущее сообщение (discard).

Режим конфигурирования: Режим настройки интерфейсов

Описание: Когда удаленная MIB заполнена полностью, выбор опции discard приводит к отбрасыванию принятого сообщения. Если выбрана опция delete, из удаленной таблицы будет удалено сообщение с наименьшим TTL.

Пример: Задать для порта ethernet 0/0/5 режим delete.

```
Switch(config)#interface ethernet 0/0/5
Switch(Config-if-ethernet 0/0/5)#lldp tooManyNeighbors delete
```

3.5.12 show lldp

Синтаксис: show lldp

Назначение: Позволяет вывести на дисплей информацию LLDP глобального режима конфигурирования, например, список портов, на которых включен протокол LLDP, интервал отправки сообщений обновления, настройки времени жизни сообщений, интервал ожидания модулем отправки повторной инициализации, интервал отправки сообщений TRAP, предельное число записей в удаленной таблице.

Параметры: Нет.

Значение по умолчанию: Настройки LLDP глобального режима конфигурирования на дисплей не выводятся.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Введя команду **show lldp**, пользователи могут проанализировать всю информацию LLDP глобального режима конфигурирования.

Пример: Вывести на дисплей всю информацию LLDP глобального режима конфигурирования, доступную на коммутаторе.

```
Switch(config)#show lldp
-----LLDP GLOBAL INFORMATION-----
LLDP enabled port : Ethernet 0/0/1
LLDP interval :30
LLDP txTTL :120
LLDP txShutdownWhile :2
LLDP NotificationInterval :5
LLDP txDelay :20
-----END-----
```

3.5.13 show lldp traffic

Синтаксис: show lldp traffic

Назначение: Выводит на дисплей статистику пакетов данных LLDP.

Параметры: Нет.

Значение по умолчанию: Статистика пакетов данных LLDP на дисплей не выводится.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Введя команду **show lldp traffic**, пользователи могут проверить статистику пакетов данных LLDP.

Пример: Вывести на дисплей статистику пакетов данных LLDP (функция LLDP уже включена на коммутаторе).

```
Switch(config)#show lldp traffic
PortName      Ageouts      FramesDiscarded  FramesInErrors  FramesIn  FramesOut  TLVsDiscarded  TLVsUnrecognized
-----
Ethernet0/0/14  0            0                0                0          7          0                0
```

3.5.14 show lldp interface ethernet

Синтаксис: show lldp interface ethernet {IFNAME}

Назначение: Позволяет вывести на дисплей информацию о настройках LLDP в порту, например, состояние агента LLDP.

Параметры: <IFNAME>: имя интерфейса.

Значение по умолчанию: Настройки LLDP в порту на дисплей не выводятся.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Введя команду **show lldp interface ethernet XXX**, пользователи могут проверить настройки LLDP в указанном порту.

Пример: Вывести на дисплей информацию о настройках LLDP в порту (функция LLDP включена в глобальном режиме конфигурирования).

```
Switch(config)#show lldp interface ethernet 0/0/14
Port name :Ethernet0/0/14
LLDP Agent Adminstatus : Both
LLDP Operation TLV : default
LLDP Trap Status : disable
LLDP maxRemote :100
LLDP Overflow handle : discard
LLDP interface remote status : Free
```

3.5.15 show lldp neighbors interface ethernet

Синтаксис: show lldp neighbors interface ethernet {IFNAME}

Назначение: Выводит на дисплей информацию LLDP о соседних устройствах порта.

Параметры: Нет.

Значение по умолчанию: Информация LLDP о соседних устройствах порта на дисплей не выводится.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Введя команду **show lldp neighbors interface ethernet XXX**, пользователи могут проверить информацию LLDP о соседних устройствах порта.

Пример: Вывести на дисплей информацию LLDP о соседних устройствах порта (функция LLDP включена в глобальном режиме конфигурирования).

```
Switch#show lldp neighbors interface ethernet 0/0/24
Port name : Ethernet0/0/24
Port Remote Counter : 1
TimeMark :100
ChassisIdSubtype :4
ChassisId :00-1a-81-00-18-9e
PortIdSubtype :5
PortId :Ethernet0/0/24
```

3.5.16 show debugging lldp

Синтаксис: **show debugging lldp**

Назначение: Выводит информацию о всех портах, на которых включена отладка LLDP.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Описание: Введя команду **show debugging lldp**, пользователи могут проверить информацию о всех портах, на которых включена отладка LLDP.

Пример: Вывести информацию о всех портах, на которых включена отладка LLDP.

```
Switch(config)#show debugging lldp
====BEGINNING OF LLDP DEBUG SETTINGS====
debug lldp
debug lldp packets interface Ethernet0/0/1
debug lldp packets interface Ethernet0/0/2
debug lldp packets interface Ethernet0/0/3
debug lldp packets interface Ethernet0/0/4
debug lldp packets interface Ethernet0/0/5
=====END OF DEBUG SETTINGS=====
```

3.5.17 debug lldp

Синтаксис: **debug lldp**

no debug lldp

Назначение: Позволяет включить режим отладки LLDP. Отмена команды **no debug lldp** выключает режим отладки LLDP.

Параметры: Нет.

Значение по умолчанию: Режим отладки LLDP выключен.

Режим конфигурирования: Привилегированный режим.

Описание: Когда включен режим отладки, пользователи могут проверять отправку и прием пакетов, получать другую информацию.

Пример: Включить режим отладки LLDP на коммутаторе.

```
Switch#debug lldp
```

3.5.18 debug lldp packets

Синтаксис: `debug lldp packets interface ethernet {IFNAME}`

`no debug lldp packets interface ethernet {IFNAME}`

Назначение: Позволяет вывести на дисплей информацию LLDP по отправке и приему сообщений. Отмена команды `no debug lldp packets interface ethernet {IFNAME}` включает вывод отладочной информации на коммутаторе.

Параметры: Нет.

Значение по умолчанию: Вывод на дисплей информации LLDP по отправке и приему сообщений выключен.

Режим конфигурирования: Привилегированный режим.

Описание: Когда включен этот режим отладки, пользователи могут проверять отправку и прием пакетов в порту, получать другую информацию.

Пример: Включить вывод на дисплей информации LLDP по отправке и приему сообщений на коммутаторе.

```
Switch#debug lldp packets interface ethernet 0/0/1
%Jan 13 04:25:14 2006 LLDP-pdu-receive portname is Ethernet0/0/24
```

3.5.19 clear lldp remote-table

Синтаксис: `clear lldp remote-table`

Назначение: Очищает таблицу удаленных записей в порту.

Параметры: Нет.

Значение по умолчанию: Таблица не очищается.

Режим конфигурирования: Режим настройки интерфейсов

Описание: Очищает таблицу удаленных записей в текущем порту.

Пример: Очистить таблицу удаленных записей в текущем порту.
`Switch(Config-Ethernet 0/0/1)#clear lldp remote-table`

4 Команды для настройки Port Channel

4.1.1 debug port-channel

Синтаксис: `debug port-channel {port-group-number} {all | event | fsm | packet | timer}`

`no debug port-channel [port-group-number]`

Назначение: Включает отладку port-channel.

Параметры: **all:** вся отладочная информация; **event:** отладочная информация о событиях port-channel; **fsm:** отладочная информация по состояниям port-channel; **packet:** отладочная информация по пакетам LACP; **timer:** отладочная информация по таймеру.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Вывод на дисплей отладочной информации port-channel выключен.

Описание: Эта команда используется для включения отладки LACP, при этом на дисплей начинает выводиться информация об обработке пакетов LACP.

Пример: Включить вывод отладочных сообщений LACP.

```
Switch#debug port-channel 1 fsm
```

4.1.2 interface port-channel

Синтаксис: `interface port-channel <port-channel-number>`

Назначение: Осуществляет вход в режим настройки интерфейса port-channel.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: При входе в режим агрегированного порта, к агрегированным портам будут применены настройки модулей GVRP или spanning tree. Если агрегированный порт не существует (например, порты не агрегированы), будет выведено сообщение об ошибке, при этом настройки будут сохранены – они будут восстановлены, когда порты будут агрегированы. Следует иметь в виду, что такое восстановление выполняется только один раз. Если группа агрегации разгруппирована, а затем агрегирована снова, начальные пользовательские настройки восстановлены не будут. Если это настройки для модулей – например, настройки выключения или настройки скорости, то настройки текущего порта будут применены ко всем портам-членам соответствующей группы портов.

Пример: Войти в режим настроек port-channel 1.

```
Switch(config)#interface port-channel 1
Switch(Config-If-Port-Channell)#
```

4.1.3 lacp port-priority

Синтаксис: `lacp port-priority {port-priority}`

`no lacp port-priority`

Назначение: Установка приоритета порта для протокола LACP.

Параметры: **port-priority:** приоритет порта, в диапазоне от 0 до 65535.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: 32768

Пример:

```
Switch(Config-If-Ethernet0/0/1)#lacp port-priority 30000
```

4.1.4 lacp system-priority

Синтаксис: `lacp system-priority {system-priority}`

`no lacp system -priority`

Назначение: Установка системного приоритета для протокола LACP.

Параметры: **system -priority:** системный приоритет, в диапазоне от 0 до 65535.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 32768

Пример:

```
Switch(config)# lacp system-priority 30000
```

4.1.5 lacp timeout

Синтаксис: **lacp timeout {short | long}**

no lacp timeout

Назначение: Установка таймаута для протокола LACP.

Параметры: **long:** длительный таймаут; **short:** короткий таймаут.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: long.

Пример:

```
Switch(Config-If-Ethernet0/0/1)#lacp timeout short
```

4.1.6 load-balance

Синтаксис: **load-balance {dst-src-mac | dst-src-ip}**

Назначение: Установка режима балансировки для протокола LACP.

Параметры: **dst-src-mac:** балансировка нагрузки на основе MAC-адресов источника и назначения; **dst-src-ip:** балансировка нагрузки на основе IP-адресов источника и назначения.

Режим конфигурирования: Режим конфигурирования port-channel.

Значение по умолчанию: dst-src-mac.

Пример:

```
Switch(config)#interface port-channel 1
Switch(Config-If-Port-Channel1)#load-balance dst-src-ip
```

4.1.7 port-group

Синтаксис: **port-group {port-group-number}**

no port-group {port-group-number}

Назначение: Позволяет создать группу портов. Отмена команды **no port-group {port-group-number}** удаляет эту группу.

Параметры: **port-group-number:** номер группы port channel, в пределах от 1 до 15, если группа с этим номером уже существует, будет выведено сообщение об ошибке.

Значение по умолчанию: Порты коммутатора не принадлежат port-channel. Протокол LACP не включен.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Создать новую группу портов.

```
Switch(config)#port-group 1
```

Удалить группу портов.

```
Switch(config)#no port-group 1
```

4.1.8 port-group mode

Синтаксис: **port-group {port-group-number} mode {active | passive | on}**

no port-group {port-group-number}

Назначение: Позволяет добавить физический порт в port channel. Отмена команды **no port-group {port-group-number}** удаляет указанный порт из port channel.

Параметры: **port-group-number**: номер группы port channel, в пределах от 1 до 15;

active: включает протокол LACP на порту, устанавливает на нем активный режим (Active mode); **passive**: включает протокол LACP на порту, устанавливает на нем пассивный режим (Passive mode); **on**: принудительно вводит порт в состав port channel, протокол LACP при этом не включается.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Порты коммутатора не принадлежат port-channel. Протокол LACP не включен.

Описание: Если указанная группа портов не существует, то перед добавлением портов она будет создана. Все порты в группе портов должны добавляться в одном и том же режиме, например, все порты используют режим работы первого добавленного порта. Добавление порта в режиме "on" форсирует операцию. Это означает, что агрегированный порт локального окончания коммутатора не будет руководствоваться информацией другого окончания. Агрегированный порт будет успешно работать, если имеются 2 или более портов в группе и все порты имеют непротиворечивую информацию VLAN. При добавлении порта в активном ("active") или пассивном ("passive") режиме будет включен протокол LACP. По крайней мере, на одном окончании порты должны быть добавлены в активном режиме. Если все порты находятся в пассивном режиме, группа из них создана быть не может.

Пример: В режиме настройки порта, добавить порт ethernet 0/0/1 в группу 1 в активном режиме.

```
Switch(Config-If-Ethernet0/0/1)#port-group 1 mode active
```

4.1.9 show port-group

Синтаксис: **show port-group** [**<port-group-number>**] {**brief** | **detail** | **load-balance** | **port** | **port-channel**}

Параметры: **<port-group-number>**: номер группы port channel, в пределах от 1 до 15;

brief: отображение на дисплее сводной информации;

detail: отображение на дисплее детальной информации;

load-balance: отображение на дисплее информации о балансировке нагрузки;

port: отображение на дисплее информации о портах-членах группы;

port-channel: отображение на дисплее информации об агрегированном порте.

Режим конфигурирования: Привилегированный режим, режим конфигурирования

Описание: Если параметр port-group-number не задан, на дисплей выводится информация обо всех группах портов.

Пример: Добавить порты 0/0/1 и 0/0/2 в группу портов 1. Вывести на дисплей сводную информацию для группы портов 1.

```
Switch#show port-group 1 brief
```

```
Port-group number : 1
```

```
the attributes of the port-group are as follows:
```

```
mac_type:ETH_TYPE    speed_type:ETH_SPEED_1000M
```

```
duplex_type:FULL     port_type:TRUNK
```

```
Number of ports in port-group : 2    Maxports in port-channel = 8
```

```
Number of port-channels : 1    Max port-channels : 1
```

Информация, отображаемая на дисплее	Описание
Number of ports in group	Количество портов в группе
Maxports	Максимально допустимое число портов в группе
Number of port-channels	Существуют ли агрегированные порты или нет
Max port-channels	Максимальное число агрегированных портов, которые можно создать из групп портов.

Вывести на дисплей информацию port-channel для группы портов 1.

```
Switch# show port-group 1 port-channel
```

```
Port channels in the group 1:
```

```

Port-Channel: port-channel1
Number of port : 2 Standby port : NULL
Port in the port-channel :
Index          Port          Mode
-----
1              Ethernet0/0/26 active
2              Ethernet0/0/25 active

```

Информация, отображаемая на дисплее	Описание
Port channels in the group	Если port-channel не существует, информация, приведенная выше, отображена не будет.
Number of port	Номер порта в port-channel
Standby port	Порт находится в состоянии "standby" (ожидание). Это означает, что порт квалифицирован для вступления в канал, но не может быть принят в него, так как превышено максимально допустимое число портов. Поэтому порт имеет состояние "standby" (ожидание), а не "selected" (выбран).

5 Команды для настройки работы с Jumbo-кадрами

5.1.1 jumbo enable

Синтаксис: `jumbo enable [mtu-value]`

`no jumbo enable`

Назначение: Позволяет задать размер MTU для JUMBO-кадра и включить функцию приема/передачи JUMBO-кадров. Отмена команды **no jumbo enable** восстанавливает прием/передачу обычных кадров.

Параметр: mtu-value: значение MTU jumbo-кадра, который может быть принят, в байтах, в пределах от 1500 до 9000. Коммутатор способен принимать кадры размером не более 1614 байт. Если этот параметр не задан, считается, что максимальный размер кадров равен 1614 байт.

Значение по умолчанию: Функция Jumbo не включена.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Необходимо, чтобы функция jumbo была включена на коммутатора на обоих окончаниях, в противном случае jumbo-кадры будут отбрасываться одним из коммутаторов.

Примечание: Максимальное значение MTU JUMBO-кадра составляет 1614 байт. Значение MTU, заданное в ПО может быть больше или меньше 1614 байт, однако аппаратно поддерживается только значение MTU равное 1614.

Пример: Включить на коммутаторе функцию jumbo.
`Switch(config)#jumbo enable`

6 Настройка VLAN

6.1 Команды для настройки VLAN

6.1.1 debug gvrp

Синтаксис: `debug gvrp`

`no debug gvrp`

Назначение: Включает режим отладки протокола GVRP. Отмена команды `no debug gvrp` выключает режим отладки протокола GVRP.

Режим конфигурирования: Привилегированный режим

Значение по умолчанию: Вывод на дисплей отладочной информации протокола GVRP выключен.

Описание: Эта команда используется для включения режима отладки протокола GVRP, при этом на дисплей начинает выводиться информация об обработке пакетов GVRP.

Пример: Включить режим отладки протокола GVRP.
`Switch#debug gvrp`

6.1.2 dot1q-tunnel enable

Синтаксис: `dot1q-tunnel enable`

`no dot1q-tunnel enable`

Назначение: Устанавливает для порта доступа коммутатора режим туннеля dot1q. Отмена команды `no dot1q-tunnel enable` восстанавливает настройки, используемые по умолчанию.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Функция туннеля Dot1q не включена.

Описание: После того как функция туннеля Dot1q с помощью этой команды будет включена, коммутатор сможет использовать туннель.

Пример: Включить функцию туннеля dot1q.
`Switch(config)#dot1q-tunnel enable`

6.1.3 dot1q-tunnel tpid

Синтаксис: `dot1q-tunnel tpid {8100 | 9100 | 9200}`

Назначение: Позволяет настроить тип протокола (TPID) в магистральных портах коммутатора.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: TPID порта равен 8100.

Описание: Эта функция необходима для работу с оборудованием других изготовителей. Если оборудование, подключенное к магистральному порту коммутатора, посылает пакет данных с TPID 9100, для порта будет установлен TPID 9100.

Пример: Установить TPID коммутатора 9100.
`Switch(config)#dot1q-tunnel tpid 9100`

6.1.4 gvrp

Синтаксис: `gvrp`

`no gvrp`

Назначение: Позволяет включить функцию GVRP на коммутаторе или в текущем магистральном порту. Отмена команды `no gvrp` выключает функцию GVRP в глобальном режиме конфигурирования, либо для порта.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов

Значение по умолчанию: Функция GVRP выключена.

Описание: Функция GVRP может быть включена в порту только после того, как она будет включена в глобальном режиме конфигурирования. Если функция GVRP выключена в глобальном режиме конфигурирования, настройки GVRP в портах также действовать не будут.

Примечание: Функция GVRP может быть включена только на портах, работающих в режиме trunk.

Пример: Включить функцию GVRP в глобальном режиме конфигурирования и в магистральном порту 10.

```
Switch(config)#gvrp
Switch(config)#interface ethernet 0/0/10
Switch(Config-If-Ethernet0/0/10)#gvrp
Switch(config)#exit
```

6.1.5 garp timer hold

Синтаксис: `garp timer hold {timer-value}`

`no garp timer hold`

Назначение: Позволяет установить таймер удержания для GARP. Отмена команды `no garp timer hold` восстанавливает настройку таймера, используемую по умолчанию.

Параметр: timer-value: значение таймера удержания GARP, в пределах от 100 до 327650 мс.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: 100 мс.

Описание: Когда GARP-приложение принимает сообщение join, это сообщение не будет отправлено сразу, вместо отправки сообщения начнется отсчет таймера удержания. По истечении таймера удержания все принятые, в течении времени таймера, сообщения join будут отправлены в одном кадре GVRP. Это значительно уменьшает трафик сообщений протокола.

Пример: Установить таймер удержания GARP для порта 0/0/10 равным 500 мс.

```
Switch(Config-If-Ethernet0/0/10)#garp timer hold 500
```

6.1.6 garp timer join

Синтаксис: `garp timer join {timer-value}`

`no garp timer join`

Назначение: Позволяет установить таймер слияния для GARP. Отмена команды `no garp timer join` восстанавливает настройку таймера, используемую по умолчанию.

Параметр: timer-value: значение таймера слияния GARP, в пределах от 100 до 327650 мс.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: 200 мс.

Описание: По истечении таймера слияния GARP-приложение посылает сообщение о слиянии. Другое GARP-приложение объявляет о приеме сообщения о слиянии и регистрирует его.

Пример: Установить таймер слияния GARP порта 10 равным 1000 мс.

```
Switch(Config-If-Ethernet0/0/10)#garp timer join 1000
```

6.1.7 garp timer leave

Синтаксис: `garp timer leave {timer-value}`

`no garp timer leave`

Назначение: Позволяет установить таймер времени жизни для GARP. Отмена команды `no garp timer leave` восстанавливает настройку таймера, используемую по умолчанию.

Параметр: `timer-value`: значение таймера выхода для GARP, в пределах от 100 до 327650 мс.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: 600 мс.

Описание: Когда GARP-приложение желает удалить некоторую собственную информацию, оно посылает сообщение выхода (leave). GARP-приложение регистрирует прием этого сообщения и включает таймер выхода. Если до истечения таймера сообщений о слиянии (join) не принято, собственная информация удаляется. Значение таймера выхода должно быть вдвое больше, чем таймера слияния. В противном случае, будет выведено сообщение об ошибке.

Пример: Установить таймер удержания GARP для порта 0/0/10 равным 3000 мс.

```
Switch(Config-If-Ethernet0/0/10)#garp timer leave 3000
```

6.1.8 garp timer leaveall

Синтаксис: `garp timer leaveall {timer-value}`

`no garp timer leaveall`

Назначение: Позволяет установить таймер общего выхода для GARP. Отмена команды `no garp timer leaveall` восстанавливает настройку таймера, используемую по умолчанию.

Параметр: `timer-value`: значение таймера общего выхода GARP, в пределах от 100 до 327650 мс.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 10000 мс.

Описание: При запуске GARP-приложения начинается отсчет таймера общего выхода (leaveall). По истечении таймера общего выхода, GARP-приложение отправляет сообщение общего выхода. Другие GARP-приложения удаляют всю информацию, являющуюся собственностью этого приложения и таймер общего выхода очищается для начала нового цикла.

Пример: Установить таймер общего выхода GARP равным 50000 мс.

```
Switch(config)#garp timer leaveall 50000
```

6.1.9 name

Синтаксис: `name {vlan-name}`

`no name`

Назначение: Присваивает имя VLAN. Имя VLAN — это строка с описанием VLAN. Отмена команды `no name` удаляет соответствующее имя VLAN.

Параметры: `vlan-name`: строка имени с описанием VLAN.

Режим конфигурирования: Режим настройки VLAN.

Значение по умолчанию: Имя VLAN имеет вид VLANXXX, где XXX — это VID.

Описание: Команда позволяет присвоить указанной VLAN строку имени с описанием VLAN, которое будет сохранено в памяти.

Примеры: Присвоить VLAN100 имя TestVlan.

```
Switch(Config-Vlan100)#name TestVlan
```

6.1.10 private-vlan

Синтаксис: `private-vlan {primary | isolated | community}`

`no private-vlan`

Назначение: Позволяет настроить текущий VLAN для работы в режиме private vlan. Отмена команды `no private-vlan` восстанавливает режим работы по умолчанию VLAN.

Параметры: `primary`: устанавливает текущий VLAN как первичный (Primary) VLAN; `isolated`: устанавливает текущий VLAN как изолированный VLAN; `community`: устанавливает текущий VLAN как общий VLAN.

Режим конфигурирования: Режим настройки VLAN

Значение по умолчанию: Настройки private vlan не включены.

Описание: Имеется три режима private VLAN: первичный (primary) VLAN, изолированный (isolated) VLAN и общий (community) VLAN. Порты в первичном VLAN являются портами трех частных VLAN. Порты первичного VLAN, изолированного VLAN и общего VLAN могут связываться с портами isolated VLAN и VLAN community, принадлежащими этому первичному VLAN. Порты в isolated VLAN изолированы друг от друга и могут связываться только с портами primary VLAN, которому они принадлежат. Порты community VLAN могут связываться друг с другом и с портами primary VLAN, которому они принадлежат. Связь между портами community VLAN и портами isolated VLAN отсутствует. Только VLAN, содержащие пустые Ethernet-порты могут быть настроены как private VLAN. Только private VLAN с соответствующими частными связями могут устанавливать порты своих членов как Ethernet-порты доступа. Когда обычный VLAN устанавливается как private, закрепления Ethernet-портов для него стираются. Следует отметить, что сообщения private VLAN не передаются по протоколу GVRP.

Пример: Установить VLAN100, 200, 300 private VLAN, а именно: VLAN100 primary, VLAN200 isolated, а VLAN300 — community VLAN.

```
Switch(config)#vlan 100
Switch(Config-Vlan100)#private-vlan primary
Note:This will remove all the ports from vlan 100
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#private-vlan isolated
Note:This will remove all the ports from vlan 200
Switch(Config-Vlan200)#exit
Switch(config)#vlan 300
Switch(Config-Vlan300)#private-vlan community
Note:This will remove all the ports from vlan 300
Switch(Config-Vlan300)#exit
```

6.1.11 private-vlan association

Синтаксис: `private-vlan association {<secondary-vlan-list>}`

`no private-vlan association`

Назначение: Позволяет установить ассоциацию private VLAN. Отмена команды `no private-vlan association` удаляет соответствующую ассоциацию private VLAN.

Параметры: `<secondary-vlan-list>`: список вторичных VLAN, ассоциированных с первичным VLAN. Вторичные VLAN могут быть двух видов: изолированные (isolated) VLAN и общие (community) VLAN. При указании в команде нескольких VLAN можно использовать символ-разделитель “;”.

Режим конфигурирования: Режим настройки VLAN.

Значение по умолчанию: Ассоциация private VLAN не задана.

Описание: Эта команда используется только для private VLAN. Порты вторичных VLAN, ассоциированных с первичным VLAN могут связываться с портами первичного VLAN. Перед настройкой ассоциации private VLAN, private VLAN всех трех типов не должны иметь портов членов; private VLAN с ассоциацией не могут быть удалены. Когда пользователи удаляют ассоциацию private VLAN, все ассоциированные порты членов в private VLAN удаляются, в том числе и из соответствующих private VLAN.

Пример: Ассоциировать isolated VLAN200 и community VLAN300 с primary VLAN100.
Switch(Config-Vlan100)#private-vlan association 200;300

6.1.12 show dot1q-tunnel

Синтаксис: show dot1q-tunnel

Назначение: Когда туннель dot1q установлен, выводит на дисплей информацию о всех портах.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим, другие режимы конфигурирования.

Описание: Когда туннель dot1q установлен, эта команда выводит на дисплей информацию о состоянии всех портов.

Пример: Вывести на дисплей текущее состояние туннеля dot1q.

```
Switch#show dot1q-tunnel
Tpid: 9100 Port      Type
Ethernet0/0/1 Customer
Ethernet0/0/20 Uplink
```

6.1.13 show garp

Синтаксис: show garp [<interface-name>]

Назначение: Позволяет вывести на дисплей информацию GARP глобального режима конфигурирования и для порта.

Параметр: <interface-name>: имя магистрального порта, информация для которого выводится на дисплей.

Режим конфигурирования: Привилегированный режим, другие режимы конфигурирования.

Описание: нет

Пример: Вывести на дисплей информацию GARP глобального режима конфигурирования.

```
Switch#show garp
```

6.1.14 show gvrp

Синтаксис: show gvrp [<interface-name>]

Назначение: Позволяет вывести на дисплей информацию GVRP глобального режима конфигурирования и для порта.

Параметры: <interface-name>: имя магистрального порта, информация для которого выводится на дисплей.

Режим конфигурирования: Привилегированный режим, другие режимы конфигурирования.

Описание: нет

Пример: Вывести на дисплей информацию GVRP глобального режима конфигурирования.

```
Switch#show gvrp
----- Gvrp Information -----
Gvrp status : enable
Gvrp Timers(milliseconds)LeaveAll : 10000
```

6.1.15 show vlan

Синтаксис: show vlan [brief | summary] [id <vlan-id>] [name <vlan-name>] [internal usage [id <vlan-id> | name <vlan-name>]] [private-vlan [id <vlan-id> | name <vlan-name>]]

Назначение: Выводит на дисплей подробную информацию о всех VLAN либо только об указанном VLAN.

Параметры: **brief:** вывод краткой информации; **summary:** вывод статистики VLAN; **<vlan-id>:** идентификатор VLAN ID того VLAN, для которого на дисплей выводится информация, в пределах от 1 до 4094; **<vlan-name>:** имя VLAN, информация о котором выводится на дисплей, строка длиной от 1 до 11 символов; **private-vlan:** на дисплей выводится ID, имя private VLAN, информация о портах.

Режим конфигурирования: Привилегированный режим, режим конфигурирования.

Описание: Если параметры <vlan-id> или <vlan-name> не заданы, на дисплей выводится информация о всех VLAN коммутатора.

Пример: Вывести на дисплей информацию для текущей VLAN и статистики для него.
Switch#show vlan

VLAN	Name	Type	Media	Ports	
1	default	Static	ENET	Ethernet0/0/1	Ethernet0/0/2
				Ethernet0/0/3	Ethernet0/0/4
				Ethernet0/0/9	Ethernet0/0/10
				Ethernet0/0/11	Ethernet0/0/12
2	VLAN0002	Static	ENET	Ethernet0/0/5	Ethernet0/0/6
				Ethernet0/0/7	Ethernet0/0/8

Информация, отображаемая на дисплее	Описание
VLAN	Номер VLAN
Name	Имя VLAN
Type	Тип VLAN, статическая настройка либо полученная при динамическом обучении.
Media	Тип интерфейса VLAN: Ethernet
Ports	Порт доступа в VLAN

6.1.16 show vlan-translation

Синтаксис: show vlan-translation

Назначение: Отображение настройки трансляции vlan.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show vlan-translation
Interface Ethernet0/0/1:
  vlan-translation is enable, miss drop is not set
  vlan-translation 5 to 10 in
Interface Ethernet0/0/2:
  vlan-translation is enable, miss drop is set both
  vlan-translation 6 to 12 out
```

6.1.17 switchport dot1q-tunnel

Синтаксис: switchport dot1q-tunnel mode {customer | uplink}

no switchport dot1q-tunnel

Назначение: Настраивает для порта режим работы с туннелем dot1q.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов

Настройки по умолчанию: Туннель dot1q не включен.

Описание: Эта команда в режиме настройки портов позволяет настроить для порта режим работы с туннелем dot1q, при этом туннели dot1q предварительно должны быть включены в глобальном режиме конфигурирования. Для того чтобы разрешить работу клиентских сетей VLAN используется режим настройки клиентов, при этом должны быть настроены порты доступа. Для подключения к операторской сети используется режим uplink, он должен быть установлен в магистральном порту. К пакетам без идентификаторов VLAN ID, принятым от клиентских портов, добавляются теги верхнего уровня. К пакетам с VLAN ID добавляются VLAN ID внешнего уровня. VLAN ID — это ID виртуальной сети, которой принадлежит порт. Для пакетов, посланных из портов в режиме uplink, в качестве тега будет прикреплен TPID. Для пакетов с двойными тегами передача будет определяться MAC-адресом и внешними тегами.

Пример: Установить для порта 1 в VLAN 3 клиентский режим для подключения к клиентской сети. Установить для порта 25 режим uplink для подключения к операторской сети.

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 0/0/1
Switch(Config-Vlan3)#exit
Switch(config)#dot1q-tunnel enable
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#switchport dot1q-tunnel mode customer
Switch(Config-If-Ethernet0/0/1)#exit
Switch(config)#interface ethernet 0/0/25
Switch(Config-If-Ethernet0/0/25)#switchport mode trunk
Switch(Config-If-Ethernet0/0/25)#switchport dot1q-tunnel mode uplink
Switch(Config-If-Ethernet0/0/25)#exit
```

6.1.18 switchport access vlan

Синтаксис: `switchport access vlan {<vlan-id>}`

`no switchport access vlan`

Назначение: Добавляет текущий порт доступа в указанный VLAN. Отмена команды `no switchport access vlan` удаляет соответствующий порт из указанного VLAN, после этого порт будет принадлежать VLAN1.

Параметр: `<vlan-id>`: идентификатор VLAN ID того VLAN, в который добавляется порт, в пределах от 1 до 4094.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Все порты коммутатора принадлежат VLAN1.

Описание: В указанный VLAN можно добавить только порт доступа коммутатора. Одной командой к VLAN может быть добавлен только один порт доступа.

Пример: Добавить указанный порт в VLAN100.

```
Switch(config)#interface ethernet 0/0/8
Switch(Config-If-Ethernet0/0/8)#switchport mode access
Switch(Config-If-Ethernet0/0/8)#switchport access vlan 100
Switch(Config-If-Ethernet0/0/8)#exit
```

6.1.19 switchport hybrid allowed vlan

Синтаксис: `switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD} {tag | untag}`

`no switchport hybrid allowed vlan`

Назначение: Перевод порта в гибридный режим работы для передачи кадров со снятием или установкой тега.

Параметр: **WORD**: перечень разрешенных vlan; **all**: разрешены все vlan; **add WORD**: добавить номера vlan к списку разрешенных; **except WORD**: разрешены все vlan, кроме указанных; **remove WORD**: удалить указанные vlan из списка разрешенных; **tag**: передавать указанные vlan с сохранением тега; **untag**: передавать указанные vlan со снятием тега.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Любой трафик запрещен.

Описание: Эта команда может быть использована для указания vlan, трафик которых разрешен для передачи через порт, трафик остальных vlan запрещен. При указании параметра **untag** трафик через порт передается со снятием указанных vlan. При указании параметра **tag** трафик через порт передается с сохранением указанных vlan.

Пример: Перевести порт в гибридный режим и передавать трафик vlan 1, 3, 5-20 со снятием тега и трафик vlan 100, 300, 500-2000 с сохранением тега.

```
Switch(config)#interface ethernet 0/0/5
Switch(Config-If-Ethernet0/0/5)#switchport mode hybrid
Switch(Config-If-Ethernet0/0/5)#switchport hybrid allowed vlan 1;3;5-20 untag
Switch(Config-If-Ethernet0/0/5)#switchport hybrid allowed vlan 100;300;500-2000 tag
Switch(Config-If-Ethernet0/0/5)#exit
```

6.1.20 switchport hybrid native vlan

Синтаксис: `switchport hybrid native vlan {<vlan-id>}`

no switchport hybrid native vlan

Назначение: Установка native vlan для гибридного порта.

Параметр: <vlan-id>: native vlan.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: 1

Описание: Нетегированному кадру, пришедшему на гибридный порт, будет назначен тег, заданный данной командой.

Пример:

```
Switch(config)#interface ethernet 0/0/5
Switch(Config-If-Ethernet0/0/5)#switchport mode hybrid
Switch(Config-If-Ethernet0/0/5)#switchport hybrid native vlan 100
Switch(Config-If-Ethernet0/0/5)#exit
```

6.1.21 switchport interface

Синтаксис: `switchport interface [ethernet | portchannel] [interface-name | interface-list]`

no switchport interface [ethernet | portchannel] [interface-name | interface-list]

Назначение: Позволяет добавить в VLAN интерфейс Ethernet. Отмена команды **no switchport interface [ethernet | portchannel] [<interface-name | interface-list>]** удаляет соответствующие интерфейсы Ethernet из VLAN.

Параметр: **ethernet:** добавляемый Ethernet-порт.

portchannel: добавляемый порт является агрегированным.

interface-name: имя порта, например, e0/0/1.

interface-list: список интерфейсов, добавляемых в VLAN или удаляемых из него; в списке можно использовать символы-разделители “,” или “-”.

Режим конфигурирования: Режим настройки интерфейсов VLAN.

Значение по умолчанию: У вновь созданного VLAN портов нет.

Описание: Порты доступа коммутатора — это обычные порты, которые могут быть добавлены в один и только один VLAN.

Пример: Добавить порты ethernet 0/0/1;3;4-7;8 в VLAN100.

```
Switch(Config-Vlan100)#switchport interface ethernet 0/0/1;3;4-7;8
```

6.1.22 switchport mode

Синтаксис: `switchport mode {trunk | access | hybrid}`

Назначение: Позволяет настроить порт для работы в режимах access или trunk.

Параметры: **trunk:** включает для порта режим, в котором разрешена передача различных VLAN; **access:** включает для порта режим, когда он может принадлежать только одному VLAN; **hybrid:** включает для порта режим, в котором разрешена передача различных VLAN с возможностью сохранения и снятия тега.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Порт работает в режиме access.

Описание: Порты, настроенные для работы в режиме trunk, называются магистральными портами. Через магистральные порты могут передаваться пакеты, поступающие из многих VLAN. Порты, работающие в режиме access, называются портами доступа. Если порт работает в режиме доступа, он может принадлежать только одному VLAN.

Пример: Включить для порта 5 магистральный режим, а для порта 8 — режим доступа.

```
Switch(config)#interface ethernet 0/0/5
Switch(Config-If-Ethernet0/0/5)#switchport mode trunk
Switch(Config-If-Ethernet0/0/5)#exit
Switch(config)#interface ethernet 0/0/8
Switch(Config-If-Ethernet0/0/8)#switchport mode access
Switch(Config-If-Ethernet0/0/8)#exit
Switch(config)#interface ethernet 0/0/10
Switch(Config-If-Ethernet0/0/10)#switchport mode hybrid
Switch(Config-If-Ethernet0/0/10)#exit
```

6.1.23 switchport trunk allowed vlan

Синтаксис: **switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD}**

no switchport trunk allowed vlan

Назначение: Позволяет настроить список VLAN, пакеты которых могут проходить через магистральный порт. Отмена команды **no switchport trunk allowed vlan** восстанавливает значения, заданные по умолчанию.

Параметры: **WORD:** идентификаторы VID, указываемые в команде; ключевое слово; **add:** добавить указанные VID в список разрешенных; **except:** все VID добавляются к разрешенным vlan, за исключением указанных VID; **remove:** удалить указанные vlan из списка разрешенных.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Все пакеты всех VLAN могут проходить через магистральный порт.

Описание: Эта команда позволяет задать, пакеты каких VLAN смогут проходить через магистральный порт. Пакеты тех VLAN, которые не указаны в команде, будут отбрасываться.

Пример: Установить для порта 5 магистральный режим. Разрешить пакетам VLAN 1, 3, 5, 20 проходить через порт.

```
Switch(config)#interface ethernet 0/0/5
Switch(Config-If-Ethernet0/0/5)#switchport mode trunk
Switch(Config-If-Ethernet0/0/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-If-Ethernet0/0/5)#exit
```

6.1.24 switchport trunk native vlan

Синтаксис: **switchport trunk native vlan {<vlan-id>}**

no switchport trunk native vlan

Назначение: Позволяет задать идентификатор PVID для магистрального порта. Отмена команды **no switchport trunk native vlan** восстанавливает значения, заданные по умолчанию.

Параметры: **<vlan-id>:** идентификатор PVID для магистрального порта.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Магистральному порту присвоен PVID 1.

Описание: Идентификаторы PVID определены в стандарте 802.1Q. Когда магистральный порт принимает непометенный кадр (untagged frame), к этому кадру прикрепляется метка — PVID, после этого кадр передается в порт назначения.

Пример: Задать PVID 100 для порта ethernet 0/0/5.

```
Switch(config)#interface ethernet 0/0/5
Switch(Config-If-Ethernet0/0/5)#switchport mode trunk
Switch(Config-If-Ethernet0/0/5)#switchport trunk native vlan 100
Switch(Config-If-Ethernet0/0/5)#exit
```

6.1.25 vlan

Синтаксис: `vlan {<vlan-id>}`

`no vlan {<vlan-id>}`

Назначение: Позволяет создать VLAN и войти в режим настройки VLAN. В режиме VLAN можно задать имена VLAN, указать используемые интерфейсы. Отмена команды `no vlan <vlan-id>` удаляет указанный VLAN.

Параметры: `<vlan-id>`: идентификатор создаваемого или удаляемого VLAN. Диапазон значений 1 — 4094.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Сконфигурирована только VLAN1.

Описание: VLAN1 – это VLAN, сконфигурированный в системе по умолчанию. Он не может быть удален. Максимальное число созданных VLAN равно 4094. Динамические VLAN, полученные с помощью GVRP не могут быть удалены этой командой.

Пример: Создать VLAN с идентификатором 100, войти в режим настройки VLAN.

```
Switch(config)#vlan 100
Switch(Config-Vlan100)#
```

6.1.26 vlan-translation

Синтаксис: `vlan-translation {<old-vlan-id>} to {<new-vlan-id>} {in | out}`

`no vlan-translation {<old-vlan-id>} {in | out}`

Назначение: Позволяет установить трансляцию VLAN, при этом исходный VLAN ID преобразовывается в новый VLAN ID. Отмена команды `no vlan-translation <old-vlan-id> in` удаляет соответствующее отображение.

Параметры: `old-vlan-id`: идентификатор исходного VLAN; `new-vlan-id`: идентификатор транслированного VLAN; `in`: задает трансляцию по входу; `out`: задает трансляцию по выходу.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Команда позволяет настроить связь между исходным VLAN и VLAN, в который выполняется трансляция (VLAN трансляции). Пакеты данных будут проверяться на соответствие заданным в команде правилам трансляции, при соответствии правилам, их VLAN ID будет заменяться указанным в команде. Если пакеты не соответствуют заданным правилам, направление их передачи будет определяться командой `vlan-translation miss drop`.

Пример: Передать данные VLAN100, поступающие с порта1 в VLAN2 (трансляция входящих пакетов) и данные из VLAN2 в VLAN100 после их трансляции в порт10.

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#vlan-translation enable
Switch(Config-If-Ethernet0/0/1)#vlan-translation 100 to 2 in
Switch(Config-If-Ethernet0/0/1)#exit
Switch(config)#interface ethernet 0/0/10
Switch(Config-If-Ethernet0/0/10)#vlan-translation enable
Switch(Config-If-Ethernet0/0/10)#vlan-translation 2 to 100 in
Switch(Config-If-Ethernet0/0/10)#exit Switch(config)#
```

6.1.27 vlan-translation enable

Синтаксис: `vlan-translation enable`

no vlan-translation enable

Назначение: Включает трансляцию VLAN на указанном магистральном порту коммутатора. Отмена команды **no vlan-translation enable** восстанавливает значения, заданные по умолчанию.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Трансляция VLAN в порту не включена.

Описание: Эта команда позволяет включить трансляцию VLAN в магистральном порту.

Пример: Включить трансляцию VLAN в порту 1.

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet 0/0/1)#vlan-translation enable
```

6.1.28 vlan-translation miss drop

Синтаксис: **vlan-translation miss drop {in | out | both}**

no vlan-translation miss drop {in | out | both}

Назначение: Позволяет задать отбрасывание пакетов, не соответствующих заданным правилам трансляции. Отмена команды **no vlan-translation miss drop {in | out | both}** восстанавливает значение, заданное по умолчанию.

Параметры: **in:** отбрасывание для входящих пакетов; **out:** отбрасывание для исходящих пакетов; **both:** отбрасывание всех пакетов;

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: При не соответствии пакетов заданным правилам трансляции, их отбрасывание не производится.

Описание: Когда установлена трансляция из исходного VLAN в текущий VLAN (заданы их идентификаторы VID), пакеты, не соответствующие правилам трансляции по умолчанию отбрасываются не будут. Их отбрасывание можно задать, введя описываемую команду.

Пример: Задать отбрасывание входящих пакетов на порт Ethernet 0/0/1, не соответствующих правилам трансляции.

```
Switch(Config-If-Ethernet0/0/1)#vlan-translation miss drop in
```

6.1.29 vlan ingress enable

Синтаксис: **vlan ingress enable**

no vlan ingress enable

Назначение: Позволяет включить правило для входящих пакетов VLAN в порту. Отмена команды **no vlan ingress enable** удаляет правило для входящих пакетов.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Правила для входящих пакетов VLAN включены.

Описание: Когда в порту включены правила для входящих пакетов VLAN выполняется следующее: система принимает данные и проверяет состояние порта-источника, а затем передает данные в порт назначения только в том случае, если этот порт является членом VLAN.

Пример: Выключить в порту правила для входящих пакетов VLAN.

```
Switch(Config-If-Ethernet0/0/1)#no switchport ingress-filtering
```

6.2 Команды для настройки динамических VLAN

6.2.1 protocol-vlan mode

Синтаксис: `protocol-vlan mode {ethernetii etype <etype-id> | llc {dsap <dsap-id> ssap <ssap-id>} | snap etype <etype-id>} {vlan <vlan-id>} [priority <priority-id>]`

`no protocol-vlan {mode {ethernetii etype <etype-id> | llc {dsap <dsap-id> ssap <ssap-id>} | snap etype <etype-id>} | all}`

Назначение: Позволяет добавить соответствие между протоколом и VLAN, а именно – указать протокол, ассоциируемый с указанным VLAN. Отмена команды **no protocol-vlan** удаляет все соответствия.

Параметры: **mode:** тип инкапсуляции, может иметь значения **ethernetii**, **llc** и **snap**; **etype:** тип инкапсуляции ethernetii соответствует EthernetII; **etype-id:** тип протокола, диапазон значений 1536 - 65535; **llc:** формат инкапсуляции LLC; **dsap-id:** точка доступа услуги назначения, диапазон значений 0 - 255; **ssap-id:** точка доступа услуги назначения, диапазон значений 0 - 255; **snap:** формат инкапсуляции SNAP; **etype-id:** тип протокола пакета, диапазон значений 1536 - 65535; **vlan-id:** ID VLAN, диапазон значений 1 - 4094; **all:** указывает все инкапсулируемые протоколы; **priority:** приоритет в диапазоне от 0 до 7.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Протоколы с VLAN не ассоциированы.

Описание: Эта команда используется для добавления в VLAN конкретных протоколов. Если пакеты указанных протоколов без тегов VLAN принимаются коммутатором, они проверяются на соответствие с VLAN с идентификатором VLAN ID и затем передаются в этот VLAN. Теги VLAN у этих пакетов будут одним и тем же, независимо от того, с какого порта приняты пакеты. Когда эта команда введена, пакеты, уже имеющие теги VLAN, не будут изменены. Если задан IP-протокол, то предполагается, что задан и протокол ARP. В противном случае, настройки могут повлиять на работу некоторых приложений.

Пример: Присвоить протокол IP-пакета данных, инкапсулированный в EthernetII сети LAN200.

```
Switch(config)#protocol-vlan mode ethernetii etype 2048 vlan 200
```

```
Switch(config)#protocol-vlan mode ethernetii etype 2054 vlan 200
```

6.2.2 show protocol-vlan

Синтаксис: `show portocol-vlan`

Назначение: Выводит на дисплей информацию о VLAN, сконфигурированных на коммутаторе на основе протоколов.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Выводит на дисплей информацию о VLAN, сконфигурированных на коммутаторе на основе протоколов.

Пример: Показать информацию о текущих VLAN, сконфигурированных на коммутаторе на основе протоколов.

```
Switch#show protocol-vlan
```

Protocol_Type	VLAN_ID
mode ethernetii etype 0x800	200
mode ethernetii etype 0x860	200
mode snap etype 0xabc	100
mode llc dsap 0xac ssap 0xbd	100

7 Команды для настройки selective QinQ

7.1.1 match

Синтаксис: `match {access-group <acl-index-or-name> | ip dscp <dscp-list> | ip precedence <ip-precedence-list> | ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <cos-list>}`

no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos}

Назначение: Позволяет задать стандарт соответствия карте классов (class map). Отмена команды `no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos}` удаляет указанный стандарт соответствия карте классов.

Параметры: `access-group <acl-index-or-name>`: согласование с указанным списком доступом ACL, параметром является номер или имя списка ACL; `ip dscp <dscp-list>` и `ipv6 dscp <dscp-list>`: согласование с указанным значением DSCP, параметром является список значений DSCP, содержащий не более 8 значений DSCP; `ip precedence <ip-precedence-list>`: согласование с указанным значением IP Precedence, параметром является список IP Precedence, содержащий не более 8 значений IP Precedence, каждое из которых задано в пределах 0~7; `ipv6 access-group <acl-index-or-name>`: согласование с указанным списком доступом IPv6 ACL, параметром является номер или имя списка IPv6 ACL; `ipv6 flowlabel <flowlabel-list>`: согласование с указанной меткой потока IPv6. Параметром является значение метки потока IPv6, допустимое значение - от 0 до 1048575; `vlan <vlan-list>`: согласование с указанным VLAN ID, параметром является список VLAN ID, содержащий не более 8 VLAN ID; `<cost-list>`: согласование с указанным значением Cos, параметром является список Cos, содержащий не более 8 значений Cos.

Режим конфигурирования: Режим карты классов.

Значение по умолчанию: Стандарт согласования не задан.

Описание: Эта команда используется для выбора тех кадров, которым будет присвоен второй тег с помощью команды `set`. Если для отбора кадров используется ACL, то правило должно быть разрешающим, иначе кадр не будет считаться удовлетворившим условию.

Пример:

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match ip precedence 0
Switch(config-classmap-c1)#exit
```

7.1.2 service-policy

Синтаксис: `service-policy <policy-map-name> in`

no service-policy <policy-map-name> in

Назначение: Привязывает указанную политику selective QinQ ко входу порта.

Параметры: `service-policy <policy-map-name>`: имя policy-map.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Политика не установлена.

Описание: Только одна команда может быть привязано к порту.

Пример:

```
Switch(Config-If-Ethernet1/0/1)#service-policy p1 in
```

7.1.3 set

Синтаксис: `set nested-vlan <vid>`

no set nested-vlan

Назначение: Добавляет кадрам соответствующего класса второй тег.

Параметры: `<vid>`: идентификатор тега, который добавляется.

Режим конфигурирования: Режим настройки карты классов.

Значение по умолчанию: Второй тег не добавляется.

Описание: Данная команда позволяет добавить второй тег кадрам, удовлетворившим условиям карты классов.

Пример:

```
Switch(config)#policy-map p1
```

```
Switch(Config-PolicyMap-p1)#class c1
```

```
Switch(Config-PolicyMap-p1-Class-c1)#set nested-vlan 2
```

8 Команды для работы с таблицей MAC-адресов

8.1 Команды для настройки таблицы MAC-адресов

8.1.1 clear mac-address-table dynamic

Синтаксис: `clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]`

Назначение: Очистка динамических MAC-адресов.

Параметры: `<mac-addr>`: MAC-адрес подлежащий удалению; `<interface-name>`: наименование интерфейса; `<vlan-id>`: идентификатор vlan.

Режим конфигурирования: Привилегированный режим.

Описание: Удаление всех записей динамических MAC-адресов из таблицы MAC-адресов, за исключением MAC-адресов приложений и системных.

Пример:

```
Switch# clear mac-address-table dynamic
```

8.1.2 mac-address-table aging-time

Синтаксис: `mac-address-table aging-time {<0 | aging-time>}`

no mac-address-table aging-time

Назначение: Позволяет задать время жизни для адресов в таблице MAC-адресов, полученных в результате динамического обучения. Отмена команды **no mac-address-table aging-time** восстанавливает время жизни соответствий адресов, равное 300 секунд.

Параметры: `<aging-time>`: время жизни адресов в секундах, в пределах от 10 до 100000; 0 соответствует нулевому времени жизни.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Установлено время жизни соответствий адресов 300 секунд.

Описание: Команда позволяет установить наилучшее время жизни MAC-адресов, соответствующее условиям работы сети. Если время жизни адресов в таблице MAC-адресов слишком мало, производительность коммутатора может ухудшиться из-за вещания, в котором, на самом деле, нет необходимости. Если время жизни адресов в таблице MAC-адресов слишком велико, некоторые записи в ней не смогут быть удалены, хотя уже и являются устаревшими. Следовательно, время жизни соответствий адресов необходимо выбирать внимательно, исходя из реальной ситуации. Если время жизни соответствий адресов установить нулевым, обновление адресов в таблице будет прекращено. При этом MAC-адрес, полученный коммутатором при обучении, будет всегда существовать в таблице MAC-адресов.

Пример: Установить время жизни MAC-адреса в таблице, полученного обучением, равным 600 секунд.

```
Switch (config)#mac-address-table aging-time 600
```

8.1.3 mac-address-table static | blackhole

Синтаксис: `mac-address-table {static | blackhole} address <mac-addr> vlan <vlan-id> [interface [ethernet | portchannel] <interface-name>] | [source | destination | both]`

no mac-address-table {static | blackhole | dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]

Назначение: Позволяет добавлять или изменять статические и фильтруемые адреса. Отмена команды **no mac-address-table {static | blackhole | dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]** удаляет соответствующие адреса.

Параметры: **static**: статические адреса; **blackhole**: фильтруемые адреса, позволяющие отбрасывать пакеты, поступающие с некоторого MAC-адреса. Фильтрация может осуществляться как по адресам источников, так и по адресам назначений (либо и по тем, и по другим). Если

введены фильтруемые адреса, они не оказывают никакого влияния на порты. **dynamic**: динамические адреса; **<mac-addr>**: добавляемый или удаляемый MAC-адрес; **<interface-name>**: имя порта, передавшего пакет с MAC-адресом; **<vlan-id>**: номер VLAN; **source**: фильтрация по адресу источника; **destination**: фильтрация по адресу назначения; **both**: фильтрация по обоим адресам – источника и назначения. Этот режим фильтрации задан по умолчанию.

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: Если настроен и включен интерфейс VLAN, система сгенерирует статический MAC-адрес, соответствующий номеру VLAN.

Описание: В некоторых особых случаях, например, когда коммутатор не может осуществлять динамическое обучение MAC-адресам, пользователи могут использовать эту команду для установки вручную соответствия между MAC-адресом, портом и VLAN. Команда **no mac-address-table all** используется для удаления всех динамических, статических и фильтруемых MAC-адресов из списка MAC-адресов коммутатора, за исключением соответствий таблицы, заданных в системе по умолчанию.

Пример: Порт 0/0/1 принадлежит VLAN200, задать соответствие с MAC-адресом 00-1a-81-00-18-9e.

```
Switch(config)#mac-address-table static address 00-1a-81-00-18-9e vlan 200
interface ethernet 0/0/1
```

8.1.4 show mac-address-table

Синтаксис: `show mac-address-table [static | blackhole | multicast | aging-time<aging-time> | count] [address <mac-addr>] [vlan <vlan-id>] [count] [interface <interface-name>]`

Назначение: Выводит на дисплей текущую таблицу MAC-адресов.

Параметры: **static**: статические адреса;

blackhole: фильтруемые адреса;

aging-time <aging-time>: время жизни адресов;

count: счетчик адресов;

multicast: multicast-адреса;

<mac-addr>: MAC-адреса;

<vlan-id>: номер VLAN;

<interface-name>: имя интерфейса.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Таблица MAC-адресов не выведена на дисплей.

Описание: С помощью этой команды можно выводить на дисплей информацию о MAC-адресах, используя разные критерии сортировки. Для вывода на дисплей всех MAC-адресов используйте команду `show mac-address-table`.

Пример: Вывести на дисплей все MAC-адреса.

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

```
Read mac address table....
```

Vlan	Mac Address	Type	Creator	Ports
1	00-1a-81-00-18-9e	DYNAMIC	Hardware	Port-Channell
1	00-80-c8-f8-72-c2	DYNAMIC	Hardware	Ethernet0/0/14

8.2 Команды для настройки привязки MAC-адресов

8.2.1 clear port-security dynamic

Синтаксис: `clear port-security dynamic [address <mac-addr> | interface <interface-id>]`

Назначение: Очищает динамические MAC-адреса для указанного порта.

Режим конфигурирования: Привилегированный режим

Параметры: <mac-addr>: MAC-адрес;

<interface-id>: номер порта.

Описание: Для того, чтобы удаление динамических MAC-адресов стало возможным, безопасный порт сначала необходимо заблокировать. Если порты и MAC-адреса не указаны, будут удалены все динамические MAC-адреса на заблокированных безопасных портах. Если указан только порт, а MAC-адрес – не указан, будут удалены все MAC-адреса указанного порта.

Пример: Удалить все динамические MAC-адреса порта 1.

```
Switch#clear port-security dynamic interface Ethernet 0/0/1
```

8.2.2 show port-security

Синтаксис: show port-security

Назначение: Выводит на дисплей безопасный адрес порта.

Режим конфигурирования: Привилегированный режим, другие режимы конфигурирования.

Значение по умолчанию: Настройки безопасных портов не отображаются на дисплее.

Описание: Эта команда позволяет вывести на дисплей детальную информацию по настройке безопасных MAC-адресов на портах.

Пример:

```
Switch#show port-security
Security Port      MaxSecurity Addr      CurrentAddr      Security Action  (count)
(count)
Ethernet0/0/1     1                      1                Protect
Ethernet0/0/1     10                     1                Protect
Max Addresses limit in System :128
Total Addresses in System :2
```

Надписи в таблице	Описание
Security Port	Безопасный порт
MaxSecurityAddr	Максимальное число безопасных адресов
CurrentAddr	Текущий MAC-адрес безопасного порта
Security Action	Действия системы безопасности, выполняемые для порта
Total Addresses in System	Количество безопасных MAC-адресов в системе
Max Addresses limit in System	Предельное значение, установленное в системе для максимального числа безопасных MAC-адресов

8.2.3 show port-security address

Синтаксис: show port-security address [interface <interface-id>]

Назначение: Выводит на дисплей безопасный MAC-адрес порта.

Режим конфигурирования: Привилегированный режим, другие режимы конфигурирования.

Параметры: <interface-id>: порт, для которого на дисплей выводится адрес.

Описание: Эта команда позволяет вывести на дисплей информацию о безопасном MAC-адресе порта. Если порт не указан, отображаются безопасные MAC-адреса всех портов.

Пример:

```
Switch#show port-security address interface ethernet 0/0/1 Security Mac
Address Table
Vlan Mac Address Type  Ports  0000.0000.1111 SecureConfigured
Ethernet0/0/1
Total Addresses : 1
```

Надписи в таблице	Описание
Vlan	VLAN ID для безопасного MAC-адреса
Mac Address	Безопасный MAC-адрес.

Type	Тип безопасного MAC-адреса.
Ports	Порт, которому принадлежат безопасные MAC-адреса.
Total Addresses	Номер текущего безопасного MAC-адреса в системе.

8.2.4 show port-security interface

Синтаксис: `show port-security interface {<interface-id>}`

Назначение: Выводит на дисплей настройки безопасного порта.

Режим конфигурирования: Привилегированный режим, другие режимы конфигурирования.

Параметры: `<interface-id>`: порт, для которого на дисплей выводятся настройки.

Значение по умолчанию: Настройки безопасности порта не отображаются на дисплее.

Описание: Эта команда позволяет вывести на дисплей детальную информацию для безопасного порта.

Пример:

```
Switch#show port-security interface ethernet 0/0/1
Port Security : Enabled
Port status : Security Up
Violation mode : Protect
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Lock Timer is ShutDown
Mac-Learning function is : Opened
```

Надписи в таблице	Описание
Port Security :	Включена или нет система безопасности для порта.
Port status :	Состояние безопасности порта.
Violation mode :	Режим запрета, установленный для порта.
Maximum MAC Addresses :	Максимальное число безопасных MAC-адресов, заданное для порта
Total MAC Addresses :	Количество безопасных MAC-адресов порта.
Configured MAC Addresses :	Количество безопасных безопасных статических MAC-адресов порта.
Lock Timer	Включен или нет таймер блокирования порта.
Mac-Learning function	Доступно или нет обучение MAC-адресам для порта.

8.2.5 switchport port-security

Синтаксис: `switchport port security`

`no switchport port security`

Назначение: Включает функцию привязки MAC-адресов. Отмена команды `no switchport-security` выключает функцию привязки MAC-адресов для порта и восстанавливает для него режим обучения MAC-адресам.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Привязка MAC-адресов не включена.

Описание: Привязка MAC-адресов, протокол Spanning Tree и агрегирование порта являются взаимоисключающими. Поэтому, если включена функция привязки MAC-адреса к порту, протокол Spanning Tree и агрегирование порта должны быть выключены. Кроме того, порт, на котором включена привязка MAC-адресов, не должен быть магистральным портом.

Пример: Включить функцию привязки MAC-адреса для порта 1.
Switch(config)#interface Ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#switchport port security

8.2.6 switchport port-security convert

Синтаксис: `switchport port-security convert`

Назначение: Преобразует безопасные динамические MAC-адреса, которым обучился порт, в безопасные статические MAC-адреса.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Команда преобразования динамического MAC-адреса в статический может быть выполнена только после того, как безопасный порт будет заблокирован. После выполнения команды, безопасные динамические MAC-адреса, которым был обучен порт, будут преобразованы в безопасные статические MAC-адреса. Команда не сохраняет настройки.

Пример: Преобразовать MAC-адреса порта 1 в статические безопасные MAC-адреса.
Switch(config)#interface Ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#switchport port-security convert

8.2.7 switchport port-security lock

Синтаксис: `switchport port-security lock`

`no switchport port-security lock`

Назначение: Блокирует порт. Если порт заблокирован, обучение MAC-адресам для порта будет выключено. Отмена команды `no switchport port-security lock` восстанавливает обучение MAC-адресам.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Все интерфейсы не заблокированы.

Описание: Эта команда доступна только в том случае, если предварительно была включена функция привязки MAC-адреса. Если порт заблокирован, обучение динамическим MAC-адресам для порта будет выключено.

Примеры: Блокировать порт 1.
Switch(config)#interface Ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#switchport port-security lock

8.2.8 switchport port-security mac-address

Синтаксис: `switchport port-security mac-address {<mac-address>}`

`no switchport port-security mac-address {<mac-address>}`

Назначение: Добавляет безопасный статический MAC-адрес. Отмена команды `no switchport port-security mac-address` удаляет безопасный статический MAC-адрес.

Режим конфигурирования: Режим настройки интерфейсов.

Параметры: `<mac-address>`: добавляемый или удаляемый MAC-адрес.

Описание: Для того, чтобы добавление безопасного статического MAC-адреса стало возможным, предварительно должна быть включена функция привязки MAC-адресов.

Пример: Добавить MAC-адрес 00-1a-81-00-18-9e для порта 1.
Switch(config)#interface Ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#switchport port-security mac-address 00-1a-81-00-18-9e

8.2.9 switchport port-security maximum

Синтаксис: `switchport port-security maximum {<value>}`

`no switchport port-security maximum`

Назначение: Задаёт максимальное число безопасных MAC-адресов для порта. Отмена команды **no switchport port-security maximum** восстанавливает значение, используемое по умолчанию – максимальное число безопасных MAC-адресов равно 1.

Режим конфигурирования: Режим настройки интерфейсов.

Параметры: **<value>**: предельное число безопасных статических MAC-адресов, от 1 до 128.

Значение по умолчанию: Максимальное число безопасных MAC-адресов равно 1.

Описание: Для того, чтобы стало возможно задать максимальное число безопасных статических MAC-адресов, предварительно должна быть включена функция привязки MAC-адресов. Если число безопасных статических MAC-адресов порта больше заданного в команде максимального числа, настройка будет считаться неправильной; лишние MAC-адреса должны быть удалены. Если число безопасных статических MAC-адресов порта меньше заданного в команде максимального числа, команда будет выполнена успешно.

Пример: Задать максимальное число MAC-адресов для портов 1 – 4.

```
Switch(config)#interface Ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)# switchport port-security maximum 4
```

8.2.10 switchport port-security timeout

Синтаксис: **switchport port-security timeout <value> no switchport port-security timeout**

Назначение: Устанавливает таймер блокирования порта. Отмена команды **no switchport port-security timeout** восстанавливает настройки, используемые по умолчанию.

Параметры: **<value>** : значение времени таймера, в пределах от 0 до 300 с.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Таймер блокирования порта не включен.

Описание: Функция таймера блокирования порта – это функция блокирования динамических MAC-адресов. По истечении времени таймера блокирования, MAC-адреса будут блокированы, при этом динамические MAC-адреса будут преобразованы в безопасные адреса. До ввода этой команды должна быть включена функция привязки MAC-адреса.

Пример: Установить таймер блокирования порта на 30 секунд.

```
Switch(config)#interface Ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)# switchport port-security timeout 30
```

8.2.11 switchport port-security violation

Синтаксис: **switchport port-security violation {protect | shutdown} [recovery <30-3600>] no switchport port-security violation**

Назначение: Задаёт для порта режим запрета. Отмена команды **no switchport port-security violation** выключает режим запрета, при этом восстанавливается режим защиты порта.

Режим конфигурирования: Режим настройки портов.

Параметры: **protect**: переход в режим защиты порта; **shutdown**: переход в режим, в котором порт выключается; **recovery**: автоматический возврат порта в исходный режим спустя время в диапазоне от 30 до 3600 сек.

Значение по умолчанию: Установлен режим защиты порта.

Описание: Настройка режима запрета порта возможна только в том случае, если предварительно включена функция привязки MAC-адреса. Когда число безопасных MAC-адресов превышает установленное предельное значение и установлен режим порта **protect**, для порта только будет выключено обучение динамическим MAC-адресам. В остальных случаях порт будет выключен. Пользователи могут вручную включить порт с помощью команды **no shutdown**.

Пример: Установить для порта 1 режим, в котором он выключен (**shutdown**).

```
Switch(config)#interface Ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#switchport port-security violation shutdown
```

9 Команды для настройки протокола MSTP

9.1 Команды работы с протоколом MSTP

9.1.1 show

Синтаксис: show

Назначение: Выводит на дисплей информацию о работающей в данный момент системе.

Режим конфигурирования: Режим настройки регионов MSTP.

Описание: Команда позволяет получить подробную информацию о работающей в данный момент системе.

Пример: Вывести на дисплей информацию о работающей системе.

```
Switch(Config-Mstp-Region)#show
```

9.1.2 abort

Синтаксис: abort

Назначение: Отменяет текущую настройку региона MSTP, осуществляет выход из режима настройки регионов MSTP в глобальный режим конфигурирования.

Режим конфигурирования: Режим настройки регионов MSTP.

Описание: Эта команда выполняет выход из режима настройки регионов MSTP в глобальный режим конфигурирования без сохранения текущих настроек. При этом начинают использоваться предыдущие настройки региона MSTP.

Пример: Выйти из режима настройки регионов MSTP без сохранения сделанных настроек.

```
Switch(Config-Mstp-Region)#abort  
Switch(config)#
```

9.1.3 exit

Синтаксис: exit

Назначение: Сохраняет текущую настройку региона MSTP, затем осуществляет выход из режима настройки регионов MSTP в глобальный режим конфигурирования.

Режим конфигурирования: Режим настройки регионов MSTP

Описание: Эта команда сохраняет сделанные настройки, а затем выполняет выход из режима настройки регионов MSTP в глобальный режим конфигурирования.

Пример: Выйти из режима настройки регионов MSTP с сохранением сделанных настроек.

```
Switch(Config-Mstp-Region)#exit  
Switch(config)#
```

9.1.4 instance vlan

Синтаксис: instance {<instance-id>} vlan {<vlan-list>}

no instance {<instance-id>} [vlan <vlan-list>]

Назначение: В режиме настройки регионов MSTP эта команда позволяет создать экземпляр связующего дерева и задать соответствия между VLAN и экземплярами связующего дерева. Отмена команды **no instance <instance-id> [vlan <vlan-list>]** удаляет указанный экземпляр связующего дерева и указанные соответствия между VLAN и экземплярами связующего дерева.

Параметры: <instance-id>: номер экземпляра связующего дерева. Диапазон значений - от 0 до 48. В команде **no instance <instance-id> [vlan <vlan-list>]** <instance-id> обозначает номер экземпляра связующего дерева. Диапазон значений - от 1 до 48.

<vlan-list>: задает последовательность номеров VLAN, либо отдельные номера VLAN. “-” используется для ввода последовательности номеров, символ “;” позволяет ввести отдельные номера с помощью их перечисления.

Режим конфигурирования: Режим настройки регионов MSTP

Значение по умолчанию: До создания экземпляров связующего дерева имеется всего один экземпляр с номером 0, которому принадлежат все VLAN 1 - 4094 .

Описание: Эта команда позволяет задать соответствие между VLAN и экземплярами связующего дерева. Коммутаторы считаются принадлежащими одному и тому же региону MSTP только в том случае, если одинаковы все заданные соответствия и другие атрибуты. До настройки экземпляров связующего дерева все VLAN принадлежат экземпляру 0. Протокол MSTP может поддерживать не более 48 экземпляров MSTI (не считая экземпляры общих связующих деревьев CIST). Общее связующее дерево CIST можно трактовать, как экземпляр дерева MSTI с номером 0. Все остальные экземпляры имеют номера с 1 по 48.

Пример: Поставить в соответствие VLAN 1-10 и VLAN 100-110 экземпляру связующего дерева 1.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110
```

9.1.5 name

Синтаксис: name <name>

no name

Назначение: В режиме настройки регионов MSTP позволяет задать имя региона MSTP; команда **no name** восстанавливает настройки, заданные по умолчанию.

Параметры: <name>: имя региона MSTP. Длина имени не должна превышать 32 символов.

Режим конфигурирования: Режим настройки регионов MSTP

Значение по умолчанию: Пустое значение.

Описание: Команда используется для задания имени региона MSTP. Коммутаторы с одинаковыми именами региона MSTP и одинаковыми другими атрибутами рассматриваются, как один и тот же регион MSTP.

Пример: Задать имя региона MSTP: mstp-test.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#name mstp-test
```

9.1.6 no

Синтаксис: no <instance-id> | <name> | <revision-level>

Назначение: Отменяет команду или устанавливает начальное значение.

Параметры: <instance-id>: Идентификатор ID экземпляра связующего дерева MSTP.

<name>: имя региона MSTP,

<revision-level>: счетчик номеров версий настроек MST.

Режим конфигурирования: Режим настройки регионов MSTP

Значение по умолчанию: 0.

Описание: Команда позволяет удалить указанный экземпляр и имя региона MSTP, восстановить значение, используемое по умолчанию (0).

Пример: Удалить экземпляр связующего дерева 1.

```
Switch(Config-Mstp-Region)#no instance 1
```

9.1.7 revision-level

Синтаксис: `revision-level <level>`

`no revision-level`

Назначение: В режиме MSTP, позволяет задать номер версии настроек конфигурирования MSTP. Отмена команды `no revision-level` восстанавливает настройку по умолчанию: 0.

Параметры: `<level>`: номер версии. Допустимые значения – от 0 до 65535.

Режим конфигурирования: Режим настройки регионов MSTP.

Значение по умолчанию: 0.

Описание: Эта команда позволяет задать номер версии настроек MSTP. Коммутаторы с одинаковыми именами региона MSTP и одинаковыми другими атрибутами рассматриваются, как один и тот же регион MSTP.

Пример: Установить номер версии 2000.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#revision-level 2000
```

9.1.8 spanning-tree

Синтаксис: `spanning-tree`

`no spanning-tree`

Назначение: В глобальном режиме конфигурирования и в режиме настройки интерфейсов включает протокол MSTP. Отмена команды `no spanning-tree` выключает протокол MSTP.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов

Значение по умолчанию: Протокол MSTP не включен.

Описание: Если в глобальном режиме конфигурирования протокол MSTP включен, то он включен на всех портах, за исключением тех, для которых использование MSTP выключено.

Пример: Включить MSTP в глобальном режиме конфигурирования, выключить MSTP в интерфейсе 0/0/2.

```
Switch(config)#spanning-tree
Switch(config)#interface ethernet 0/0/2
Switch(Config-If-Ethernet0/0/2)#no spanning-tree
```

9.1.9 spanning-tree forward-time

Синтаксис: `spanning-tree forward-time <time>`

`no spanning-tree forward-time`

Назначение: Позволяет установить время задержки (forward delay) передачи на коммутаторе. Отмена команды `no spanning-tree forward-time` восстанавливает настройки, используемые по умолчанию.

Параметры: `<time>`: время задержки передачи в секундах.

Допустимые значения – от 4 до 30.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Установлено время задержки форвардинга 15 секунд.

Описание: Когда топология сети изменяется, состояние порта меняется с блокирующего (blocking) на состояние, в котором передача разрешена (forwarding). Задержка, возникающая при таком изменении состояния порта, называется задержкой передачи. Задержка форвардинга связана с задержкой hello time и максимальным сроком жизни (max age).

Пример: В глобальном режиме конфигурирования задать время задержки передачи MSTP 20 секунд.

```
Switch(config)#spanning-tree forward-time 20
```

9.1.10 spanning-tree hello-time

Синтаксис: `spanning-tree hello-time <time>`

`no spanning-tree hello-time`

Назначение: Позволяет установить время hello time на коммутаторе. Отмена команды `no spanning-tree hello-time` восстанавливает настройки, используемые по умолчанию.

Параметры: `<time>`: время задержки hello time в секундах. Допустимые значения – от 1 до 10.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 2 секунды.

Описание: Время hello time – интервал времени, по прошествии которого, коммутатор посылает сообщения BPDU. Время hello time связано с задержкой передачи (forward delay) и максимальным сроком жизни (max age).

Пример: Установить время hello time протокола MSTP 5 секунд в глобальном режиме конфигурирования.

```
Switch(config)#spanning-tree hello-time 5
```

9.1.11 spanning-tree cost

Синтаксис: `spanning-tree cost <cost>`

`no spanning-tree cost`

Назначение: Позволяет задать метрику маршрута к текущему порту в указанном экземпляре связующего дерева. Отмена команды `no spanning-tree mst <instance-id> cost` восстанавливает настройки, используемые по умолчанию.

Параметры: `<cost>`: метрика маршрута. Допустимые значения – от 1 до 200 000 000.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Метрика маршрута к порту соответствует пропускной способности порта.

Тип порта	Метрика маршрута к порту, используемая по умолчанию	Предполагаемый диапазон
10Mbps	2000000	2000000 — 00000
100Mbps	200000	200000 — 2000000
1Gbps	20000	20000 — 200000
10Gbps	2000	2000 — 20000

Для агрегированных портов, метрики маршрутов, используемые по умолчанию, следующие:

Тип порта	Допустимое число агрегированных портов	Метрика маршрута, используемая по умолчанию
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N
10Gbps	N	2000/N

Описание: Установив метрику для порта, пользователи могут контролировать метрику маршрута от текущего порта до корневого порта коммутатора. Это необходимо для управления выбором корневого порта и порта назначения для экземпляра связующего дерева.

Пример: В порте 0/0/2 установить метрику MSTP 3000000.

```
Switch(Config-If-Ethernet0/0/2)#spanning-tree cost 3000000
```

9.1.12 spanning-tree link-type p2p

Command: `spanning-tree link-type p2p {auto | force-true | force-false}`

no spanning-tree link-type

Назначение: Отмена команды **no spanning-tree link-type** восстанавливает тип линии, полученный при автоматическом согласовании.

Параметры: **auto:** использовать автоматическое согласование, **force-true:** принудительно устанавливает тип линии «точка-точка», **force-false:** принудительно устанавливает для линии тип «не точка-точка».

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Установлен тип линии auto, MSTP определяет тип линии автоматически.

Описание: Если порт работает в режиме полного дуплекса, MSTP устанавливает для линии порта тип «точка-точка». Если порт работает в режиме полудуплекса, MSTP устанавливает для линии порта тип «разделяемая».

Пример: Принудительно установить для порта 0/0/7-8 тип «точка-точка».
`Switch(config)#interface ethernet 0/0/7-8`
`Switch(Config-Port-Range)#spanning-tree link-type p2p force-true`

9.1.13 spanning-tree maxage

Синтаксис: `spanning-tree maxage <time>`

no spanning-tree maxage

Назначение: Позволяет установить максимальный срок жизни (max age) для BPDU. Отмена команды **no spanning-tree maxage** восстанавливает настройки, используемые по умолчанию.

Параметры: **<time>:** время максимального срока жизни в секундах. Допустимые значения – от 6 до 40.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Установлен максимальный срок жизни 20 секунд.

Описание: Срок жизни BPDU называется максимальным сроком жизни. Максимальный срок жизни связан с задержкой передачи (forward delay) и с задержкой hello time.

Пример: В глобальном режиме конфигурирования задать максимальный срок жизни адреса коммутатора 25 секунд.
`Switch(config)#spanning-tree maxage 25`

9.1.14 spanning-tree max-hop

Синтаксис: `spanning-tree max-hop <hop-count>`

no spanning-tree max-hop

Назначение: Позволяет задать максимальное число хопов BPDU в регионе MSTP. Отмена команды **no spanning-tree max-hop** восстанавливает значения, используемые по умолчанию.

Параметры: **<hop-count>:** задает максимальное число хопов. Допустимые значения – от 1 до 40.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Установлено максимальное число хопов, равное 20.

Описание: В протоколе MSTP для подсчета срока жизни BPDU используется максимальный срок жизни (max age). Кроме того, в протоколе MSTP для подсчета срока жизни BPDU используется и максимальное число хопов. Максимальное число хопов в сети уменьшается. Максимальное число хопов BPDU имеет максимальное значение при инициализации, выполняемой корневым коммутатором MST1. После того, как сообщение BPDU принято, максимальное число хопов уменьшается на 1. После того, как порт примет сообщение BPDU при

максимальном числе хопов равно 0, он отбрасывает это сообщение BPDU и объявляет себя портом назначения (designated port), чтобы посылать сообщения BPDU.

Пример: Установить максимальное число хопов 32.

```
Switch(config)#spanning-tree max-hop 32
```

9.1.15 spanning-tree mcheck

Синтаксис: spanning-tree mcheck

Назначение: Принудительно устанавливает для порта режим работы MSTP.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Порт работает в режиме MSTP.

Описание: Если сеть, которая подключена к текущему порту работает по протоколу IEEE 802.1D STP, порт автоматически преобразуется для работы в режиме STP. Команда используется для принудительной установки для порта режима MSTP. Однако, как только порт примет сообщение STP, он снова переключится в режим STP. Эта команда может использоваться только в том случае, когда коммутатор работает в режиме IEEE 802.1s MSTP. Если коммутатор работает в режиме IEEE 802.1D STP, то применение этой команды некорректно.

Пример: Принудительно установить для порта 0/0/2 режим работы MSTP.

```
Switch(Config-If-Ethernet0/0/2)#spanning-tree mcheck
```

9.1.16 spanning-tree mode

Синтаксис: spanning-tree mode {mstp | stp | rstp}

no spanning-tree mode

Назначение: Позволяет установить на коммутаторе режим spanning-tree. Отмена команды **no spanning-tree mode** восстанавливает настройки, используемые по умолчанию.

Параметры: **mstp:** устанавливает в коммутаторе режим IEEE 802.1s MSTP;

stp: устанавливает в коммутаторе режим IEEE 802.1D STP;

rstp: устанавливает в коммутаторе режим IEEE 802.1D RSTP;

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Коммутатор работает в режиме MSTP.

Описание: Когда коммутатор работает в режиме IEEE 802.1D STP, он посылает сообщения BPDU стандарта IEEE 802.1D и TCN BPDU. Он отбрасывает все BPDU протокола MSTP.

Пример: Установить на коммутаторе режим STP.

```
Switch(config)#spanning-tree mode stp
```

9.1.17 spanning-tree mst configuration

Синтаксис: spanning-tree mst configuration

no spanning-tree mst configuration

Назначение: Позволяет войти в режим конфигурирования MSTP. В режиме конфигурирования MSTP можно задать атрибуты MSTP. Отмена команды **no spanning-tree mst configuration** восстанавливает значения атрибутов MSTP, используемые по умолчанию.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Значения атрибутов региона MSTP, используемые по умолчанию, приведены ниже:

Параметры MSTP	Значения по умолчанию
Instance (экземпляр)	Существует только один экземпляр связующего дерева 0. Все VLAN (1 — 4094) привязаны к экземпляру 0.
Name (Имя)	Пусто
Номер версии	0

Описание: Коммутатор может находиться в режиме настройки регионов MSTP или в другом режиме, пользователи могут войти в режим конфигурирования MSTP, настроить атрибуты и сохранить эти настройки. Когда коммутатор работает в режиме MSTP, система генерирует идентификатор конфигурации MST, соответствующий конфигурации MSTP. Только коммутаторы с одинаковыми идентификаторами конфигурации MST считаются коммутаторами одного и того же региона.

Пример: Войти в режим настройки регионов MSTP.
 Switch(config)#spanning-tree mst configuration
 Switch(Config-Mstp-Region)#

9.1.18 spanning-tree mst cost

Синтаксис: spanning-tree mst <instance-id> cost <cost>

no spanning-tree mst <instance-id> cost

Назначение: Позволяет задать метрику маршрута к текущему порту в указанном экземпляре связующего дерева. Отмена команды **no spanning-tree mst <instance-id> cost** восстанавливает настройки, используемые по умолчанию.

Параметры: <instance-id>: Идентификатор (ID) экземпляра связующего дерева. Диапазон значений – от 0 до 48.

<cost>: метрика маршрута. Диапазон значений – от 1 до 200 000 000.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Метрика маршрута к порту соответствует пропускной способности порта.

Тип порта	Метрика маршрута к порту, используемая по умолчанию	Предполагаемый диапазон
10Mbps	2000000	2000000 — 000000
100Mbps	200000	200000 — 2000000
1Gbps	20000	20000 — 200000
10Gbps	2000	2000 — 20000

Для агрегированных портов, метрики маршрутов, используемые по умолчанию, следующие:

Тип порта	Допустимое число агрегированных портов	Метрика маршрута, используемая по умолчанию
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N
10Gbps	N	2000/N

Описание: Установив метрику для порта, пользователи могут контролировать метрику маршрута от текущего порта до корневого порта моста. Это необходимо для управления выбором корневого порта и порта назначения для экземпляра связующего дерева.

Пример: В порте 0/0/2 установить метрику MSTP порта 3000000 для экземпляра связующего дерева 2.
 Switch(Config-If-Ethernet0/0/2)#spanning-tree mst 2 cost 3000000

9.1.19 spanning-tree mst loopguard

Синтаксис: spanning-tree [mst <instance-id>] loopguard

no spanning-tree [mst <instance-id>] loopguard

Назначение: Позволяет задействовать функцию loopguard для указанного экземпляра связующего дерева.

Параметры: <instance-id>: Идентификатор (ID) экземпляра связующего дерева. Диапазон значений – от 0 до 48.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Функция выключена.

Описание: Данная функция позволяет избежать возникновения петель в случае возникновения однонаправленных соединений, когда кадры BPDU отправляются, но не принимаются.

Пример:

```
Switch(Config)#interface ethernet 0/0/2
Switch(Config-Ethernet-0/0/2)#spanning-tree mst 0 loopguard
```

9.1.20 spanning-tree mst port-priority

Синтаксис: `spanning-tree mst <instance-id> port-priority <port-priority>`

`no spanning-tree mst <instance-id> port-priority`

Назначение: Позволяет задать приоритет порта для указанного экземпляра связующего дерева. Отмена команды `no spanning-tree mst <instance-id> port-priority` восстанавливает настройки, используемые по умолчанию.

Параметры: `<instance-id>`: Идентификатор (ID) экземпляра связующего дерева. Диапазон значений – от 0 до 48.

`<port-priority>`: приоритет порта. Допустимые значения — от 0 до 240. Значение должно быть кратно 16, например, 0, 16, 32...240.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Установлен приоритет порта 128.

Описание: Задавая приоритет порта, пользователи могут управлять ID порта экземпляра связующего дерева, чтобы управлять корневым портом и портом назначения этого экземпляра. Чем меньше значение приоритета порта, тем выше его приоритет.

Пример: Установить приоритет порта 32 на порту 0/0/2 экземпляра связующего дерева 1.

```
Switch(config)#interface ethernet 0/0/2
Switch(Config-If-Ethernet0/0/2)#spanning-tree mst 1 port-priority 32
```

9.1.21 spanning-tree mst priority

Синтаксис: `spanning-tree mst <instance-id> priority <bridge-priority>`

`no spanning-tree mst <instance-id> priority`

Назначение: Позволяет задать приоритет коммутатора для указанного экземпляра связующего дерева. Отмена команды `no spanning-tree mst <instance-id> priority` восстанавливает настройки, используемые по умолчанию.

Параметры: `<instance-id>`: Идентификатор (ID) экземпляра связующего дерева. Диапазон значений – от 0 до 48.

`<bridge-priority>`: приоритет коммутатора. Допустимые значения — от 0 до 61440. Значение должно быть кратно 4096, например, 0, 4096, 8192...61440.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Установлен приоритет порта 32768.

Описание: Задавая приоритет коммутатора, пользователи могут изменять ID коммутатора для указанного экземпляра связующего дерева. ID коммутатора может влиять на выбор корневого коммутатора и порта назначения коммутатора для указанного экземпляра связующего дерева.

Пример: Установить приоритет 4096 для экземпляра связующего дерева 2.

```
Switch(config)#spanning-tree mst 2 priority 4096
```

9.1.22 spanning-tree mst rootguard

Синтаксис: `spanning-tree [mst <instance-id>] rootguard`

`no spanning-tree [mst <instance-id>] rootguard`

Назначение: Включает функцию защиты корневого порта (rootguard function) для указанного экземпляра связующего дерева. Функция rootguard запрещает порту быть корневым

портом MSTP. Отмена команды **no spanning-tree mst <instance-id> rootguard** выключает функцию rootguard.

Параметры: **<instance-id>**: Идентификатор (ID) экземпляра связующего дерева MSTP.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Функция rootguard не включена.

Описание: Команда используется в режиме настройки интерфейсов. Если для порта функция rootguard включена, ему запрещено быть корневым портом дерева MSTP. Если от порта, для которого включена функция rootguard, принят пакет BPDU более высокого уровня иерархии, протокол MSTP не вычисляет связующее дерево. Он просто задает состояние порта root_inconsistent (порт не может быть корневым) и блокирует порт. Если пакет BPDU более высокого уровня иерархии не принят от порта, для которого включена функция rootguard, состояние порта будет восстановлено – ему будет разрешена передача. Функция rootguard может использоваться для обслуживания относительно стабильных топологий связующего дерева при добавлении в сеть нового коммутатора.

Пример: Включить функцию rootguard для порта 0/0/2 экземпляра связующего дерева 0.
Switch(config)#interface ethernet 0/0/2
Switch(Config-If-Ethernet0/0/2)#spanning-tree mst 0 rootguard

9.1.23 spanning-tree port-priority

Синтаксис: **spanning-tree port-priority <port-priority>**

no spanning-tree port-priority

Назначение: Позволяет установить приоритет порта. Отмена команды **no spanning-tree port-priority** восстанавливает настройки, используемые по умолчанию.

Параметры: **<port-priority>**: приоритет порта. Допустимые значения — от 0 до 240. Значение должно быть кратно 16, например, 0, 16, 32, 48...240.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Установлен приоритет порта 32768.

Описание: Команда позволяет установить приоритет для указанного порта. Чем меньше значение приоритета порта, тем выше его приоритет.

Пример: Установить приоритет 32 для порта 1.
Switch(Config-If-Ethernet0/0/1)#spanning-tree port-priority 32

9.1.24 spanning-tree rootguard

Синтаксис: **spanning-tree rootguard**

no spanning-tree rootguard

Назначение: Включает функцию защиты корневого порта. Отмена команды **no spanning-tree rootguard** выключает режим защиты корневого порта.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Порт не является корневым.

Описание: Команда используется в режиме настройки интерфейсов. Если для порта функция rootguard включена, ему запрещено быть корневым портом дерева MSTP. Если от порта, для которого включена функция rootguard, принят пакет BPDU более высокого уровня иерархии, протокол MSTP не вычисляет связующее дерево. Он просто задает состояние порта root_inconsistent (порт не может быть корневым) и блокирует порт. Если пакет BPDU более высокого уровня иерархии не принят от порта, для которого включена функция rootguard, состояние порта будет восстановлено – ему будет разрешена передача. Функция rootguard может использоваться для обслуживания относительно стабильных топологий связующего дерева при добавлении в сеть нового коммутатора.

Пример: Включить для порта 1 режим корневого порта.
Switch(Config-If-Ethernet0/0/1)#spanning-tree rootguard

9.1.25 spanning-tree portfast

Синтаксис: `spanning-tree portfast [bpdufilter | bpduguard]`

`no spanning-tree portfast`

Назначение: Объявляет текущий порт граничным портом, выполняющим фильтрацию пакетов BPDU. Режим защиты BPDU может быть указан в команде, либо использоваться по умолчанию. Отмена команды **no spanning-tree portfast** объявляет порт не принадлежащим границе.

Параметры: **bpdufilter:** для фильтрации пакетов BPDU устанавливает в порту режим граничного порта;

bpduguard: устанавливает защиту BPDU для граничного порта.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: После включения протокола MSTP все порты не являются граничными портами.

Описание: Когда порт объявлен граничным портом, его состояние преобразуется из discarding (отбрасывание пакетов BPDU) в состояние, в котором разрешена передача, при этом задержка передачи (forward delay) отсутствует. Как только граничный порт принимает пакет BPDU, он вновь становится неграничным портом.

Пример: Включить в граничном порту режим фильтрации пакетов BPDU.

```
Switch(config)#interface ethernet 0/0/2
Switch(Config-If-Ethernet0/0/2)#spanning-tree portfast bpdufilter
```

9.1.26 spanning-tree priority

Синтаксис: `spanning-tree priority <bridge-priority>`

`no spanning-tree priority`

Назначение: Позволяет задать приоритет коммутатора. Отмена команды **no spanning-tree priority** восстанавливает настройки, используемые по умолчанию.

Параметры: **<bridge-priority>**: приоритет коммутатора. Допустимые значения — от 0 до 61440. Значение должно быть кратно 4096, например, 0, 4096, 8192...61440.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Установлен приоритет коммутатора 32768.

Описание: Задавая приоритет коммутатора, пользователи могут изменять ID коммутатора. Приоритет коммутатора может влиять на выбор корневого коммутатора и заданных портов. Чем меньше значение приоритета коммутатора, тем выше его приоритет.

Пример: Установить приоритет коммутатора равным 4096.

```
Switch(config)#spanning-tree priority 4096
```

9.1.27 spanning-tree format

Синтаксис: `spanning-tree format {standard | privacy | auto}`

`no spanning-tree format`

Назначение: Позволяет настроить формат пакета для взаимодействия с оборудованием других изготовителей. Отмена команды **no spanning-tree format** восстанавливает настройки, используемые по умолчанию.

Параметры: **Standard:** формат пакета, соответствующий стандарту IEEE.

Privacy: специальный формат пакета, совместимый с оборудованием CISCO.

Auto: автоматическое определение формата пакета на основе принятых пакетов.

Значение по умолчанию: автоматическое определение формата пакета на основе принятых пакетов.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Так как формат пакетов CISCO отличается от формата IEEE, многие компании поддерживают также и формат CISCO. Наша компания также поддерживает оба формата. Стандартный формат пакета разработан IEEE, специальный формат пакета поддерживает оборудование CISCO. Если Вы не имеете полной информации о том, какой формат пакетов используется на оборудовании других производителей, подключенном к коммутатору, настройка AUTO является более предпочтительной — формат будет определен по принятым пакетам. По умолчанию установлено определение формата по принятым пакетам (AUTO) для лучшей совместимости с уже существующей продукцией и продукцией других компаний. Если установлен режим AUTO, то до первого принятого пакета будет использоваться специальный формат пакетов.

Когда опция AUTO не выбрана и первый принятый от партнеров пакет не согласуется с установленным форматом, для порта установлено состояние DISCARDING (отбрасывание пакетов), что приведет к отбрасыванию несогласующихся пакетов. Это предотвращает ситуацию, когда обе стороны считают, что у них находится корневой узел сети.

Когда опция AUTO выбрана и к порту подключено несовместимое оборудование (например, оборудование подключено через концентратор (HUB), либо используется прозрачная передача BPDU по нескольким направлениям, в которых используется протокол MSTP), будут записаны счетчики изменения формата и порт будет выключен при достижении счетчиками некоторого порогового значения. Включить порт снова может только пользователь с правами администратора.

Пример: Установить для порта формат пакетов IEEE.

```
Switch(config)#interface ethernet 0/0/2 Switch(Config-If-  
Ethernet0/0/2)#spanning-tree format standard
```

9.1.28 spanning-tree digest-snooping

Синтаксис: spanning-tree digest-snooping

no spanning-tree digest-snooping

Назначение: Устанавливает для порта режим использования строки аутентификации партнерского порта. Отмена команды **no spanning-tree digest-snooping** восстанавливает для порта использование генерированной портом строки аутентификации.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Строка аутентификации партнерского порта не используется.

Описание: В соответствии с протоколом MSTP, строка аутентификации региона автоматически генерируется алгоритмом MD5 с общедоступным ключом аутентификации, с ID экземпляра связующего дерева и VLAN ID. Некоторые производители не используют общедоступный ключ аутентификации. Это является причиной несовместимости. После ввода команды порт сможет использовать строку аутентификации партнерского порта, что обеспечит совместимость с оборудованием этих производителей.

Примечание: Так как строка аутентификации зависит от ID экземпляра связующего дерева и VLAN ID, команда может привести к распознаванию оборудования с отличающимися ID экземпляра связующего дерева и VLAN ID, как принадлежащего одному и тому же региону.

Перед выполнением команды удостоверьтесь в правильности соответствий VLAN и экземпляра связующего дерева для всего оборудования. Если подключено более одного оборудования, эта команда должна быть выполнена на всех подключенных портах.

Пример: Установить строку аутентификации партнерского порта.

```
Switch(config)#interface ethernet 0/0/2  
Switch(Config-If-Ethernet0/0/2)#spanning-tree digest-snooping
```

9.1.29 spanning-tree tcflush (глобальный режим конфигурирования)

Синтаксис: spanning-tree tcflush enable

spanning-tree tcflush disable

spanning-tree tcflush protect

no spanning-tree tflush

Назначение: Позволяет включить режим flush, в котором связующее дерево строится сразу, как только изменяется топология. Отмена команды **no spanning-tree tflush** восстанавливает настройки, используемые по умолчанию.

Параметры: enable: Связующее дерево строится сразу, как только изменяется топология.

disable: При изменении топологии связующее дерево не строится.

protect: Связующее дерево строится через каждые 10 секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: enable — связующее дерево строится сразу, как только изменяется топология.

Описание: В соответствии с протоколом MSTP, когда топология изменяется, порт посылает сообщение об изменении, которое очищает таблицу MAC/ARP (FLUSH). Фактически, для некоторых сетей нет необходимости выполнять операцию FLUSH при каждом изменении топологии. Однако для предотвращения атак на сеть администратор сети может настроить режим FLUSH с помощью этой команды.

Примечание: Для сложных сетей, особенно для тех, в которых необходимо быстрое переключение с одной ветви связующего дерева на другую ветвь, выключать режим изменения топологии не рекомендуется.

Пример: Выключить режим flush, в котором связующее дерево строится сразу, как только изменяется топология.

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

9.1.30 spanning-tree tflush (режим настройки интерфейсов)

Синтаксис: spanning-tree tflush {enable| disable| protect}

no spanning-tree tflush

Назначение: Позволяет включить режим flush, в котором связующее дерево строится сразу, как только изменяется топология. Отмена команды **no spanning-tree tflush** восстанавливает настройки, используемые по умолчанию.

Параметры:

enable: Связующее дерево строится сразу, как только изменяется топология.

disable: При изменении топологии связующее дерево не строится.

protect: Связующее дерево строится через каждые 10 секунд.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Настройки, сделанные в глобальном режиме конфигурирования.

Описание: В соответствии с протоколом MSTP, когда топология изменяется, порт посылает сообщение об изменении, которое очищает таблицу MAC/ARP (FLUSH). Фактически, для некоторых сетей нет необходимости выполнять операцию FLUSH при каждом изменении топологии. Однако для предотвращения атак на сеть, администратор сети может настроить режим FLUSH с помощью этой команды.

Примечание: Для сложных сетей, особенно для тех, в которых необходимо быстрое переключение с одной ветви связующего дерева на другую ветвь, выключать режим изменения топологии не рекомендуется.

Пример: Выключить режим flush, в котором связующее дерево строится сразу, как только изменяется топология.

```
Switch(config)#interface ethernet 0/0/2  
Switch(Config-If-Ethernet0/0/2)#spanning-tree tflush disable
```

9.2 Команды мониторинга и отладки MSTP

9.2.1 show spanning-tree

Синтаксис: `show spanning-tree [mst [<instance-id> | <config> | <detail> | <interface>]] [interface <interface-list>] [detail]`

Назначение: Выводит на дисплей информацию MSTP.

Параметры: <interface-list>: список интерфейсов;

<instance-id>: ID экземпляра связующего дерева. Допустимые значения – от 0 до 48;

<config>: информация конфигурирования региона работы;

<detail>: вывод подробной информации;

<interface>: порт;

detail: вывод подробной информации о связующем дереве;

Режим конфигурирования: Привилегированный режим

Описание: С помощью этой команды может быть выведена информация только для экземпляров связующего дерева текущего коммутатора.

Пример: Вывести на дисплей информацию о коммутаторе MSTP в виде таблиц:

```
Switch#show spanning-tree
-- MSTP Bridge Config Info --
Standard      : IEEE 802.1s
Bridge MAC    : 00:1a:81:00:18:9e
Bridge Times  : Max Age 20, Hello Time 2, Forward Delay 15
Force Version: 3
##### Instance 0 #####
Self Bridge Id : 32768 - 00:1a:81:00:18:9e
Root Id        : this switch
Ext.RootPathCost : 0
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID   : 0
Current port list in Instance 0:
Ethernet0/0/8 (Total 1)
  PortName      ID      ExtRPC  IntRPC  State Role      DsgBridge
DsgPort
-----
---
Ethernet0/0/8 128.008      0        0 FWD  DSGN 32768.001a8100189e
128.008
```

Параметры в таблице на экране	Описание
Информация о коммутаторе	
Standard	Версия STP
Bridge MAC	MAC-адрес коммутатора
Bridge Times	Максимальный срок жизни адреса, время hello time и задержка передачи для коммутатора
Force Version	Версия STP
Информация для экземпляра связующего дерева	
Self Bridge Id	Приоритет и MAC-адрес текущего коммутатора для текущего экземпляра связующего дерева
Root Id	Приоритет и MAC-адрес корневого коммутатора для текущего экземпляра связующего дерева
Ext.RootPathCost	Полная метрика для маршрута от текущего коммутатора до корневого узла всей сети
Int.RootPathCost	Метрика маршрута от текущего коммутатора до корневого

	узла региона для текущего экземпляра связующего дерева
Root Port ID	Корневой порт текущего экземпляра связующего дерева на текущем коммутаторе
Список портов MSTP текущего экземпляра связующего дерева	
PortName	Имя порта
ID	Приоритет порта и номер порта
ExtRPC	Метрика порта относительно корневого узла всей сети
IntRPC	Метрика маршрута от текущего порта до корневого узла региона текущего экземпляра связующего дерева
State	Состояние порта текущего экземпляра связующего дерева
Role	Роль порта текущего экземпляра связующего дерева
DsgBridge	Восходящий коммутатор назначения для текущего порта в текущем экземпляре связующего дерева
DsgPort	Восходящий порт назначения для текущего порта в текущем экземпляре связующего дерева

9.2.2 show spanning-tree mst config

Синтаксис: show spanning-tree mst config

Назначение: В привилегированном режиме выводит на дисплей настройки протокола MSTP.

Режим конфигурирования: Привилегированный режим

Описание: В привилегированном режиме эта команда позволяет вывести на дисплей параметры MSTP, например, имя MSTP, номер версии, привязки VLAN к экземплярам связующего дерева.

Пример: Вывести на дисплей настройки протокола MSTP.

```
Switch#show spanning-tree mst config
Name          Test
Revision      0
Instance      Vlans Mapped
-----
00            1-4094
-----
```

9.2.3 show mst-pending

Синтаксис: show mst-pending

Назначение: В режиме настройки регионов MSTP позволяет вывести на дисплей настройки текущего региона MSTP.

Режим конфигурирования: Привилегированный режим

Описание: В режиме настройки регионов MSTP позволяет вывести на дисплей настройки текущего региона MSTP – имя MSTP, номер версии, привязки VLAN к экземплярам связующего дерева.

Примечание: До выхода из режима настройки регионов MSTP показанные на дисплее параметры еще могут не возыметь действия.

Пример: Вывести на дисплей настройки для текущего региона MSTP.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#show mst-pending
Name          Test
Revision      0
Instance      Vlans Mapped
-----
00            1-4094
-----
Switch(Config-Mstp-Region)#
```

9.2.4 debug spanning-tree

Синтаксис: `debug spanning-tree`

`no debug spanning-tree`

Назначение: Включает вывод на дисплей отладочной информации MSTP. Отмена команды `no debug spanning-tree` прекращает вывод на дисплей отладочной информации MSTP.

Режим конфигурирования: Привилегированный режим

Описание: Команда позволяет включить вывод на дисплей всей отладочной информации MSTP. Сначала пользователи могут включить вывод всей отладочной информации, затем — выводить на дисплей только необходимую информацию. В целом эта команда предназначена для использования квалифицированным техническим персоналом.

Пример: Включить вывод отладочной информации для сообщений BPDU в порте 0/0/1:

```
Switch#debug spanning-tree  
Switch#debug spanning-tree bpdu rx interface e0/0/1
```

10 Команды для настройки качества обслуживания (QoS)

10.1.1 class

Синтаксис: `class <class-map-name>`

no class <class-map-name>

Назначение: Позволяет поставить в соответствие классу карту правил (policy map) и включить режим карты классов (class map). Отмена команды **no class-map <class-map-name>** удаляет указанный класс.

Параметры: **<class-map-name>**: имя карты классов, используемое классом.

Значение по умолчанию: Классы правил не заданы.

Режим конфигурирования: Режим настройки карты правил.

Описание: До настройки правил классов должна быть создана карта правил и включен режим карты правил. Правила, для которых заданы настройки могут быть применены к классифицированному трафику в режиме карты правил.

Пример: Включить режим классов правил.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#exit
```

10.1.2 class-map

Синтаксис: `class-map <class-map-name>`

no class-map <class-map-name>

Назначение: Позволяет создать карту классов (class map) и включить режим карты классов. Отмена команды **no class-map <class-map-name>** удаляет указанную карту классов.

Параметры: **<class-map-name>**: имя карты классов.

Значение по умолчанию: Карты классов не заданы.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Создать, а затем удалить карту классов с именем "c1".

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#exit
Switch(config)#no class-map c1
```

10.1.3 match

Синтаксис: `match {access-group <acl-index-or-name> | ip dscp <dscp-list> | ip precedence <ip-precedence-list> | ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <cost-list>}`

no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos }

Назначение: Позволяет задать стандарт соответствия карте классов. Отмена команды **no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos}** удаляет указанный стандарт согласования карты классов.

Параметры: **access-group <acl-index-or-name>**: согласование с указанным списком доступов ACL, параметром является номер или имя списка ACL;

ip dscp <dscp-list> и **ipv6 dscp <dscp-list>**: согласование с указанным значением DSCP, параметром является список значений DSCP, содержащий не более 8 значений DSCP;

ip precedence <ip-precedence-list>: согласование с указанным значением IP Precedence, параметром является список IP Precedence, содержащий не более 8 значений IP Precedence, каждое из которых задано в пределах 0~7;

ipv6 access-group <acl-index-or-name>: согласование с указанным списком доступом IPv6 ACL, параметром является номер или имя списка IPv6 ACL;

ipv6 flowlabel <flowlabel-list>: согласование с указанной меткой потока IPv6. Параметром является значение метки потока IPv6, допустимое значение - от 0 до 1048575;

vlan <vlan-list>: согласование с указанным VLAN ID, параметром является список VLAN ID, содержащий не более 8 VLAN ID.

<cost-list>: согласование с указанным значением Cos, параметром является список Cos, содержащий не более 8 значений Cos.

Значение по умолчанию: Стандарт согласования не задан.

Режим конфигурирования: Режим карты классов.

Описание: Для карты классов может быть задан только один стандарт согласования. При настройке согласования со списком доступа ACL, доступно только правило permit (разрешить) в списках ACL.

Пример: Создать карту классов с именем c1, задать правило класса для этой карты, устанавливающее согласование для пакетов с IP Precedence 0 и 1.

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match ip precedence 0 1
Switch(Config-ClassMap-c1)#exit
```

10.1.4 mls qos

Синтаксис: mls qos

no mls qos

Назначение: Позволяет включить функции QoS в глобальном режиме конфигурирования. Отмена команды **no mls qos** выключает функции QoS в глобальном режиме конфигурирования.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Функции QoS выключены.

Описание: При QoS формируются 4 очереди и соответственно 4 различных уровня приоритетов (precedence). Когда функции QoS выключены в глобальном режиме конфигурирования, коммутатор не анализирует поля сообщений, определяющие QoS. Он не распределяет потоки данных по очередям и не изменяет поле precedence сообщений.

Пример: Включить, а затем выключить функции QoS.

```
Switch(config)#mls qos
Switch(config)#no mls qos
```

10.1.5 mls qos cos

Синтаксис: mls qos cos {<default-cos>}

no mls qos cos

Назначение: Позволяет задать значение CoS, используемое портом по умолчанию. Отмена команды **no mls qos cos** восстанавливает настройки, заданные по умолчанию.

Параметры: **<default-cos>**: значение CoS для порта, используемое по умолчанию, в пределах от 0 до 7.

Значение по умолчанию: Задано значение CoS 0.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Позволяет задать значения CoS для порта коммутатора, используемые по умолчанию. Когда порт принимает нетегированное сообщение, оно обрабатывается коммутатором с CoS, заданным по умолчанию (если функции QoS включены в глобальном режиме конфигурирования, в соответствии со значением CoS будет создан внутренний приоритет (precedence)).

Пример: Установить значение CoS по умолчанию 5 для порта Ethernet 0/0/1 . В результате пакетам, проходящим через порт, по умолчанию будет присвоено значение CoS 5 (если не задано иного значения CoS).

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#mls qos cos 5
```

10.1.6 mls qos aggregate-policy

Синтаксис: `mls qos aggregate-policy <aggregate-policy-name> <rate-kbps> <burst-kbyte> [exceed-action {drop | policed-dscp-transmit}]`

`no mls qos aggregate-policy <aggregate-policy-name>`

Назначение: Позволяет задать набор правил, которые могут использоваться в одной карте правил несколькими классами. Отмена команды `no mls qos aggregate-policy <aggregate-policy-name>` удаляет указанный набор правил.

Параметры: `<aggregate-policy-name>`: имя набора правил;

`<rate-kbps>`: средняя бодовая скорость классифицированного трафика в кбит/с, в пределах от 1 до 10 000 000;

`<burst-kbyte>`: средняя скорость кадров классифицированного трафика в кбит/с, превышающих допустимую скорость, в пределах от 1 до 1 000 000;

`exceed-action drop`: когда указанная скорость превышена, пакеты отбрасываются;

`exceed-action policed-dscp-transmit`: задает снижение значения DSCP пакета в соответствии с картой `policed-dscp` снижения значений DSCP, когда указанная скорость превышена.

Значение по умолчанию: наборы правил не заданы.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Если в карте правил используется набор правил, то его невозможно удалить без очищения ссылки на этот набор в соответствующей карте правил, с помощью команды `no policy aggregate <aggregate-policy-name>`. Удаление должно выполняться в глобальном режиме конфигурирования с помощью команды `no mls qos gregate-policy<aggregate-policy-name>`.

Пример: Задать набор правил с именем "agg1", определяющий пропускную способность для пакетов до 20 Мбит/с, скорость кадров, превышающих допустимую скорость, 2 Мбит/с. Все пакеты, превышающие указанную пропускную способность, должны быть отброшены.

```
Switch(config)#mls qos aggregate-policy agg1 20000 2000 exceed-action drop
```

10.1.7 mls qos trust

Синтаксис: `mls qos trust {cos | dscp | ip-precedence | port priority <cos> [[pass-through-cos] | [pass-through-dscp]]}`

`no mls qos trust`

Назначение: Переводит порт в режим доверия меткам входящих кадров. Отмена команды `no mls qos trust` отменяет данный режим.

Параметры: `cos`: порт доверяет значению CoS;

`cos pass-through-dscp`: порт доверяет значению CoS, но не изменяет значение DSCP пакетов;

`dscp`: порт доверяет значению DSCP;

`cos pass-through-cos`: порт доверяет значению DSCP, но не изменяет значение CoS пакетов;

`ip-precedence`: порт доверяет значению IP precedence;

`ip-precedence pass-through-cos`: порт доверяет значению IP precedence, но не изменяет значение CoS пакетов;

`port priority <cos>`: присваивает приоритет физическому порту;

cos: присваиваемый приоритет. Приоритеты всех входящих пакетов порта будут установлены равными значению **cos**. Эта операция не изменяет собственных приоритетов пакетов, с самими пакетами никаких действий не выполняется.

Значение по умолчанию: Порт не является безопасным.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Если для пакетов заданы оба значения (CoS и DSCP), в команде необходимо использовать ключевое слово **pass-through** для защиты значения (CoS или DSCP) (если оно не должно измениться после классификации).

Примечание: В данной версии не поддерживается операция **pass-through-cos**.

2. Когда в порту включена функция **trust cos**, значение **cos** сообщений не будет изменено, когда они покидают коммутатор. Это означает, что будут сохранены оригинальные метки **cos** пакетов, а не совместный результат операций **cos-to-dscp** и **dscp-to-cos**.

Пример: Задать для порта Ethernet port 0/0/1 режим доверия значению CoS, классификация пакетов должна вестись по значению CoS.

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#mls qos trust cos
```

10.1.8 mls qos dscp-mutation

Синтаксис: **mls qos dscp-mutation <dscp-mutation-name>**

no mls qos dscp-mutation <dscp-mutation-name>

Назначение: Позволяет применить карту изменения значений DSCP в порту. Отмена команды **no mls qos dscp-mutation <dscp-mutation-name>** восстанавливает карту изменения значений DSCP, используемую по умолчанию.

Параметры: **<dscp-mutation-name>**: имя карты изменения значений DSCP.

Значение по умолчанию: Правила не заданы.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: При использовании карты изменения значений DSCP, в результате внутренней обработки сообщений на основе карты изменений будут созданы новые значения **dscp** и новые приоритеты **precedence**, соответствующие новым значениям DSCP.

Примечание: Для конфигурирования карты изменения значений DSCP, порт должен иметь режим доверия DSCP. Если в команде одновременно указаны **trust dscp** и **pass-through-dscp**, то значения DSCP будут взяты из карты изменения значений DSCP.

Пример: Задать для Ethernet-порта 0/0/1 состояние **trust DSCP**, используя карту изменения значений DSCP с именем **mu1**.

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#mls qos trust dscp
Switch(Config-If-Ethernet0/0/1)#mls qos dscp-mutation mu1
```

10.1.9 mls qos map

Синтаксис: **mls qos map {cos-dscp <dscp1...dscp8> | dscp-cos <dscp-list> to <cos> | dscp-mutation <dscp-mutation-name> <in-dscp> to <out-dscp> | ip-prec-dscp <dscp1...dscp8> | policed-dscp <dscp-list> to <mark-down-dscp>}**

no mls qos map { cos-dscp | dscp-cos | dscp-mutation <dscp-mutation-name> | ip-prec-dscp | policed-dscp }

Назначение: Позволяет задать карты соответствия значений CoS значениям DSCP, карты соответствия значений DSCP значениям CoS, карты изменения значений DSCP, карты соответствия значений IP **precedence** значениям DSCP и карты привязки правил к значениям DSCP. Отмена команды **no mls qos map {cos-dscp | dscp-cos | dscp-mutation <dscp-mutation-name> | ip-prec-dscp | policed-dscp }** восстанавливает карты, используемые по умолчанию.

Параметры: **cos-dscp <dscp1...dscp8>**: карта соответствия значений CoS значениям DSCP,

<dscp1...dscp8>: 8 значений DSCP, соответствующих значениям CoS (которые могут быть в пределах от 0 до 7). Каждое значение DSCP может быть величиной в пределах от 0 до 63;

dscp-cos <dscp-list> to <cos> : карта соответствия значений DSCP значениям CoS,

<dscp-list>: список значений DSCP, содержащий до 8 значений DSCP,

<cos>: значения CoS, соответствующие значениям DSCP в списке;

dscp-mutation <dscp-mutation-name> <in-dscp> to <out-dscp>: карта изменения значений DSCP,

<dscp-mutation-name>: имя карты изменения значений DSCP,

<in-dscp>: входные значения DSCP, поддерживается до 8 значений, каждое задается в пределах от 0 до 63, значения должны быть отделены друг от друга пробелом,

<out-dscp>: единственное выходное значение DSCP, 8 входных значений DSCP будут преобразованы в заданное выходное значение DSCP;

ip-prec-dscp <dscp1...dscp8>: соответствие между IP precedence и значениями DSCP,

<dscp1...dscp8>: 8 значений DSCP, соответствующих значениям IP precedence (которые могут быть в пределах от 0 до 7). Каждое значение DSCP может принимать величину в пределах от 0 до 63, значения должны быть разделены пробелом;

policed-dscp <dscp-list> to <mark-down-dscp>: карта снижения значений DSCP (mark down), где **<dscp-list>** - это список значений DSCP (поддерживается до 8 значений DSCP),

<mark-down-dscp>: значение DSCP после снижения (mark down).

Значение по умолчанию: Используются следующие карты:

Карта соответствия значений CoS значениям DSCP								
Значение CoS	0	1	2	3	4	5	6	7
Значение DSCP	0	8	16	24	32	40	48	56
Карта соответствия значений DSCP значениям CoS								
Значение DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Значение CoS	0	1	2	3	4	5	6	7
Карта соответствия значений IP Precedence значениям DSCP								
Значение IP Precedence	0	1	2	3	4	5	6	7
Значение DSCP	0	8	16	24	32	40	48	56

Снижение значений DSCP и привязки правил к значениям DSCP по умолчанию не заданы.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: С помощью команды police у классифицированного пакетного трафика может быть понижен приоритет, если превышена указанная скорость передачи или скорость передачи кадров. Опция policed-dscp <dscp-list> to <mark-down-dscp> позволяет снизить значения DSCP пакетов, что приведет к уменьшению их приоритета.

Примечание: При установке карты dscp-cos, восьми последовательным значения dscp будет поставлено в соответствие одно значение cos. Например, при указании соответствия dscp2 to cos2, на дисплей будет выведено сообщение: dscp 0-7 map to cos 2; this switch doesn't support ip-prec-dscp, the mutation from ip precedence to dscp will follow the default map rules. (Коммутатор не поддерживает ip-prec-dscp, будет использована карта изменения значений dscp, заданная по умолчанию.)

Пример: Задать карту соответствий значений CoS значениям DSCP, принятую по умолчанию, т. е. 0 8 16 24 32 40 48 56 должны соответствовать 0 1 2 3 4 5 6 7.
Switch(config)#mls qos map cos-dscp 0 1 2 3 4 5 6 7

10.1.10 policy

Синтаксис: `policy <rate-kbps> <burst-kbyte> [exceed-action { drop | policed-dscp-transmit }]`

`no policy <rate-kbps> <burst-kbyte> [exceed-action { drop | policed-dscp-transmit }]`

Назначение: Позволяет задать правило для классифицированного трафика. Отмена команды `no policy <rate-kbps> <burst-kbyte> [exceed-action { drop | policed-dscp-transmit }]` удаляет указанное правило.

Параметры: `<rate-kbps>`: средняя скорость классифицированного трафика в бодах (кбит/с), в пределах от 1 до 10 000 000;

`<burst-kbyte>`: средняя скорость в бодах (кбит/с) кадров классифицированного трафика, превышающих допустимую скорость, в пределах от 1 до 1 000 000;

exceed-action drop: когда указанная скорость превышена, пакеты отбрасываются;

exceed-action policed-dscp-transmit: задает снижение значения DSCP пакета в соответствии с картой `policed-dscp` снижения значений DSCP, когда указанная скорость превышена.

Значение по умолчанию: Правило не задано.

Режим конфигурирования: Режим настройки карты классов правил.

Описание: Диапазоны `<rate-kbps>` и `<burst-kbyte>` большие. Если введенные настройки превышают реальную скорость работы порта, карта правил, применившая это правило, не будет привязана к портам коммутатора.

Примечание: Для того, чтобы в команде можно было задать опцию `policed-dscp-transmit`, должно быть указано значение `dscp`, соответствующее безопасному порту.

Если для порта одновременно заданы карта изменения значений `dscp` и в команде выбрана опция `policed-dscp-transmit`, карта значений `dscp` тех сообщений, скорость которых превышает заданную, будет соблюдаться в соответствии с заданной картой изменения значений `dscp`.

Пример: Задать пропускную способность для пакетов, согласующихся с правилами класса `c1` до скорости 20 Мбит/с, скорость передачи кадров, превышающих допустимую скорость, 2 Мбит/с; все пакеты, превышающие указанную пропускную способность должны быть отброшены.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#policy 20000 2000 exceed-action drop
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

10.1.11 policy aggregate

Синтаксис: `policy aggregate <aggregate-policy-name>`

`no policy aggregate <aggregate-policy-name>`

Назначение: Позволяет применить к классифицированному трафику набор правил. Отмена команды `no policy aggregate <aggregate-policy-name>` удаляет указанный набор правил.

Параметры: `<aggregate-policy-name>`: имя набора правил.

Значение по умолчанию: Наборы правил не заданы.

Режим конфигурирования: Режим настройки карты правил для классов.

Описание: На один и тот же набор правил могут ссылаться разные карты правил для классов.

Пример: Применить набор правил "agg1" к пакетам, удовлетворяющим правилу класса `c1`.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#policy aggregate agg1
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

10.1.12 policy-map

Синтаксис: `policy-map <policy-map-name>`

`no policy-map <policy-map-name>`

Назначение: Позволяет создать карту правил и включить режим карты правил. Отмена команды `no policy-map <policy-map-name>` удаляет указанную карту правил.

Параметры: `<policy-map-name>`: имя карты правил.

Значение по умолчанию: Карты правил не заданы.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: В режиме настройки карты правил эта команда позволяет задать операции, выполняемые при наличии согласования с QoS, и операции снижения приоритетов.

Пример: Создать и удалить карту правил с именем "p1".

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#exit
Switch(config)#no policy-map p1
```

10.1.13 priority-queue out

Синтаксис: `priority-queue out`

`no priority-queue out`

Назначение: Позволяет настроить рабочий режим очереди — задать обслуживание по приоритетам (Strict Priority) или режим весов WRR. Отмена команды `no priority-queue out` восстанавливает настройки, заданные по умолчанию.

Параметры: Нет.

Значение по умолчанию: Режим очереди с весами WRR.

Режим конфигурирования: Глобальный режим конфигурирования

Описание: Когда задана эта команда, пакеты не будут передаваться с использованием алгоритма весов WRR, они будут передаваться в соответствии с приоритетами очередей. При этом передача сообщений из следующей очереди начнется только после того, как будут переданы все сообщения из текущей очереди.

Примеры: Включить режим обслуживания по приоритетам очередей на порту ethernet0/0/1.

```
Switch(Config-If-Ethernet0/0/1)#priority-queue out
```

10.1.14 set

Синтаксис: `set {ip dscp <new-dscp> | ip precedence <new-precedence> | ipv6 dscp <new-dscp> | ipv6 flowlabel <new-flowlabel> | ip nexthop <ip-address> | cos <new-cos>}`

`no set {ip dscp <new-dscp> | ip precedence <new-precedence> | ipv6 dscp <new-dscp> | ipv6 flowlabel <new-flowlabel> | ip nexthop <ip-address> | cos}`

Назначение: Позволяет задать для классифицированного трафика новые значения DSCP, IP Precedence, IPv6 DSCP или IPv6 FL. Отмена команды `no set {ip dscp <new-dscp> | ip precedence <new-precedence> | ipv6 dscp <new-dscp> | ipv6 flowlabel <new-flowlabel> | ip nexthop <ip-address> | cos}` удаляет присвоенные новые значения.

Параметры: `ip dscp <new-dscp>`: новое значение DSCP;

`ip precedence <new-precedence>`: новое значение IP IPv4 Precedence;

`ipv6 dscp <new-dscp>`: новое значение IPv6 DSCP;

`ipv6 flowlabel <new-flowlabel>`: новое значение IPv6 FL;

`cos <new cos>`: новое значение COS.

Значение по умолчанию: Не присвоено.

Режим конфигурирования: Режим карты классов-правил.

Описание: Новые значения будут присвоены только классифицированному трафику, соответствующему стандарту отбора.

Пример: Задать значение IP DSCP 3 для пакетов, согласующихся с классом правил c1.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

10.1.15 service-policy

Синтаксис: `service-policy input <policy-map-name>`

no service-policy input <policy-map-name>

Назначение: Позволяет применить карту правил на указанном порту. Отмена команды `no service-policy input <policy-map-name>` отменяет применение карты правил на указанном порту.

Параметры: `input <policy-map-name>`: применяет указанную карту правил к входному порту коммутатора.

Значение по умолчанию: Карты правил не привязаны к портам.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Задание режима доверия меткам входящих кадров и применение в этом порту карты правил приводит к конфликту. Будет действовать настройка, заданная последней. К каждому направлению передачи порта может быть применена только одна карта правил.

Примечание: Если на порту задан режим доверия меткам входящих кадров и карта правил соответствует cos, это значение cos должно соответствовать приоритету безопасного порта, а не значению cos сообщений.

Пример: Привязать правило p1 к входному Ethernet-порту 0/0/1

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#service-policy input p1
```

10.1.16 show class-map

Синтаксис: `show class-map [<class-map-name>]`

Назначение: Выводит на дисплей информацию о карте классов QoS.

Параметры: `<class-map-name>`: имя карты классов.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Выводит на дисплей информацию о всех заданных картах классов, либо об указанной карте классов.

Пример:

```
Switch # show class-map
Class map name:c1, used by 1 times match acl name:1
```

Информация, отображаемая на дисплее	Описание
Class map name:c1	Имя карты классов.
used by 1 times	Количество раз использования
match acl name:1	Правило классификации для этой карты классов.

10.1.17 show policy-map

Синтаксис: show policy-map [<policy-map-name>]

Назначение: Выводит на дисплей информацию о карте правил QoS.

Параметры: <policy-map-name> : имя карты правил.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Выводит на дисплей информацию о всех заданных картах правил, либо об указанной карте правил.

Пример:

```
Switch # show policy -map
Policy Map p1, used by 0 port
Class Map name: c1 policy 80 1 exceed-action drop
```

Информация, отображаемая на дисплее	Описание
Policy Map p1	Имя карты правил
used by 0 port	Используемый порт
Class map name:c1	Имя карты классов, которая ссылается на эту карту правил
policy 80 1 exceed-action drop	Реализованное правило

10.1.18 show mls qos aggregate-policy

Синтаксис: show mls qos aggregate-policy [<aggregate-policy-name>]

Назначение: Позволяет вывести на дисплей информацию о наборах правил QoS.

Параметры: <aggregate-policy-name>: имя набора правил.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Позволяет вывести на дисплей информацию о всех наборах правил QoS, либо только об указанном наборе правил.

Пример:

```
Switch #show mls qos aggregate-policy policy1
aggregate-policy policy1 80000 80 exceed-action drop
Not used by any policy map
```

Информация, отображаемая на дисплее	Описание
aggregate-policy policy1 80000 80	Настройки для набора правил.
exceed-action drop	Действие, когда указанная скорость превышена
Not used by any policy map	Число ссылок карт правил на этот набор правил.

10.1.19 show mls qos interface

Синтаксис: show mls qos interface [<interface-id>] [buffers | policy | queuing | statistics]

Назначение: Позволяет вывести на дисплей информацию о настройках QoS порта.

Параметры: <interface-id>: идентификатор порта;

buffers: число буферов очередей, заданное в порту;

policy: настройки правил для порта;

queuing: настройки очередей для порта;

statistics: число пакетов, которым разрешено проходить через входной и выходной профили порта в соответствии с правилом, привязанным к порту.

Значение по умолчанию: нет

Режим конфигурирования: Привилегированный режим.

Описание: Статистики доступны только в том случае, если задано правило для входящих пакетов.

Пример:

```
Switch #show mls qos interface ethernet 0/0/2
Ethernet 0/0/2 default cos:0
DSCP Mutation Map: Default DSCP Mutation Map Attached policy map for Ingress:
p1
```

Информация, отображаемая на дисплее	Описание
Ethernet0/0/2	Имя порта
default cos:0	Значение CoS, выбираемое в порту по умолчанию.
DSCP Mutation Map: Default DSCP Mutation Map	Имя карты снижения значений DSCP для порта
Attached policy map for Ingress: p1	Имя карты правил, привязанной к порту.

```
Switch # show mls qos interface buffers ethernet 0/0/2
Ethernet 0/0/2 packet number of 4 queue: 0x200 0x200 0x200 0x200
```

Информация, отображаемая на дисплее	Описание
Ethernet0/0/2	Имя порта
packet number of 4 queue: 0x200 0x200 0x200 0x200	Число пакетов для всех четырех выходных очередей порта — фиксированная настройка, которую невозможно изменить.

10.1.20 show mls qos maps

Синтаксис: `show mls qos maps [cos-dscp | dscp-cos | dscp-mutation<dscp-mutation-name> | ip-prec-dscp | policed-dscp]`

Назначение: Позволяет вывести на дисплей информацию о настройках карт QoS.

Параметры: **cos-dscp:** карта CoS - соответствие CoS-DSCP;

dscp-cos: карта DSCP - соответствие DSCP-CoS,

dscp-mutation <dscp-mutation-name>: карта снижения значений DSCP <имя карты>,

<dscp-mutation-name>: имя карты снижения значений DSCP;

ip-prec-dscp: IP-адрес карты соответствия IP precedence значениям DSCP;

policed-dscp: карта привязок правил к значениям DSCP.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Позволяет вывести на дисплей информацию о настройках карт QoS

Пример:

```
Switch#show mls qos maps
```

```
Cos-dscp map:
```

```
cos: 0 12 3 4 5 6 7
```

```
dscp: 0 8 16 24 32 40 48 56
```

```
Cos-queue map:
```

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

```
Queue 1 1 2 2 3 3 4 4
```

```
Dscp-cos map:
```

```
d1 : d2 0 1 2 3 4 5 6 7 8 9
```

```
0: 0 0 0 0 0 0 0 0 0 1 1
```

```
1: 1 1 1 1 1 1 2 2 2 2
```

```
2: 2 2 2 2 3 3 3 3 3 3
```

```
3: 3 3 4 4 4 4 4 4 4 4
```

```
4: 5 5 5 5 5 5 5 5 6 6
```

```
5: 6 6 6 6 6 6 7 7 7 7
```

```
6: 7 7 7 7
```

```
IpPrecedence-dscp map:
```

```
ipprec: 0 1 2 3 4 5 6 7
```

```
-----  
dscp: 0 8 16 24 32 40 48 56
```

```
Policed-dscp map:
```

```
d1 : d2 0 1 2 3 4 5 6 7 8 9
```

```
0: 0 1 2 3 4 5 6 7 8 9
```

```
1: 10 11 12 13 14 15 16 17 18 19
```

```
2: 20 21 22 23 24 25 26 27 28 29
```

```
3: 30 31 32 33 34 35 36 37 38 39
```

```
4: 40 41 42 43 44 45 46 47 48 49
```

```
5: 50 51 52 53 54 55 56 57 58 59
```

```
6: 60 61 62 63
```

10.1.21 show mls-qos

Синтаксис: show mls-qos

Назначение: Позволяет вывести на дисплей информацию о QoS в глобальном режиме конфигурирования.

Параметры: нет

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Эта команда позволяет вывести на дисплей информацию о том, включены функции QoS или нет.

Пример:

```
Switch#show mls-qos
```

```
Qos is enabled!
```

10.1.22 wrr-queue cos-map

Синтаксис: wrr-queue cos-map <queue-id> <cos1 ... cos8>

no wrr-queue cos-map

Назначение: Позволяет задать значение CoS для указанной выходной очереди. Отмена команды “no wrr-queue cos-map” восстанавливает настройки, используемые по умолчанию.

Параметры: **<queue-id>**: идентификатор (ID) выходной очереди, в пределах от 1 до 4;
<cos1 ... cos4> значения CoS для выходных очередей, в пределах 0 - 7, поддерживается до 8 значений.

Значение по умолчанию: Значение CoS 0 1 2 3 4 5 6 7, номер очереди 1 1 2 2 3 3 4 4

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Когда функции QoS выключены в глобальном режиме конфигурирования, используются соответствия, заданные по умолчанию.

Пример: Задать значение CoS 2 и 3 для пакетов выходной очереди 1.
`Switch(config)#wrr-queue cos-map 1 2 3`

11 Команды для настройки перенаправления на основе потоков

11.1.1 access-group redirect to interface ethernet

Синтаксис: `access-group <aclname> redirect to interface [ethernet <IFNAME>| <IFNAME>]
no access-group <aclname> redirect`

Назначение: Позволяет задать перенаправление на основе потоков для порта. Отмена команды `no access-group <aclname> redirect` используется для отмены перенаправления потоков

Параметры: `<aclname>`: имя потока, поддерживаются только числовые стандартные IP ACL, числовые расширенные IP ACL, IP ACL со стандартным именем, IP ACL с расширенным именем, числовые стандартные IPv6 ACL, IPv6 ACL со стандартным именем;

В ACL не должны быть заданы параметры `Timerange` и `Portrange`, тип ACL должен быть `Permit` (разрешить).

`<IFNAME>`: порт назначения перенаправления.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Отмена команды `no access-group <aclname> redirect` используется для отмены перенаправления на основе потоков. Функция перенаправления на основе потоков позволяет коммутатору передавать кадры данных, удовлетворяющие специальному условию в другой указанный порт.

Примеры: Перенаправить кадры от источника с IP-адресом 192.168.1.111, принятые от порта 1, в порт 25.

```
Switch(config)#access-list 1 permit host 192.168.1.111
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#access-group 1 redirect to interface ethernet 0/0/25
```

11.1.2 show flow-based-redirect

Синтаксис: `show flow-based-redirect {interface [ethernet <IFNAME>| <IFNAME>]}`

Назначение: Позволяет вывести информацию о текущих настройках перенаправления на основе потоков для системы или порта.

Параметры: Если порт не указан, выводит на дисплей информацию о всех текущих настройках перенаправления на основе потоков в системе. Если в `<IFNAME>` указаны порты, выводит на дисплей информацию о текущих настройках перенаправления на основе потоков для портов, указанных в списке интерфейсов.

Режим конфигурирования: Привилегированный режим.

Описание: Эта команда позволяет вывести на дисплей информацию о текущих настройках перенаправления на основе потоков для системы или порта.

Примеры:

```
Switch(config)#show flow-based-redirect
Flow-based-redirect config on interface ethernet 0/0/1:  RX flow (access-list 1) is redirected to interface Ethernet0/0/25
```

12 Команды для настройки управления уровня 3

12.1 Команды для настройки интерфейса уровня 3

12.1.1 shutdown

Синтаксис: shutdown

no shutdown

Назначение: Выключает указанный интерфейс VLAN коммутатора. Отмена команды **no shutdown** включает указанный интерфейс VLAN.

Режим конфигурирования: Режим настройки интерфейсов VLAN.

Значение по умолчанию: Интерфейс VLAN включен.

Описание: Когда интерфейс VLAN коммутатора выключен, он не передает кадры данных. Если интерфейсу VLAN необходимо присвоить IP-адрес по протоколу BootP или DHCP, он должен быть включен.

Пример: Включить интерфейс VLAN1 коммутатора.

```
Switch(Config-if-Vlan1)#no shutdown
```

12.1.2 interface vlan

Синтаксис: interface vlan <vlan-id>

no interface vlan <vlan-id>

Назначение: Позволяет создать интерфейс VLAN (интерфейс уровня 3). Отмена команды **no interface vlan <vlan-id>** удаляет указанный интерфейс уровня 3.

Параметры: <vlan-id>: числовой идентификатор VLAN ID, присвоенный VLAN, в пределах от 1 до 4094.

Значение по умолчанию: Интерфейс уровня 3 не сконфигурирован.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Перед созданием интерфейса VLAN (интерфейса уровня 3), сначала должен быть создан VLAN. Подробнее об этом см. в главах, посвященных VLAN. Когда с помощью этой команды создан интерфейс VLAN (интерфейса уровня 3), будет включен режим настройки интерфейса уровня 3. После создания интерфейса VLAN (интерфейса уровня 3), команду **interface vlan** можно использовать для входа в режим настройки интерфейса уровня 3.

Пример: Создать интерфейс VLAN (интерфейс уровня 3).

```
Switch (config)#interface vlan 1
```

12.2 Команды для настройки протоколов IPv4/v6

12.2.1 clear ipv6 neighbor

Синтаксис: clear ipv6 neighbors

Назначение: Очищает кэш, в котором содержатся IPv6-адреса соседних устройств.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим

Значение по умолчанию: Нет.

Описание: Команда не очищает статические адреса.

Пример: Очистить список соседних устройств.

```
Switch#clear ipv6 neighbors
```

12.2.2 debug ip packet

Синтаксис: debug ip packet

no debug ip packet

Назначение: Позволяет включить функцию отладки IP-пакетов. Отмена команды **no debug IP packet** выключает функцию отладки.

Параметры: Нет.

Значение по умолчанию: Вывод на дисплей отладочной информации для IP-пакетов не включен.

Режим конфигурирования: Привилегированный режим

Описание: Позволяет вывести на дисплей статистику для принятых и посланных IP-пакетов, в том числе байты и адреса источника и назначения и т. д.

Пример: Включить вывод отладочной информации для IP-пакетов.

```
Switch#debug ip pa IP PACKET: rcvd, src1.1.1.1, dst1.1.1.2, size 100
```

12.2.3 debug ipv6 packet

Синтаксис: debug ipv6 packet

no debug ipv6 packet

Назначение: Вывод на дисплей сообщений отладки приема и передачи IPv6-пакетов.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch#debug ipv6 packet
```

```
IPv6 PACKET: rcvd, src <fe80::203:fff:fe01:2786>, dst <fe80::1>, size <64>, proto <58>, from Vlan1
```

Информация, отображаемая на дисплее	Описание
IPv6 PACKET: rcvd	Приема IPv6-пакета
Src <fe80::203:fff:fe01:2786>	IPv6-адрес источника.
Dst <fe80::1>	IPv6-адрес назначения.
size <64>	Размер принятых данных
proto <58>	Поле протокола в заголовке IPv6-пакета.
from Vlan1	IPv6-данные получены интерфейсом vlan1 уровня 3

12.2.4 debug ipv6 icmp

Синтаксис: debug ipv6 icmp

no debug ipv6 icmp

Назначение: Вывод на дисплей сообщений отладки приема и передачи ICMP-пакетов.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch#debug ipv6 icmp IPv6
```

ICMP: sent, type <129>, src <2003::1>, dst <2003::20a:ebff:fe26:8a49> from Vlan1

Информация, отображаемая на дисплее	Описание
IPv6 ICMP: sent	Отправка IPv6-пакета
type <129>	Результат выполнения команды Ping (номер протокола)
Src <2003::1>	IPv6-адрес источника.
Dst <2003::20a:ebff:fe26:8a49>	IPv6-адрес назначения.
from Vlan1	Порт уровня 3, отправивший данные.

12.2.5 debug ipv6 nd

Синтаксис: `debug ipv6 nd [ns | na | rs | ra | redirect]`

no debug ipv6 nd [ns | na | rs | ra | redirect]

Назначение: Включает отладку приема и передачи определенных типов IPv6-сообщений ND. Параметры ns, na, rs, ra и redirect соответственно обозначают: запрос соседних устройств, оповещение соседних устройств, запрос маршрута, оповещение о маршруте и перенаправление маршрута. Если команда введена без параметров, будет включен вывод отладочных сообщений по всем пяти типам сообщений ND. Отмена команды `no debug ipv6 nd [ns | na | rs | ra | redirect]` выключает режим отладки приема и передачи определенных типов IPv6-сообщений ND. При вводе отмены команды без параметров будут выключен режим отладки для всех пяти типов сообщений ND.

Параметры: Нет.

Значение по умолчанию: Режим отладки приема и передачи всех пяти типов IPv6-сообщений ND выключен.

Режим конфигурирования: Привилегированный режим

Описание: Протокол ND является важной частью протокола IPv6. При возникновении неполадок эта команда позволяет вывести на дисплей сообщения ND указанного типа.

Пример:

```
Switch#debug ipv6 nd
IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst
<fe80::203:fff:fe01:59ba>
```

Информация, отображаемая на дисплее	Описание
IPv6 ND: rcvd	Прием данных ND
type <136>	Тип сообщения ND
Src <fe80::203:fff:fe01:2786>	IPv6-адрес источника.
Dst <fe80::203:fff:fe01:59ba>	IPv6-адрес назначения.

12.2.6 ip address

Синтаксис: `ip address <ip-address> <mask> [secondary]`

no ip address [<ip-address> <mask>] [secondary]

Назначение: Позволяет настроить для коммутатора IP-адрес и соответствующую маску подсети. Отмена команды `no ip address [<ip-address> <mask>] [secondary]` удаляет соответствующую настройку.

Параметры: `<ip-address>`: IP-адрес;

`<mask>`: маска сети для IP-адреса;

`[secondary]` обозначает вторичный IP-адрес.

Режим конфигурирования: Режим настройки интерфейса VLAN.

Значение по умолчанию: IP — адрес не задан.

Описание: Эта команда позволяет вручную настроить IP-адрес интерфейса VLAN. Если опция `secondary` не задана, будет сконфигурирован первичный IP-адрес интерфейса VLAN. Если опция `secondary` задана, это означает, что IP-адрес является вторичным IP-адресом VLAN. Один интерфейс VLAN может иметь только один первичный IP-адрес и несколько (более одного) вторичных IP-адресов. Первичный и вторичные IP-адреса могут использоваться при управлении по протоколам SNMP/Web/Telnet. Кроме того, коммутатор обеспечивает получение IP-адреса по протоколам BOOTP и DHCP.

Пример: Установить IP-адрес интерфейса VLAN1 коммутатора равным 192.168.1.10/24.
`Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0`

12.2.7 ip default-gateway

Синтаксис: `ip default-gateway <A.B.C.D>`

`no ip default-gateway <A.B.C.D>`

Назначение: Позволяет задать шлюз по-умолчанию.

Параметры: `<A.B.C.D>`: IP-адрес шлюза по-умолчанию.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Нет.

Примеры:

`Switch(config)#ip default-gateway 10.1.1.10`

12.2.8 ipv6 address

Синтаксис: `ipv6 address <ipv6address | prefix-length> [eui-64]`

`no ipv6 address <ipv6address | prefix-length> [eui-64]`

Назначение: Позволяет задать для интерфейса агрегируемый глобальный unicast-адрес, unique local адрес и link local адрес.

Параметры: `<ipv6address>`: префикс IPv6-адреса; `<prefix-length>`: длина префикса IPv6-адреса, в пределах от 3 до 128; `eui-64` означает, что IPv6-адрес для интерфейса будет создан автоматически.

Режим конфигурирования: Режим настройки интерфейсов

Значение по умолчанию: Нет.

Описание: Префикс IPv6-адреса не должен быть multicast-адресом, либо IPv6-адресом другого специального типа. Разным интерфейсам VLAN уровня 3 запрещено совместно использовать один и тот же префикс адреса. Как и любой глобальный unicast-адрес, префикс должен быть в пределах от 2001:: до 3fff ::, при этом длина его должна быть не менее 3. Длина префикса адреса локального сайта или линии не должна быть менее 10.

Примеры: Задать IPv6-адрес интерфейса третьего уровня для VLAN1. Задать префикс 2001:3f:ed8::99, длина префикса 64.

`Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64`

12.2.9 ipv6 default-gateway

Синтаксис: `ipv6 default-gateway <X:X::X:X>`

`no ipv6 default-gateway <X:X::X:X>`

Назначение: Позволяет задать шлюз по-умолчанию.

Параметры: `<X:X::X:X>`: IPv6-адрес шлюза по-умолчанию.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Нет.

Примеры:

```
Switch(config)#ipv6 default-gateway 2002:100::1
```

12.2.10 ipv6 nd dad attempts

Синтаксис: `ipv6 nd dad attempts <value>`

`no ipv6 nd dad attempts`

Назначение: Позволяет установить число сообщений оповещения соседних устройств, последовательно посылаемых интерфейсом при настройке обнаружения дублированных адресов.

Параметры: `<value>`: число сообщений оповещения соседних устройств, последовательно посылаемых интерфейсом при настройке обнаружения дублированных адресов, значение `<value>` должно быть в пределах от 0 до 10. Отмена команды `no ipv6 nd dad attempts` восстанавливает значение 1, используемое по умолчанию.

Режим конфигурирования: Режим настройки интерфейсов

Значение по умолчанию: Число сообщений с запросами равно 1.

Описание: Когда конфигурируется IPv6-адрес, необходимо обрабатывать протокол IPv6 Duplicate Address Detection (обнаружение дублированных адресов). Эта команда используется для установки числа сообщений ND, посылаемых при обнаружении дублированных адресов; если `value` выбрано равным 0, то обнаружение дублированных адресов выполняться не будет.

Пример: Установить число сообщений оповещения соседних устройств, последовательно посылаемых интерфейсом при настройке обнаружения дублированных адресов равным 3.

```
Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3
```

12.2.11 ipv6 nd ns-interval

Синтаксис: `ipv6 nd ns-interval <seconds>`

`no ipv6 nd ns-interval`

Назначение: Позволяет задать интервал отправки сообщений запроса соседних устройств, посылаемых интерфейсом. Отмена команды `no ipv6 nd ns-interval` восстанавливает значение интервала, заданное по умолчанию (1 с.).

Параметры: `<seconds>`: интервал отправки сообщений запроса соседних устройств, значение `<seconds>` должно быть в пределах от 1 до 3600 секунд,

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: 1 с.

Описание: Установленное значение должно учитывать условия работы на всех участках маршрута, по которым интерфейс посылает сообщения оповещения. В большинстве случаев не рекомендуется использовать очень малый временной интервал.

Пример: Установить интервал отправки интерфейсом Vlan1 сообщений запроса соседних устройств равным 8 с.

```
Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8
```

12.2.12 ipv6 neighbor

Синтаксис: `ipv6 neighbor <ipv6-address> <hardware-address> interface <interface-type> interface-number>`

`no ipv6 neighbor <ipv6-address>`

Назначение: Позволяет задать статический адрес соседнего устройства в таблице адресов.

Параметры: `ipv6-address`: статический IPv6-адрес соседнего устройства;

`hardware-address`: статический аппаратный IPv6-адрес соседнего устройства;

`interface-type`: тип Ethernet,

`interface-number`: имя интерфейса уровня 2.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Статические адреса соседних устройств в таблице адресов не заданы.

Описание: IPv6- и multicast-адреса, предназначенные для специальных целей, а также локальные адреса, не могут быть использованы в качестве адресов соседних устройств.

Пример: Задать статический адрес соседнего устройства 2001:1:2::4 в порту E0/0/1 и аппаратный MAC-адрес 00-03-0f-89-44-bc.

```
Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 0/0/1
```

12.2.13 show ip interface

Синтаксис: show ip interface { <interface-name> | vlan <vlan-id>} brief

Назначение: Позволяет вывести на дисплей параметры IP-интерфейса.

Параметры: **brief:** краткая сводная информация о настройках и состоянии IPv6-интерфейса; **<interface-name>:** имя интерфейса уровня 3; **<vlan-id>:** vlan ID.

Значение по умолчанию: Нет.

Режим конфигурирования: Любой.

Описание: Если задана только опция brief, отображается информация по всем интерфейсам уровня 3. Кроме того, в команде можно указать конкретный интерфейс уровня 3 – тогда будет отображена информация только для этого интерфейса.

Пример:

```
Switch#show ip interface vlan1 brief
Index      Interface      IP-Address      Protocol
3001      Vlan1          192.168.0.24    down
```

12.2.14 show ip traffic

Синтаксис: show ip traffic

Назначение: Позволяет вывести на дисплей статистику IP-пакетов.

Режим конфигурирования: Привилегированный режим.

Описание: Позволяет вывести на дисплей информацию о принятых и переданных пакетах IP, ICMP, TCP, UDP.

Пример:

```
Switch#show ip traffic
IP statistics:
  Rcvd: 14661 total, 21987 local destination
        0 header errors, 0 address errors
        0 unknown protocol, 0 discards
  Frags: 0 reassembled, 0 timeouts
        0 fragment rcvd, 0 fragment dropped
        0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent: 14661 generated, 0 forwarded
        0 dropped, 0 no route
ICMP statistics:
  Rcvd: 0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
  Sent: 1 total 0 errors 0 time exceeded
        0 redirects, 1 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
  TcpActiveOpens          23, TcpAttemptFails          0
  TcpCurrEstab            2, TcpEstabResets            0
  TcpInErrs               0, TcpInSegs                7326
  TcpMaxConn              264, TcpOutRsts              0
```

```

TcpOutSegs          7326, TcpPassiveOpens          23
TcpRetransSegs     6, TcpRtoAlgorithm          1
TcpRtoMax          120000, TcpRtoMin            200
UDP statistics:
UdpInDatagrams     14660, UdpInErrors              0
UdpNoPorts         1, UdpOutDatagrams        14660

```

Информация, отображаемая на дисплее	Описание
IP statistics :	Статистика IP-пакетов.
Rcvd: 14661 total, 21987 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Статистика для общего числа принятых пакетов, числа пакетов, достигших локального назначения, число пакетов с ошибками в заголовке, число ошибочных адресов, число пакетов неизвестных протоколов, число отброшенных пакетов.
Frgs : 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Статистика фрагментации: число повторно собранных пакетов, таймеры, число принятых фрагментов, число отброшенных фрагментов, число пакетов, которые не могут быть фрагментированы, число посланных фрагментов и т. д.
Sent : 0 generated, 0 forwarded 0 dropped, 0 no route	Статистика для общего числа посланных пакетов, в том числе, локальных пакетов, переданных пакетов, отброшенных пакетов и пакетов без маршрута.
ICMP statistics :	Статистика ICMP-пакетов.
Rcvd : 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Статистика для общего числа принятых ICMP-пакетов и информация классификации.
Sent : 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Статистика для общего числа посланных ICMP-пакетов и информация классификации.
TCP statistics:	Статистика TCP-пакетов.
UDP statistics:	Статистика UDP-пакетов.

12.2.15 show ipv6 interface

Синтаксис: `show ipv6 interface {brief | <interface-name>}`

Назначение: Позволяет вывести на дисплей параметры IPv6-интерфейса.

Параметры: **brief:** краткая сводная информация о настройках и состоянии IPv6-интерфейса; **<interface-name>:** имя интерфейса уровня 3.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Если задана только опция `brief`, отображается информация по всем интерфейсам уровня 3. Кроме того, в команде можно указать конкретный интерфейс уровня 3 – тогда будет отображена информация только для этого интерфейса.

Пример:

```
Switch#show ipv6 interface Vlan1
Vlan1 is up, line protocol is down, dev index is 3001
Device flag 0x1002(BROADCAST MULTICAST)
IPv6 is enabled
Link-local address(es):
 fe80::21a:81ff:fe00:189d TENTATIVE
Site-local address(es):
Global unicast address(es):
2001:506::21a:81ff:fe00:189d subnet is
2001:506::21a:81ff:fe00:189d/64 TENTATIVE
Joined group address(es):
 ff02::1
 ff02::16
 ff02::101
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts is 1
ND managed_config_flag is unset
ND other_config_flag is unset
ND NS interval is 1 second(s)
ND router advertisements is disabled
ND RA min-interval is 200 second(s)
ND RA max-interval is 600 second(s)
ND RA hoplimit is 64
ND RA lifetime is 1800 second(s)
ND RA MTU is 1500
ND advertised reachable time is 30000 millisecond(s)
ND advertised retransmit time is 1000 millisecond(s)
```

Информация, отображаемая на дисплее	Описание
Vlan1	Имя интерфейса уровня 3
[up/up]	Состояние интерфейса уровня 3
dev index	Внутренний порядковый номер устройства
fe80::21a:81ff:fe00:189d	Автоматически сконфигурированный IPv6-адрес интерфейса уровня 3.
2001:506::21a:81ff:fe00:189d	Сконфигурированный IPv6-адрес интерфейса уровня 3.

12.2.16 show ipv6 route

Синтаксис: `show ipv6 route [<destination> | <destination> / <length> | database | fib [local statistics | vrf] | nsm [connected | database] | process-detail | statistics]`

Назначение: Позволяет вывести на дисплей таблицу IPv6-маршрутизации.

Параметры: `<destination>`: сетевой адрес назначения;

`<destination> / <length>`: длина сетевого адреса назначения вместе с префиксом;

`connected`: для маршрутов, связанных напрямую;

`database`: база данных маршрутизатора;

`process-detail`: вывод подробной информации о маршрутах.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда `show ipv6 route` выводит на дисплей только информацию ядра таблицы IPv6-маршрутизации (таблицу маршрутизации в TCP/IP); в базе данных приведены все

маршрутизаторы за исключением локального. Если задана опция fib, будет выведена информация для локального маршрутизатора, опция statistics позволяет вывести информацию о статистике маршрутизатора.

Пример:

```
Switch#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
Timers: Uptime

C   ::1/128 via ::, Loopback, 1d21h32m tag:0
```

Информация, отображаемая на дисплее	Описание
IPv6 Routing Table	Состояние таблицы IPv6-маршрутизации
Codes: K - kernel route, C - connected, S - static, R - RIP,	Сокращенное обозначение типов записей в таблице маршрутизации.

12.2.17 show ipv6 neighbors

Синтаксис: show ipv6 neighbors [{vlan | Ethernet | tunnel}] nterface-number | interface-name | address <ipv6address>]

Назначение: Позволяет вывести на дисплей таблицу адресов соседних устройств.

Параметры: {vlan | Ethernet | tunnel} interface-number | interface-name: задает поиск на основе указанного интерфейса.

ipv6-address: задает поиск на основе указанного IPv6-адреса. Если параметры не заданы, на дисплей выводится вся таблица адресов соседних устройств.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show ipv6 neighbors IPv6 neighbour unicast items: 1, valid: 1,
matched: 1, incomplete: 0, delayed: 0, manage items 5
IPv6 Address          State          Age-time(sec)  Hardware Addr      Interface
Port
2002:ca60:c801:1:250:baff:fef2:a4f4 00-50-ba-f2-a4-f4 Vlan1
Ethernet0/0/2 reachable
IPv6 neighbour table: 1 entries
```

Информация, отображаемая на дисплее	Описание
IPv6 Address	IPv6-адрес соседнего устройства
Link-layer Addr.	MAC-адрес соседнего устройства
Interface	Имя выходного интерфейса.
Port	Имя выходного интерфейса.
State	Состояние соседнего устройства (досягаемое, стабильное, задержка, тестируется, постоянное, неполное, неизвестное)

12.2.18 show ipv6 traffic

Синтаксис: show ipv6 traffic

Назначение: Позволяет вывести на дисплей статистическую информацию о передаче IPv6-пакетов.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Пример:

Switch#show ipv6 traffic

```
IP statistics: Rcvd: 90 total, 17 local destination
0 header errors, 0 address errors 0 unknown protocol, 13 discards
Frgs: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0
fragmented, 0 couldn't fragment, 0 fragment sent
Sent:      110 generated, 0 forwarded 0 dropped, 0 no route
ICMP statistics: Rcvd: 0 total 0 errors 0 time exceeded 0 redirects, 0
unreachable, 0 echo, 0 echo replies
```

Информация, отображаемая на дисплее	Описание
IP statistics	Статистика IPv6-данных
Rcvd: 90 total, 17 local destination 0 header errors, 0 address errors 0 unknown protocol, 13 discards	Статистика принятых IPv6-пакетов
Frgs: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Статистика фрагментирования IPv6-пакетов
Sent: 110 generated, 0 forwarded 0 dropped, 0 no route	Статистика переданных IPv6-пакетов

12.3 Команды для настройки ARP

12.3.1 arp

Синтаксис: `arp <ipaddress> <macaddress> {interface [ethernet] <portName>}`

`no arp <ipaddress>`

Назначение: Позволяет задать статическую запись ARP. Отмена команды `no arp <ip_address>` удаляет статическую запись ARP.

Параметры: `<ipaddress>`: IP-адрес;

`<macaddress>`: MAC-адрес;

`ethernet`: Ethernet-порт;

`<portName>`: имя порта уровня 2.

Значение по умолчанию: Статическая запись ARP не задана.

Режим конфигурирования: Режим настройки интерфейса VLAN.

Описание: На коммутаторе можно создавать статические записи ARP.

Пример: Создать статическую запись ARP для интерфейса VLAN1.

```
Switch(Config-if-Vlan1)#arp 1.1.1.1 00-1a-81-00-18-9d eth 0/0/2
```

12.3.2 clear arp-cache

Синтаксис: `clear arp-cache`

Назначение: Очищает таблицу ARP.

Режим конфигурирования: Привилегированный режим.

Описание: Команда очищает текущее содержимое таблицы ARP, за исключением записей со статическими адресами.

Пример:

```
Switch#clear arp-cache
```

12.3.3 clear arp traffic

Синтаксис: clear arp traffic

Назначение: Очищает статистическую информации сообщений ARP коммутатора.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#clear arp traffic
```

12.3.4 debug arp

Синтаксис: debug arp {receive | send | state}

no debug arp {receive | send | state}

Назначение: Включает функцию вывода отладочной информации ARP на дисплей. Отмена команды **no debug arp {receive|send|state}** выключает функцию вывода отладочной информации ARP на дисплей..

Параметры: **receive:** вывод отладочной информации по принятым ARP-пакетам;

send: вывод отладочной информации по переданным ARP-пакетам;

state: вывод отладочной информации по изменениям состояния ARP коммутатора.

Значение по умолчанию: Вывод отладочной информации ARP выключен.

Режим конфигурирования: Привилегированный режим.

Описание: Позволяет вывести на дисплей число принятых и посланных ARP-пакетов, в том числе адреса источника и назначения и т. д.

Пример: Включить вывод отладочной информации ARP на дисплей.

```
Switch#debug arp receive
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-1a-81-00-18-9d, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-1a-81-00-18-9d, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.e
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-1a-81-00-18-9d, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-1a-81-00-18-9d, dst172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.
```

12.3.5 show arp

Синтаксис: show arp [<ipaddress>] [<vlan-id>] [<hw-addr>] [type {static | dynamic}] [count] [vrf word]

Назначение: Позволяет вывести на дисплей таблицу ARP.

Параметры: **<ipaddress>:** заданный IP-адрес;

<vlan-id>: идентификатор заданной VLAN;

<hw-addr>: для записи с указанным MAC-адресом;

“static” запись ARP является статической;

“dynamic” запись ARP является динамической;

“count” число адресов ARP.

word: заданное имя vrf.

Режим конфигурирования: Привилегированный режим.

Описание: Позволяет вывести на дисплей содержимое текущей таблицы ARP: IP- и MAC-адреса, тип аппаратуры, имя интерфейса и т. д.

Пример:

```
Switch#show arp ARP
Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed:
0, None: 0 Address Hardware Addr Interface Port Flag
50.1.1.6 00-0a-eb-51-51-38 Vlan50 Ethernet0/0/11 Dynamic
50.1.1.9 00-00-00-00-00-09 Vlan50 Ethernet0/0/1 Static
150.1.1.2 00-00-58-fc-48-9f Vlan150 Ethernet0/0/4 Dynamic
```

Информация, отображаемая на дисплее	Описание
Total arp items	Общее число записей ARP.
Valid	Число записей ARP, согласующихся с условиями фильтра и атрибутами легальных состояний.
Matched	Число записей ARP, согласующихся с условиями фильтра.
Verifying	Число записей ARP, используемых при верификации правильности ARP.
InCompleted	Число записей ARP, для которых запрос ARP был послан, но ответа на него не поступило.
Failed	Число записей ARP в состоянии сбоя.
None	Число записей ARP в состоянии начала поиска.
Address	IP-адрес записи ARP.
Hardware Address	MAC-адрес записи ARP.
Interface	Интерфейс уровня 3, соответствующий записи ARP.
Port	Физический интерфейс (уровня 2), соответствующий записи ARP.
Flag	Указывает, какой является запись ARP – статической или динамической.

12.3.6 show arp traffic

Синтаксис: show arp traffic

Назначение: Позволяет вывести на дисплей статистическую информацию сообщений ARP коммутатора.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей статистическую информацию по принятым и переданным ARP-сообщениям коммутатора.

Пример:

```
Switch#show arp traffic
ARP statistics: Rcvd: 10 request, 5 response Sent: 5 request, 10 response
```

12.4 Команды для настройки защиты от ARP-сканирования

12.4.1 anti-arpscan enable

Синтаксис: anti-arpscan enable

no anti-arpscan enable

Назначение: Позволяет включить функцию защиты от ARP-сканирования в глобальном режиме конфигурирования. Отмена команды **no anti-arpscan enable** выключает функцию защиты от ARP-сканирования в глобальном режиме конфигурирования.

Параметры: Нет.

Настройки по умолчанию: Функция защиты от ARP-сканирования выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: При удаленном управлении коммутатором, например, по telnet, пользователи должны до включения функции защиты от ARP-сканирования установить в uplink-порту режим супербезопасного порта (Super Trust port). Это предотвращает выключение порта при приеме слишком большого числа ARP-сообщений. После того, как функция защиты от ARP-сканирования выключена, порт снова примет свои прежние атрибуты – он вновь станет небезопасным портом.

Пример: Включить функцию защиты от ARP-сканирования коммутатора.
`Switch(config)#anti-arpscan enable`

12.4.2 anti-arpscan port-based threshold

Синтаксис: `anti-arpscan port-based threshold <threshold-value>`

`no anti-arpscan port-based threshold`

Назначение: Позволяет задать пороговое значение по принятым сообщениям при методе защиты от ARP-сканирования на основе портов. Если скорость поступления ARP-сообщений превысит пороговое значение, порт будет выключен. Скорость поступления сообщений измеряется в пакетах/секунду. Отмена команды **no anti-arpscan port-based threshold** восстанавливает значение, используемое по умолчанию: 10 секунд.

Параметры: Пороговое значение скорости поступления пакетов, в пределах от 2 до 200.

Настройки по умолчанию: 10 пакетов в секунду.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Пороговое значение защиты от ARP-сканирования на основе портов должно быть больше порогового значения защиты от ARP-сканирования на основе IP-адресов, в противном случае защита от ARP-сканирования на основе IP-адресов даст сбой.

Пример: Задать пороговое значение защиты от ARP-сканирования на основе портов, равное 10 пакетов/с.

```
Switch(config)#anti-arpscan port-based threshold 10
```

12.4.3 anti-arpscan ip-based threshold

Синтаксис: `anti-arpscan ip-based threshold <threshold-value>`

`no anti-arpscan ip-based threshold`

Назначение: Позволяет задать пороговое значение при методе защиты от ARP-сканирования на основе IP-адресов. Если скорость поступления принимаемых ARP-сообщений превысит пороговое значение, IP-сообщения, поступающие с этого IP-адреса будут блокированы. Скорость поступления сообщений измеряется в пакетах/секунду. Отмена команды **no anti-arpscan ip-based threshold** восстанавливает значение, используемое по умолчанию: 3 секунды.

Параметры: Пороговое значение скорости поступления пакетов, в пределах от 1 до 200.

Настройки по умолчанию: 3 пакета в секунду.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Пороговое значение защиты от ARP-сканирования на основе портов должно быть больше порогового значения защиты от ARP-сканирования на основе IP-адресов, в противном случае защита от ARP-сканирования на основе IP-адресов даст сбой.

Пример: Задать пороговое значение защиты от ARP-сканирования на основе IP-адресов 6 пакетов/с.

```
Switch(config)#anti-arpscan ip-based threshold 6
```

12.4.4 anti-arpscan trust

Синтаксис: anti-arpscan trust [port | supertrust-port]

no anti-arpscan trust [port | supertrust-port]

Назначение: Позволяет объявить порт безопасным или супербезопасным. Отмена команды **no anti-arpscan trust [port | supertrust-port]** снова установит порт, как небезопасный.

Параметры: Нет.

Настройки по умолчанию: Все порты считаются небезопасными.

Режим конфигурирования: Режим настройки порта

Описание: Если порт объявлен безопасным, функция защиты от ARP-сканирования не будет работать на этом порту даже в том случае, если скорость поступления ARP-сообщений превысит заданное пороговое значение, при этом порт не будет выключен. В то же время небезопасные IP-адреса этого порта будут продолжать проверяться. Если порт объявлен супербезопасным, то никакая защита от ARP-сканирования не будет работать (ни на основе портов, ни по IP-адресам).

Если порт выключен защитой от ARP-сканирования, то после объявления его безопасным портом он будет снова включен. При удаленном управлении коммутатором, например, по telnet, пользователи должны до включения функции защиты от ARP-сканирования установить в uplink-порту режим супербезопасного порта (Super Trust port). Это предотвращает выключение порта при приеме слишком большого числа ARP-сообщений.

После того, как функция защиты от ARP-сканирования выключена, порт снова примет свои прежние атрибуты – он вновь станет небезопасным портом.

Пример: Объявить порт ethernet 0/0/5 коммутатора безопасным портом.

```
Switch(Config-If-Ethernet0/0/5)#anti-arpscan trust port
```

12.4.5 anti-arpscan trust ip

Синтаксис: anti-arpscan trust ip <ip-address> [<netmask>]

no anti-arpscan trust ip <ip-address> [<netmask>]

Назначение: Позволяет задать безопасный IP-адрес. Отмена команды **no anti-arpscan trust ip <ip-address> [<netmask>]** делает этот IP-адрес вновь небезопасным.

Параметры: <ip-address>: безопасный IP-адрес;

<netmask>: маска сети IP-адреса.

Настройки по умолчанию: Все IP-адреса считаются небезопасными. По умолчанию используется маска 255.255.255.255.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Если порт объявлен безопасным, функция защиты от ARP-сканирования не будет работать на этом порту даже в том случае, если скорость поступления ARP-сообщений превысит заданное пороговое значение, при этом порт не будет выключен. Если порт был выключен защитой от ARP-сканирования, его трафик будет немедленно восстановлен.

Пример: Объявить 192.168.1. 0/24 безопасным IP-адресом.

```
Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0
```

12.4.6 anti-arpscan recovery enable

Синтаксис: anti-arpscan recovery enable

no anti-arpscan recovery enable

Назначение: Позволяет включить функцию автоматического восстановления. Отмена команды **no anti-arpscan recovery enable** выключает функцию автоматического восстановления.

Параметры: Нет.

Настройки по умолчанию: функция автоматического восстановления включена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Используйте эту функцию, если необходимо, чтобы после того, как порт выключался или блокировался IP-адрес, восстанавливались их нормальные режимы работы.

Пример: Включить на коммутаторе функцию автоматического восстановления.
`Switch(config)#anti-arp scan recovery enable`

12.4.7 anti-arp scan recovery time

Синтаксис: `anti-arp scan recovery time <seconds>`

`no anti-arp scan recovery time`

Назначение: Позволяет задать время автоматического восстановления. Отмена команды `no anti-arp scan recovery time` восстанавливает значение времени автоматического восстановления, заданное по умолчанию.

Параметры: время автоматического восстановления, в пределах от 5 до 86400 секунд.

Настройки по умолчанию: 300 секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Перед выполнением этой команды должна быть включена функция автоматического восстановления (в глобальном режиме конфигурирования).

Пример: Задать время автоматического восстановления 3600 секунд.
`Switch(config)#anti-arp scan recovery time 3600`

12.4.8 anti-arp scan log enable

Синтаксис: `anti-arp scan log enable`

`no anti-arp scan log enable`

Назначение: Включает функцию вывода системных сообщений защиты от ARP-сканирования. Отмена команды `no anti-arp scan log enable` выключает эту функцию.

Параметры: Нет.

Настройки по умолчанию: Функция вывода системных сообщений защиты от ARP-сканирования включена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Когда функция вывода системных сообщений защиты от ARP-сканирования включена, пользователям доступна подробная информация о выключенных и автоматически восстановленных портах, заблокированных и восстановленных IP-адресах. Сообщения имеет уровень значимости предупреждений.

Пример: Включить функцию защиты от ARP-сканирования коммутатора.
`Switch(config)#anti-arp scan log enable`

12.4.9 anti-arp scan trap enable

Синтаксис: `anti-arp scan trap enable`

`no anti-arp scan trap enable`

Назначение: Позволяет включить отправку SNMP Trap сообщений защиты от ARP-сканирования. Отмена команды `no anti-arp scan trap enable` выключает функцию SNMP Trap защиты от ARP-сканирования.

Параметры: Нет.

Настройки по умолчанию: Функция SNMP Trap защиты от ARP-сканирования выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Когда функция SNMP Trap защиты от ARP-сканирования включена, пользователи будут принимать сообщение Trap (особая ситуация), если защитой от ARP-сканирования выключен или восстановлен порт, либо заблокирован или восстановлен IP-адрес.

Пример: Включить в коммутаторе функцию SNMP Trap защиты от ARP-сканирования.
`Switch(config)#anti-arp scan trap enable`

12.4.10 show anti-arpscan

Синтаксис: `show anti-arpscan [trust [ip | port | supertrust-port] | prohibited [ip | port]]`

Назначение: Позволяет вывести на дисплей информацию о состоянии защиты от ARP-сканирования

Параметры: Нет.

Настройки по умолчанию: Выводит на дисплей информацию о портах – являются ли они безопасными, включены или выключены. Если порт выключен, будет показано время, в течение которого он находится в выключенном состоянии. На дисплей выводится информация о всех безопасных и заблокированных IP-адресах.

Режим конфигурирования: Привилегированный режим.

Описание: Команду `show anti-arpscan trust port` следует использовать, если необходимо проверить безопасные порты. Небезопасные порты проверяются таким же образом.

Пример: Проверить работу защиты от ARP-сканирования после ее включения.
`Switch(config)#show anti-arpscan`

Total port: 28			
Name	Port-property	beShut	shutTime(seconds)
Ethernet0/0/1	untrust	N	0
Ethernet0/0/2	untrust	N	0
Ethernet0/0/3	untrust	N	0
Ethernet0/0/4	untrust	N	0
Ethernet0/0/5	untrust	N	0
Ethernet0/0/6	untrust	N	0
Ethernet0/0/7	untrust	N	0
Ethernet0/0/8	untrust	N	0
Ethernet0/0/9	untrust	N	0
Ethernet0/0/10	untrust	N	0
Ethernet0/0/11	untrust	N	0
Ethernet0/0/12	untrust	N	0
Ethernet0/0/13	untrust	N	0
Ethernet0/0/14	untrust	N	0
Ethernet0/0/15	untrust	N	0
Ethernet0/0/16	trust	N	0
Ethernet0/0/17	untrust	N	0
Ethernet0/0/18	supertrust	N	0
Ethernet0/0/19	untrust	Y	30
Ethernet0/0/20	trust	N	0
Ethernet0/0/21	untrust	N	0
Ethernet0/0/22	untrust	N	0
Ethernet0/0/23	untrust	N	0
Ethernet0/0/24	untrust	N	0
Ethernet0/0/25	untrust	N	0
Ethernet0/0/26	untrust	N	0

Prohibited IP: IP shutTime(seconds)

1.1.1.2 132

Trust IP:

192.168.99.5 255.255.255.255

192.168.99.6 255.255.255.255

12.4.11 debug anti-arpscan

Синтаксис: `debug anti-arpscan [port | ip]`

`no debug anti-arpscan [port | ip]`

Назначение: Позволяет включить отладку защиты от ARP-сканирования. Отмена команды **no debug anti-arpscan [port | ip]** выключает отладку защиты от ARP-сканирования.

Параметры: Нет.

Настройки по умолчанию: Функция создания отладочных сообщений о защите от ARP-сканирования выключена.

Режим конфигурирования: Привилегированный режим.

Описание: Когда функция создания отладочных сообщений о защите от ARP-сканирования включена, можно проверять соответствующую отладочную информацию о работе защиты от ARP-сканирования с портами и IP-адресами (имеются отдельные выключатели обоих режимов): выключен или восстановлен порт, заблокирован или восстановлен IP-адрес.

Пример: Включить функцию отладки защиты от ARP-сканирования коммутатора.
`Switch(config)#debug anti-arpscan`

12.5 Команды для настройки защиты от подмены протоколов (ARP, ND spoofing)

12.5.1 ip arp-security updateprotect

Синтаксис: `ip arp-security updateprotect`

no ip arp-security updateprotect

Назначение: Позволяет запретить автоматическое обновление таблиц ARP. Отмена команды **no ip arp-security updateprotect** вновь включает автоматическое обновление таблиц ARP.

Параметры: Нет.

Значение по умолчанию: Автоматическое обновление таблиц ARP включено.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Описание: Если автоматическое обновление таблицы ARP запрещено, будут отбрасываться пакеты ARP, конфликтующие с текущей записью ARP (например, пакеты с тем же IP-адресом, но отличающимся MAC-адресом или портом). Остальные пакеты будут приниматься – для обновления таймера времени жизни, либо для создания новой записи. В результате текущая запись ARP не изменится, вместе с тем будет продолжаться и обучение (будут создаваться новые записи ARP).

Пример:

```
Switch(Config-if-Vlan1)#ip arp-security updateprotect
Switch(config)#ip arp-security updateprotect
```

12.5.2 ipv6 nd-security updateprotect

Синтаксис: `ipv6 nd-security updateprotect`

no ipv6 nd-security updateprotect

Назначение: Позволяет запретить автоматическое обновление ND (при IPv6). Отмена команды: “no ipv6 nd-security updateprotect” вновь включает автоматическое обновление ND.

Параметры: Нет.

Значение по умолчанию: автоматическое обновление ND выполняется.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Описание: Если автоматическое обновление таблицы ND запрещено, будут отбрасываться пакеты ND, конфликтующие с текущей записью ND (например, пакеты с тем же IP-адресом, но отличающимся MAC-адресом или портом). Остальные пакеты будут приниматься – для обновления таймера времени жизни, либо для создания новой записи. В результате текущая запись ND не изменится, вместе с тем будет продолжаться и обучение (будут создаваться новые записи ND).

Пример:

```
Switch(Config-if-Vlan1)#ipv6 nd -security updateprotect Switch(config)#ipv6  
nd -security updateprotect
```

12.5.3 ip arp-security learnprotect

Синтаксис: ip arp-security learnprotect

no ip arp-security learnprotect

Назначение: Позволяет запретить обучение ARP (при IPv4). Отмена команды **no ip arp-security learnprotect** вновь включает функцию обучения ARP.

Параметры: Нет.

Значение по умолчанию: Обучение ARP включено.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Описание: Эта команда позволяет выключить автоматическое обучение и обновление ARP. В отличие от защиты, даваемой командой ip arp-security update, эта команда устанавливает таймер даже в том случае, если коммутатор продолжает посылать сообщения запросов и ответов.

Пример:

```
Switch(Config-if-Vlan1)# ip arp-security learnprotect  
Switch(config)# ip arp-security learnprotect
```

12.5.4 ipv6 nd-security learnprotect

Синтаксис: ipv6 nd-security learnprotect

no ipv6 nd-security learnprotect

Назначение: Позволяет запретить обучение ND (при IPv6). Отмена команды **no ipv6 nd-security learnprotect** вновь включает функцию обучения ND.

Параметры: Нет.

Значение по умолчанию: Обучение ND включено.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Описание: Эта команда позволяет выключить автоматическое обучение и обновление ND. В отличие от защиты, даваемой командой ip nd-security update, эта команда устанавливает таймер даже в том случае, если коммутатор продолжает посылать сообщения запросов и ответов.

Пример:

```
Switch(Config-if-Vlan1)#ipv6 nd-security learnprotect Switch(config)#ipv6 nd-  
security learnprotect
```

12.5.5 ip arp-security convert

Синтаксис: ip arp-security convert

Назначение: Позволяет преобразовать все динамические записи ARP в статические.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Описание: Команда позволяет преобразовать все динамические записи ARP в статические, что в сочетании с выключением автоматического обучения может помешать привязке ARP. Сразу после ввода команда прекращает свое действие.

Пример:

```
Switch(Config-if-Vlan1)#ip arp -security convert  
Switch(config)#ip arp -security convert
```

12.5.6 ipv6 nd-security convert

Синтаксис: `ipv6 nd-security convert`

Назначение: Позволяет преобразовать все динамические записи ND в статические.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Описание: Команда позволяет преобразовать все динамические записи ND в статические, что в сочетании с выключением автоматического обучения может помешать привязке ND. Сразу после ввода команда прекращает свое действие.

Пример:

```
Switch(Config-if-Vlan1)#ipv6 nd-security convert
Switch(config)#ipv6 nd-security conver
```

12.5.7 clear ip arp dynamic

Синтаксис: `clear ip arp dynamic`

Назначение: Очищает все динамические записи ARP на интерфейсе.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Команда позволяет очистить динамические записи перед привязкой ARP.

Сразу после ввода команда прекращает свое действие.

Пример:

```
Switch(Config-if-Vlan1)#clear ip arp dynamic
```

12.5.8 clear ipv6 nd dynamic

Синтаксис: `clear ipv6 nd dynamic`

Назначение: Очищает все динамические записи ND на интерфейсе.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Команда позволяет очистить динамические записи перед привязкой ND.

Сразу после ввода команда прекращает свое действие.

Пример:

```
Switch(Config-if-Vlan1)#clear ipv6 nd dynamic
```

12.6 Команды для настройки защиты ARP (ARP Guard)

12.6.1 arp-guard ip

Синтаксис: `arp-guard ip <addr>`

`no arp-guard ip <addr>`

Назначение: Позволяет добавить адрес ARP GUARD. Отмена команды `no arp-guard ip <addr>` удаляет адрес ARP GUARD.

Параметры: `<addr>`: защищенный IP-адрес.

Значение по умолчанию: Адрес ARP GUARD не задан.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: После настройки адреса ARP GUARD, ARP-сообщения, принятые от портов, на которых сконфигурирован ARP GUARD, будут фильтроваться. Если IP-адреса источников ARP-сообщений согласуются с адресами ARP GUARD, заданными на этом порту, они будут считаться

подмененными ARP-сообщениями и будут отброшены. Они не будут переданы в CPU коммутатора или на другие порты. Для каждого порта можно задать 16 адресов ARP GUARD.

Пример:

Задать адрес ARP GUARD 100.1.1.1 для порта Ethernet0/0/1.

```
Switch(config)#interface ethernet0/0/1
Switch(Config-If-Ethernet 0/0/1)#arp-guard ip 100.1.1.1
```

Удалить адрес ARP GUARD 100.1.1.1 для порта Ethernet0/0/1.

```
Switch(config)#interface ethernet0/0/1
Switch(Config-If-Ethernet 0/0/1)#no arp-guard ip 100.1.1.1
```

12.7 Команды для настройки самообращенных запросов (Gratuitous ARP)

12.7.1 ip gratuitous-arp

Синтаксис: ip gratuitous-arp [<interval-time>]

no ip gratuitous-arp

Назначение: Позволяет включить запросы gratuitous ARP и указать интервал их обновления. Отмена команды **no ip gratuitous-arp** выключает запросы gratuitous ARP.

Параметры: <interval-time>: интервал обновления запросов gratuitous ARP, диапазон значений - от 5 до 1200 с, значение по умолчанию 300 с.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов. Значение по умолчанию: По умолчанию запросы Gratuitous ARP выключены.

Описание: Если запросы gratuitous ARP включены в глобальном режиме конфигурирования, все интерфейсы уровня 3 коммутатора способны посылать запросы gratuitous ARP. Если запросы gratuitous ARP включены в режиме настройки интерфейсов, их сможет посылать только указанный интерфейс. При конфигурировании gratuitous ARP, интервал обновления, заданный в режиме настройки интерфейсов будет иметь приоритет больше, чем этот же интервал, но заданный в глобальном режиме конфигурирования.

Пример: Включить запросы gratuitous ARP в глобальном режиме конфигурирования, установить интервал обновления 400 с.

```
Switch(config)#ip gratuitous-arp 400
```

Включить запросы gratuitous ARP для интерфейса VLAN 10, установить интервал обновления 350 с.

```
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 350
```

12.7.2 show ip gratuitous-arp

Синтаксис: show ip gratuitous-arp [interface vlan <vlan-id>]

Назначение: Позволяет вывести на дисплей информацию о настройках запросов gratuitous ARP.

Параметры: <vlan-id> : номер VLAN. Допустимые значения - от 1 до 4094.

Режим конфигурирования: Все режимы конфигурирования.

Описание: При вводе команды show ip gratuitous arp в любом режиме конфигурирования на дисплей будет выведена информация о настройках запросов gratuitous ARP в глобальном режиме конфигурирования и в режиме настройки интерфейсов. Команда show ip gratuitous-arp interface vlan <vlan-id> позволяет вывести на дисплей информацию о настройках запросов gratuitous ARP для указанного интерфейса VLAN.

Пример: Вывести на дисплей информацию о настройках запросов gratuitous ARP в глобальном режиме конфигурирования и в режиме настройки интерфейсов.

```
Switch#show ip gratuitous-arp
Gratuitous ARP send is Global enabled, Interval-Time is 300(s)
Gratuitous ARP send enabled interface vlan information: Name Interval-
Time(seconds) Vlan1 400 Vlan10 350
```

Вывести на дисплей информацию о настройках запросов gratuitous ARP для интерфейса VLAN 10.

```
Switch#show ip gratuitous-arp interface vlan 10
Gratuitous ARP send interface Vlan10 information: Name Interval-
Time(seconds) Vlan10 350
```

12.8 Команды для настройки ND snooping

12.8.1 clear ipv6 nd snooping binding

Синтаксис: clear ipv6 nd snooping binding [<interface-name>]

Назначение: Очищаются все динамические привязки ND SNOOPING.

Параметры: <interface-name>: наименование Ethernet-порта.

Режим конфигурирования: Привилегированный режим.

Описание: Очищаются все записи в таблице привязок ND SNOOPING.

Пример:

```
Switch(config)#ipv6 nd snooping enable
Switch#clear ipv6 nd snooping binding
```

12.8.2 debug ipv6 nd snooping

Синтаксис: debug ipv6 nd snooping {packet | event | binding}

no debug ipv6 nd snooping

Назначение: Эта команда используется для включения отладки ND SNOOPING. Позволяет отслеживать процесс обработки сообщений.

Параметры: **event:** отладочная информация о событиях ND SNOOPING; **packet:** отладочная информация по пакетам ND SNOOPING; **binding:** отладочная информация о привязках ND SNOOPING.

Значение по умолчанию: Вывод отладочной информации отключен.

Режим конфигурирования: Привилегированный режим.

Описание: Отладочная информация позволяет отслеживать, как ND SNOOPING обрабатывает сообщения.

12.8.3 Ipv6 nd snooping enable (Глобальный режим)

Синтаксис: ipv6 nd snooping enable

no ipv6 nd snooping enable

Назначение: Включает функцию ND Snooping.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: Функция ND Snooping не включена.

Описание: Когда эта функция включена, NA/NS-пакеты не будут передаваться через порт, а будут передаваться на CPU. После обработки функцией ND Snooping будут обрабатываться в соответствии с установленными правилами.

Пример: Включает функцию ND Snooping

```
Switch(config)#ipv6 nd snooping enable
```

12.8.4 ipv6 nd snooping mac-binding-limit

Синтаксис: ipv6 nd snooping mac-binding-limit <number>

no ipv6 nd snooping mac-binding-limit

Назначение: Задаёт максимальное количество IPv6-адресов, которые могут быть привязаны к одному MAC-адресу.

Параметры: <number>: количество IPv6-адресов. Имеет отношение только к динамическим привязкам. В диапазоне от 1 до 10.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 10.

Описание: Количество созданных привязок считается глобально, на весь коммутатор. Если количество привязок превышает указанное данной командой значение, то будут удалены привязки, созданные ранее остальных. Удаление будет производиться до тех пор, пока количество привязок не будет соответствовать указанному значению. Если количество созданных привязок не превышает указанное значение, то привязки создаются в обычном режиме.

Пример:

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping mac-binding-limit 10
```

12.8.5 ipv6 nd snooping max-dad-delay

Синтаксис: `ipv6 nd snooping max-dad-delay <max-dad-delay>`

no `ipv6 nd snooping max-dad-delay`

Назначение: Устанавливает время жизни для SAC_START состояния привязки.

Параметры: <max-dad-delay>: время жизни для SAC_START состояния, в диапазоне от 1 до 10 сек.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 1 сек.

Пример:

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping max-dad-delay 10
```

12.8.6 ipv6 nd snooping max-dad-prepare-delay

Синтаксис: `ipv6 nd snooping max-dad-prepare-delay <max-dad-prepare-delay>`

no `ipv6 nd snooping max-dad-prepare-delay`

Назначение: Устанавливает время жизни для SAC_QUERY состояния привязки.

Параметры: <max-dad-delay>: время жизни для SAC_START состояния, в диапазоне от 1 до 10 сек.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 0,5 сек.

Пример:

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping max-dad-prepare-delay 10
```

12.8.7 ipv6 nd snooping max-sac-lifetime

Синтаксис: `ipv6 nd snooping max-sac-lifetime <max-sac-lifetime>`

no `ipv6 nd snooping max-sac-lifetime`

Назначение: Устанавливает время жизни для SAC_BOUND состояния привязки.

Параметры: <max-dad-delay>: время жизни для SAC_START состояния, в диапазоне от 1 до 31536000 сек.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 7200 сек. (2 часа).

Пример:

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping max-sac-lifetime 36000
```

12.8.8 ipv6 nd snooping policy

Синтаксис: `ipv6 nd snooping policy {bind-eui64-address | bind-non-eui64-address}`
`no ipv6 nd snooping policy`

Назначение: Устанавливает политику динамических привязок для адресов ND Snooping.

Параметры: **bind-eui64-address:** привязываются только глобальные unicast-адреса EUI-64; **bind-non-eui64-address:** привязываются только глобальные unicast-адреса не содержащие идентификатор EUI-64.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Привязываются любые глобальные unicast-адреса.

Описание: После конфигурирования политики, привязываются только адреса, указанные данной командой. В случае возникновения конфликта, наличия адреса, несоответствующего политике, выдается сообщение на дисплей.

Пример:

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#ipv6 nd snooping policy bind-eui64-address
```

12.8.9 ipv6 nd snooping port-binding-limit

Синтаксис: `ipv6 nd snooping port-binding-limit <binding-number>`
`no ipv6 nd snooping port-binding-limit`

Назначение: Устанавливает количество динамических привязок для порта.

Параметры: **<binding-number>:** максимальное количество привязок, которое может быть создано на одном порту. В диапазоне от 1 до 100.

Режим конфигурирования: Режим конфигурирования порта.

Значение по умолчанию: 100.

Описание: Если количество привязок превышает указанное данной командой значение, то будут удалены привязки, созданные ранее остальных. Удаление будет производиться до тех пор, пока количество привязок не будет соответствовать указанному значению. Если количество созданных привязок не превышает указанное значение, то привязки создаются в обычном режиме.

Пример:

```
Switch(config)#ipv6 nd snooping enable
Switch(config-if-ethernet0/0/1)#ipv6 nd snooping port-binding-limit 100
```

12.8.10 ipv6 nd snooping static-binding

Синтаксис: `ipv6 nd snooping static-binding <ipv6-address> hardware-address <hardware-address> interface <interface-name>`

`no ipv6 nd snooping static-binding <ipv6-address>`

Назначение: Создает статическую привязку.

Параметры: **<ipv6-address>:** может быть привязан только глобальный unicast-адрес. Не могут быть привязаны произвольные адреса, loopback-адреса и link local-адреса; **<hardware-address>:** MAC-адрес; **<interface-name>:** соответствующий интерфейс.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Нет.

Описание: При создании статической привязки производится проверка. Если существует динамическая привязка с такими же параметрами, то она будет заменена статической привязкой.

Пример:

```
Switch(config)#ipv6 nd snooping enable
```

```
Switch(config)#ipv6 nd snooping static-binding 2001::2:1 hardware-address 00-11-22-33-44-55 interface ethernet0/0/1
```

12.8.11 ipv6 nd snooping trust

Синтаксис: `ipv6 nd snooping trust`

`no ipv6 nd snooping trust`

Назначение: Устанавливает порт как безопасный (trust).

Параметры: Нет.

Режим конфигурирования: Режим конфигурирования порта.

Значение по умолчанию: Порт находится в небезопасном (untrust) режиме.

Описание: Данная команда переводит порт или группу портов в безопасный режим. Все ранее созданные динамические привязки удаляются, новые привязки более не создаются. Разрешается передача пакетов.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-if-ethernet0/0/1)#ipv6 nd snooping trust
```

12.8.12 ipv6 nd snooping user-control

Синтаксис: `ipv6 nd snooping user-control`

`no ipv6 nd snooping user-control`

Назначение: Преводит порт в режим контроля для ND Snooping.

Параметры: Нет.

Режим конфигурирования: Режим конфигурирования порта.

Значение по умолчанию: Режим контроля отключен.

Описание: Данная команда переводит порт или группу портов в режим контроля запросов ND.

Пример:

```
Switch(config)#ipv6 nd snooping enable
Switch(config)#interface ethernet 0/0/1
Switch(config-if-ethernet0/0/1)#ipv6 nd snooping user-control
```

12.8.13 show ipv6 nd snooping binding

Синтаксис: `show ipv6 nd snooping binding [<ipv6-address> | <hardware-address> | <interface-name> | <all>]`

Назначение: Отображает настройку и привязки ND Snooping.

Параметры: **<ipv6-address>**: информация о привязках для указанного IPv6-адреса; **<hardware-address>**: информация о привязках для указанного MAC-адреса; **<interface-name>**: информация о привязках для указанного интерфейса.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Нет.

Описание: Данная команда отображает конфигурацию и информацию о привязках ND Snooping.

Пример:

```
Switch#show ipv6 nd snooping binding all
ND Snooping is enabled
ND Snooping max-dad-delay: 1 s
ND Snooping max-sac-lifetime:7200 s
ND Snooping max-dad-prepare-delay: 0.5 s
ND Snooping max-mac-binding-num: 10
```

```
ND snooping binding count 1, static binding 0
MAC      IPv6 address      interface      vlan ID      State
00-11-22-33-44-55  2001::219:e0ff:fe3f:d183  Ethernet0/0/1  1  SAC_BOUND
```

13 Команды для настройки протокола DHCP

13.1 Команды для настройки DHCP-сервера

13.1.1 bootfile

Синтаксис: `bootfile <filename>`

no bootfile

Назначение: Позволяет задать имя файла для DHCP-клиента, импортируемого при загрузке. Отмена команды **no bootfile** удаляет эту настройку.

Параметры: `<filename>`: имя импортируемого файла, допустимая длина – не более 255 символов.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: Позволяет задать имя файла, импортируемого клиентом. Обычно эта команда используется для рабочих станций, не имеющих жесткого диска – при загрузке им необходимо загрузить файл с настройками сервера.

Эта команда используется вместе с командой “next server”

Пример: Указать имя импортируемого файла и путь к нему, если его местоположение “c:\temp\nos.img”.

```
Switch(dhcp-1-config)#bootfile c:\temp\nos.img
```

См. также: next-server

13.1.2 clear ip dhcp binding

Синтаксис: `clear ip dhcp binding {<address> | all }`

Назначение: Позволяет удалить запись привязки указанного аппаратного IP-адреса или все такие записи.

Параметры: `<address>`: IP-адрес записи привязки.

all: обозначает все IP-адреса записей привязок.

Режим конфигурирования: Привилегированный режим.

Описание: Для просмотра привязок IP-адресов к аппаратным DHCP-адресам клиентов можно использовать команду “show ip dhcp binding”.

Если DHCP-сервер получил информацию о том, что DHCP-клиент по некоторым причинам не использует присвоенный IP-адрес до того, как истекает срок жизни адреса, то DHCP-сервер не удаляет автоматически информацию привязки.

Администратор системы может использовать эту команду для удаления такой привязки IP-адреса к аппаратному адресу клиента вручную. Если выбрана опция “all”, то записи автоматической привязки будут удалены, а соответствующие адреса пула DHCP – перераспределены.

Пример: Удалить все записи привязок IP-адресов к аппаратным адресам. `Switch#clear ip dhcp binding all`

См. также: show ip dhcp binding

13.1.3 clear ip dhcp conflict

Синтаксис: `clear ip dhcp conflict {<address> | all }`

Назначение: Удаляет адрес, присутствующий в отчете по сообщениям о конфликте адресов.

Параметры: `<address>`: IP-адрес, для которого имеется запись о конфликте;

all: все адреса, для которых имеются записи о конфликте.

Режим конфигурирования: Привилегированный режим.

Описание: Команда “show ip dhcp conflict” позволяет проверить, какие IP-адреса конфликтуют. Используя команду “clear ip dhcp conflict”, можно удалить записи для конфликтующих адресов. Если выбрана опция “all”, будут удалены все записи о конфликтах.

После того, как записи будут удалены, соответствующие адреса будут снова доступны для распределения DHCP-сервером.

Пример: Администратор сети обнаружил, что для адреса 10.1.128.160 имеется запись о конфликте, и он больше не используется пользователями. Требуется удалить запись о конфликте адресов.

```
Switch#clear ip dhcp conflict 10.1.128.160
```

См. также:

Команда	Описание
ip dhcp conflict logging	Включает вывод системных сообщений о конфликтах адресов, обнаруженных DHCP-сервером
show ip dhcp conflict	Позволяет вывести на дисплей информацию по конфликтующим адресам

13.1.4 clear ip dhcp server statistics

Синтаксис: clear ip dhcp server statistics

Назначение: Позволяет удалить статистику DHCP-сервера. Очищает счетчик DHCP-сервера.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Используя команду “show ip dhcp server statistics” на экран можно вывести статистики DHCP-сервера. Выводится также сводная статистическая информация. С помощью команды “clear ip dhcp server statistics” можно переустановить счетчик DHCP-сервера.

Пример: Переустановить счетчики DHCP-сервера.
Switch#clear ip dhcp server statistics

См. также: show ip dhcp server statistics

13.1.5 client-identifier

Синтаксис: client-identifier <unique-identifier>

no client-identifier

Назначение: При привязке адреса вручную позволяет задать уникальный ID пользователя. Отмена команды **no client-identifier** удаляет идентификатор.

Параметры: <unique-identifier>: идентификатор пользователя в шестнадцатичном формате с точками.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: Эта команда используется вместе с командой “host” при привязке адреса вручную. Если запрашиваемый идентификатор клиента совпадает с идентификатором, указанным в команде, DHCP-сервер присваивает клиенту IP-адрес, указанный в команде “host”.

Пример: При привязке адреса вручную задать привязку IP-адреса 10.1.128.160 к пользователю с уникальным id 00-10-5a-60-af-12.
Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12
Switch(dhcp-1-config)#host 10.1.128.160 24

См. также: host

13.1.6 debug ip dhcp server

Синтаксис: `debug ip dhcp server {events | linkage | packets}`

`no debug ip dhcp server {events | linkage | packets}`

Назначение: Включает вывод отладочной информации DHCP-сервера. Отмена команды `no debug ip dhcp server {events | linkage | packets}` прекращает вывод отладочной информации DHCP-сервера.

Значение по умолчанию: Вывод отладочной информации не включен.

Режим конфигурирования: Привилегированный режим.

13.1.7 default-router

Синтаксис: `default-router {<address1>} [<address2>[...<address8>]]`

`no default-router`

Назначение: Позволяет задать для DHCP-клиентов шлюз (или шлюзы), назначаемые по умолчанию. Отмена команды `no default-router` удаляет шлюз, назначаемый по умолчанию.

Параметры: `<address1>...<address8>`: IP-адреса.

Значение по умолчанию: Шлюз для DHCP-клиентов не задан.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: IP-адрес шлюза (или шлюзов), назначаемых по умолчанию должен принадлежать той же подсети, что и IP-адрес DHCP-клиента. Коммутатор поддерживает до 8 адресов шлюзов. Адрес шлюза, присвоенный первым, имеет наивысший приоритет, поэтому адрес 1 имеет наивысший приоритет, адрес 2 – второй по значимости и т. д.

Пример: Задать шлюзы, назначаемые по умолчанию для DHCP-клиентов: 10.1.128.2 и 10.1.128.100.

```
Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100
```

13.1.8 dns-server

Синтаксис: `dns-server {<address1>} [<address2>[...<address8>]]`

`no dns-server`

Назначение: Позволяет задать DNS-серверы для DHCP-клиентов. Отмена команды `no dns-server` удаляет шлюз, назначаемый по умолчанию.

Параметры: `<address1>...<address8>`: IP-адреса.

Значение по умолчанию: DNS-сервер для DHCP-клиентов не задан.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: Может быть задано до 8 адресов DNS-серверов. Адрес DNS-сервера, присвоенный первым имеет наивысший приоритет, поэтому адрес 1 имеет наивысший приоритет, адрес 2 – второй по значимости и т. д.

Пример: Установить 10.1.128.3 в качестве адреса DNS-сервера для DHCP-клиентов.

```
Switch(dhcp-1-config)#dns-server 10.1.128.3
```

13.1.9 domain-name

Синтаксис: `domain-name {<domain>}`

`no domain-name`

Назначение: Позволяет задать доменное имя для DHCP-клиентов. Отмена команды `no domain-name` удаляет доменное имя.

Параметры: `<domain>`: доменное имя, допустимая длина – не более 255 символов.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Значение по умолчанию: Нет.

Описание: Позволяет задать доменное имя для клиента.

Пример: Задать "zelay.ru" в качестве доменного имени DHCP-клиента.
`Switch(dhcp-1-config)#domain-name zelay.ru`

13.1.10 hardware-address

Синтаксис: `hardware-address {<hardware-address>} [{Ethernet | IEEE802 | <type-number>}]`

no hardware-address

Назначение: При привязке адреса вручную позволяет задать аппаратный адрес пользователя. Отмена команды **no hardware-address** удаляет эту настройку.

Параметры: **<hardware-address>**: аппаратный адрес в шестнадцатеричном формате;

Ethernet | IEEE802: тип протокола Ethernet,

<type-number>: номер RFC, в которой определен соответствующий тип протокола, в пределах от 1 до 255, например, 0 для Ethernet и 6 для IEEE 802.

Значение по умолчанию: Задан тип протокола Ethernet

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: Эта команда используется вместе с командой "host" при привязке адреса вручную.

Если запрашиваемый аппаратный адрес клиента совпадает с аппаратным адресом, указанным в команде, DHCP-сервер присваивает клиенту IP-адрес, указанный в команде "host".

Пример: При привязке вручную задать IP-адрес 10.1.128.160 для пользователя с аппаратным адресом 00-00-e2-3a-26-04.

```
Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04
Switch(dhcp-1-config)#host 10.1.128.160 24
```

См. также: host

13.1.11 host

Синтаксис: `host {<address>} [<mask> | <prefix-length>]`

no host

Назначение: При привязке адресов вручную позволяет задать IP-адрес, присваиваемый пользователю. Отмена команды **no host** удаляет IP-адрес.

Параметры: **<address>**: IP-адрес;

<mask>: маска подсети;

<prefix-length>: означает, что маска задана префиксом.

Например, маска 255.255.255.0 имеет префикс "24", а маска 255.255.255.252 - префикс "30".

Режим конфигурирования: Режим настройки пула адресов DHCP.

Значение по умолчанию: Нет.

Описание: Если при настройке IP-адреса маска и префикс не заданы и в пуле IP-адресов информация о маске отсутствует, система присвоит маску автоматически в соответствии с классом IP-адреса.

При привязке адресов вручную, эта команда используется вместе с командами "hardware-address" или "client-identifier".

Если запрашиваемый аппаратный адрес клиента совпадает с указанным в команде идентификатором или аппаратным адресом, DHCP-сервер присваивает клиенту IP-адрес, указанный в команде "host".

Пример: При привязке вручную задать IP-адрес 10.1.128.160 для пользователя с аппаратным адресом 00-10-5a-60-af-12.

```
Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12
Switch(dhcp-1-config)#host 10.1.128.160 24
```

См. также:

Команда	Описание
hardware-address	При привязке адреса вручную позволяет задать аппаратный адрес пользователя
client-identifier	При привязке адреса вручную позволяет задать уникальный ID пользователя

13.1.12 ip dhcp conflict logging

Синтаксис: ip dhcp conflict logging

no ip dhcp conflict logging

Назначение: Включает вывод системных сообщений о конфликтах адресов, обнаруженных DHCP-сервером. Отмена команды **no ip dhcp conflict logging** прекращает вывод системных сообщений о конфликтах адресов.

Значение по умолчанию: Вывод сообщений о конфликтах адресов включен.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Когда вывод системных сообщений включен, как только DHCP-сервер обнаруживает конфликт, выводится сообщение о конфликте адресов. Адреса, для которых обнаружен конфликт, не будут динамически выделяться DHCP-сервером до тех пор, пока не будут удалены записи о конфликте.

Пример: Выключить создание системных сообщений DHCP-сервером.

```
Switch(config)#no ip dhcp conflict logging
```

См. также: **clear ip dhcp conflict**

13.1.13 ip dhcp excluded-address

Синтаксис: ip dhcp excluded-address {<low-address>} [<high-address>]

no ip dhcp excluded-address {<low-address>} [<high-address>]

Назначение: Позволяет исключить адреса из тех, которые распределяются динамически. Отмена команды **no ip dhcp excluded-address {<low-address>} [<high-address>]** отменяет эту настройку.

Параметры: <low-address>: начальный IP-адрес;

<high-address>]: конечный IP-адрес.

Значение по умолчанию: Можно исключить только один индивидуальный адрес.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Эта команда позволяет исключить один или несколько последовательных адресов в пуле из числа адресов, распределяемых динамически. Исключенные адреса могут быть использованы системным администратором для других целей.

Пример: Зарезервировать адреса в диапазоне от 10.1.128.1 до 10.1.128.10, исключить их из числа адресов, распределяемых динамически.

```
Switch(config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10
```

13.1.14 ip dhcp pool

Синтаксис: ip dhcp pool {<name>}

no ip dhcp pool {<name>}

Назначение: Позволяет настроить пул DHCP-адресов и войти в режим настройки пула. Отмена команды **no ip dhcp pool {<name>}** удаляет указанный пул адресов.

Параметры: <name>: строка с именем пула адресов, допустимая длина – не более 32 символов.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Эта команда используется для настройки пула DHCP-адресов в глобальном режиме конфигурирования и для входа в режим настройки DHCP-адресов.

Пример: Задать пул адресов с именем "1".

```
Switch(config)#ip dhcp pool 1  
Switch(dhcp-1-config)#
```

13.1.15 ip dhcp conflict ping-detection enable

Синтаксис: ip dhcp conflict ping-detection enable

no ip dhcp conflict ping-detection enable

Назначение: Включает ping-обнаружение конфликтов на DHCP-сервере. Отмена команды **no ip dhcp conflict ping-detection enable** выключает эту функцию.

Параметры: Нет.

Настройки по умолчанию: ping-обнаружение конфликтов на DHCP-сервере выключено.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Перед тем, как включить Ping-обнаружение конфликтов, необходимо включить регистрацию конфликтующих адресов.

Если клиенту не удалось принять сообщения с Ping-запросами (например, они заблокированы межсетевым экраном), эта функция проверит соответствие назначенного IP-адреса локальной записи ARP. Если назначенный IP-адрес имеет соответствующую запись ARP, то налицо конфликт адресов, в противном случае, IP-адрес назначен клиенту.

Примеры: Включить Ping-обнаружение конфликта.

```
Switch(config)#ip dhcp conflict ping-detection enable
```

См. также:

Команда	Описание
ip dhcp conflict logging	Включает вывод системных сообщений о конфликтах адресов, обнаруженных DHCP-сервером
ip dhcp ping packets	Позволяет задать число ping-пакетов, которые DHCP-сервер будет посылать по адресу из пула перед тем как присвоить адрес клиенту, запросившему сервер
ip dhcp ping timeout	Позволяет задать время ожидания DHCP-сервером ping-пакета

13.1.16 ip dhcp ping packets

Синтаксис: ip dhcp ping packets {<request-num>}

no ip dhcp ping packets

Назначение: Позволяет задать число ping-пакетов, которые DHCP-сервер будет посылать по адресу из пула перед тем как присвоить адрес клиенту, запросившему сервер. Отмена команды **no ip dhcp ping packets** удаляет эту настройку.

Параметры: <request-num>: число посылаемых ping-пакетов.

Настройки по умолчанию: Два пакета.

Режим конфигурирования: Глобальный режим конфигурирования.

Примеры: Установить число посылаемых ping-пакетов равным 3.

```
Switch(config)#ip dhcp ping packets 3
```

См. также:

Команда	Описание
ip dhcp ping timeout	Позволяет задать время ожидания DHCP-сервером ping-пакета
ip dhcp conflict ping-detection enable	Включает ping-обнаружение конфликтов на DHCP-сервере

13.1.17 ip dhcp ping timeout

Синтаксис: `ip dhcp ping timeout <timeout-value>`

`no ip dhcp ping timeout`

Назначение: Позволяет задать время ожидания DHCP-сервером ответного сообщения (Echo Request), которое должно приниматься после отправки каждого ping-пакета. По умолчанию, задано время ожидания 500 миллисекунд. Отмена команды `no ip dhcp ping timeout` восстанавливает настройки, заданные по умолчанию.

Параметры: `<timeout-value>`: время ожидания в миллисекундах.

Настройки по умолчанию: 500 миллисекунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Примеры: Задать время ожидания равным 600 миллисекунд.

```
Switch(config)#ip dhcp conflict timeout 600
```

См. также:

Команда	Описание
<code>ip dhcp ping timeout</code>	Позволяет задать время ожидания DHCP-сервером ping-пакета
<code>ip dhcp conflict ping-detection enable</code>	Включает ping-обнаружение конфликтов на DHCP-сервере

13.1.18 lease

Синтаксис: `lease {[<days>] [<hours>] [<minutes>] | infinite}`

`no lease`

Назначение: Позволяет задать срок жизни адресов пула. Отмена команды `no lease` восстанавливает настройки, используемые по умолчанию.

Параметры: `<days>`: число дней, от 0 до 365;

`<hours>`: число часов, от 0 до 23;

`<minutes>`: число минут, от 0 до 59;

`infinite`: постоянное использование.

Значение по умолчанию: 1 сутки.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: DHCP – это протокол, позволяющий распределять сетевые адреса динамически, вместо распределения их на постоянной основе. Эта команда позволяет корректировать срок жизни адресов. Настройки срока жизни адресов должны учитывать условия работы сети. Слишком большой срок жизни адресов ухудшает гибкость протокола DHCP. Слишком короткий срок жизни адресов приводит к увеличению сетевого трафика, в том числе трафика служебной информации. По умолчанию срок жизни адресов составляет 1 сутки.

Пример: Задать срок жизни адресов пула DHCP с именем “1” 3 дня 12 часов 30 минут.

```
Switch(dhcp-1-config)#lease 3 12 30
```

13.1.19 netbios-name-server

Синтаксис: `netbios-name-server {<address1>} [<address2> [...<address8>]]`

`no netbios-name-server`

Назначение: Позволяет задать адрес WINS-сервера. Отмена команды `no netbios-name-server` удаляет WINS-сервер.

Параметры: `<address1>...<address8>`: IP-адреса.

Значение по умолчанию: По умолчанию WINS-сервер не включен.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: Эта команда позволяет задать для клиента WINS-сервер. Может быть задано до 8 адресов WINS-серверов. Адрес WINS-сервера, присвоенный первым, имеет наивысший приоритет. Поэтому адрес 1 имеет высший приоритет, адрес 2 – второй по значимости и т. д.

Пример: Задать для клиента WINS-сервер равным 192.168.1.1.
Switch(dhcp-1-config)#netbios-name-server 192.168.1.1

13.1.20 netbios-node-type

Синтаксис: netbios-node-type b-node | h-node | m-node | p-node | <type-number>

no netbios-node-type

Назначение: Позволяет задать тип узла для указанного в команде порта. Отмена команды no netbios-node-type отменяет эту настройку.

Параметры: b-node: узел вещания,

h-node: гибридный узел, после разрыва соединения точка-точка может осуществлять вещание;

m-node: гибридный узел, после вещания может устанавливать соединение точка-точка;

p-node: узел точка-точка;

<type-number>: тип узла в шестнадцатеричной форме (от 0 до FF).

Значение по умолчанию: Тип клиентского узла не задан.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: Если тип клиентского узла задан, рекомендуется установить его h-node, чтобы после разрыва соединения точка-точка он осуществлял вещание.

Пример: Задать тип узла клиента пула 1 как узла, осуществляющего вещание.
Switch(dhcp-1-config)#netbios-node-type b-node

13.1.21 network-address

Синтаксис: network-address {<network-number>} [<mask> | <prefix-length>]

no network-address

Назначение: Позволяет задать диапазон присваиваемых адресов пула. Отмена команды no network-address отменяет настройки.

Параметры: <network-number>: номер сети;

<mask>: маска подсети;

<prefix-length>: маска в форме префикса.

Например, маска 255.255.255.0 имеет префикс “24”, а маска 255.255.255.252 - префикс “30”.

Примечание: Когда используется DHCP-сервер, длина маски пула не должна превышать длины IP-адреса интерфейса уровня 3 в соответствующем сегменте.

Значение по умолчанию: Если маска не задана, то по умолчанию будет присвоена маска, соответствующая классу адреса.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: Позволяет задать диапазон присваиваемых адресов пула, который DHCP-сервер может использовать в процессе динамического распределения адресов. Один пул адресов может соответствовать только одному сегменту. Эта команда исключает использование привязки адресов вручную с помощью команд “hardware address” и “host”.

Пример: Задать присваиваемый адрес в пуле 1 — 10.1.128.0/24.
Switch(dhcp-1-config)#network-address 10.1.128.0 24

13.1.22 next-server

Синтаксис: next-server {<address1>} [<address2> [...<address8>]]

no next-server

Назначение: Позволяет задать адрес сервера, на котором хранится файл, импортируемый клиентом. Отмена команды **no next-server** отменяет эту настройку.

Параметры: <address1>...<address8>: IP-адреса.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Описание: Используется для указания адреса сервера, на котором хранится файл, импортируемый клиентом. В том случае, если клиентом является рабочая станция, она будет загружать файл с настройками с сервера. Эта команда используется вместе с командой "bootfile".

Пример: Задать адрес сервера хостинга 10.1.128.4.

```
Switch(dhcp-1-config)#next-server 10.1.128.4
```

13.1.23 option

Синтаксис: option {<code>} {ascii <string> | hex <hex> | ipaddress <ipaddress>}

no option {<code>}

Назначение: Позволяет задать сетевой параметр с помощью его опционального кода. Отмена команды **no option <code>** отменяет настройку опции.

Параметры: <code>: код сетевого параметра;

<string>: строка ASCII, длиной не более 255 символов;

<hex>: шестнадцатеричное значение, большее 510, с четной длиной;

<ipaddress> : IP-адрес, может быть задано до 63 IP-адресов.

Режим конфигурирования: Режим настройки пула адресов DHCP.

Значение по умолчанию: Нет.

Описание: В коммутаторе имеются команды для настройки сетевых параметров, а также различные команды, полезные для настройки сети в соответствии с требованиями пользователя. Определения опциональных кодов даны в рекомендации RFC2123.

Пример: Задать адрес WWW-сервера 10.1.128.240.

```
Switch(dhcp-1-config)#option 72 ip 10.1.128.240
```

13.1.24 service dhcp

Синтаксис: service dhcp

no service dhcp

Назначение: Включает службу DHCP. Отмена команды **no service dhcp** выключает службу DHCP.

Параметры: Нет.

Значение по умолчанию: Служба DHCP выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: В службу DHCP входят DHCP-сервер и DHCP-relay. Когда служба DHCP включена, включены и DHCP-сервер, и DHCP-relay. Коммутатор может назначать IP-адреса DHCP-клиентам и включать DHCP-relay только тогда, когда включен DHCP-сервер.

Пример: Включить DHCP-сервер.

```
Switch(config)#service dhcp
```

13.1.25 show ip dhcp binding

Синтаксис: show ip dhcp binding [[<ip-addr>] [type {all | manual | dynamic}] [count]]

Назначение: Позволяет вывести на экран информацию привязок IP-МАС.

Параметры: <ip-addr>: заданный IP-адрес;

"all": все типы привязок (введенные вручную и назначенные динамически);

"manual": для привязок, введенных вручную;

“dynamic”: для привязок, назначенных динамически;

“count”: статистики привязок адресов в записях DHCP.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch# show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
10.1.1.233	00-00-E2-3A-26-04	Infinite	Manual
10.1.1.254	00-00-E2-3A-5C-D3	60	Automatic

Информация, отображаемая на дисплее	Описание
IP address	IP-адрес, присвоенный DHCP-клиенту
Hardware address	MAC-адрес DHCP-клиента
Lease expiration	Срок жизни IP-адреса DHCP-клиента
Type	Тип присвоения: Привязка вручную или динамическое распределение

13.1.26 show ip dhcp conflict

Синтаксис: show ip dhcp conflict

Назначение: Позволяет вывести на дисплей информацию по конфликтующим адресам.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch#show ip dhcp conflict
```

```
IP Address      Detection method      Detection Time
10.1.1.1        Ping                  FRI JAN 02 00:07:01 2002
```

Информация, отображаемая на дисплее	Описание
IP Address	Конфликтующий IP-адрес
Detection method	Метод обнаружения конфликта
Detection Time	Время и дата обнаружения конфликта.

13.1.27 show ip dhcp server statistics

Синтаксис: show ip dhcp server statistics

Назначение: Позволяет вывести на дисплей статистику для всех DHCP-пакетов DHCP-сервера.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch# show ip dhcp server statistics
```

Address pools	3
Database agents	0
Automatic bindings	2
Manual bindings	0
Conflict bindings	0
Expired bindings	0
Malformed message	0
Message	Received
BOOTREQUEST	3814
DHCPDISCOVER	1899
DHCPREQUEST	6
DHCPDECLINE	0
DHCPRELEASE	1
DHCPINFORM	1

Message	Send
BOOTREPLY	1911
DHCPOFFER	6
DHCPACK	6
DHCPNAK	0
DHCPRELAY	1907
DHCPFORWARD	0

Информация, отображаемая на дисплее	Описание
Memory usage	Объем используемой памяти EMS
Address pools	Число сконфигурированных пулов адресов DHCP
Database agents	Число агентов баз данных
Automatic bindings	Число адресов, привязанных автоматически
Manual bindings	Число адресов, привязанных вручную
Conflict bindings	Число конфликтующих адресов
Expired bindings	Число адресов, у которых истек срок жизни
Malformed message	Число сообщений об ошибках
Message Recieved	Статистика по принятым пакетам DHCP
BOOTREQUEST	Общее число принятых пакетов
DHCPDISCOVER	Число пакетов DHCPDISCOVER.
DHCPREQUEST	Число пакетов DHCPREQUEST
DHCPDECLINE	Число пакетов DHCPDECLINE
DHCPRELEASE	Число пакетов DHCPRELEASE
DHCPINFORM	Число пакетов DHCPINFORM
Message Send	Статистика по переданным пакетам DHCP
BOOTREPLY	Общее число переданных пакетов
DHCPOFFER	Число пакетов DHCPOFFER
DHCPACK	Число пакетов DHCPACK
DHCPNAK	Число пакетов DHCPNAK
DHCPRELAY	Число пакетов DHCPRELAY
DHCPFORWARD	Число пакетов DHCPFORWARD

13.2 Команды для настройки DHCP Relay

13.2.1 ip forward-protocol udp bootps

Синтаксис: ip forward-protocol udp bootps

no ip forward-protocol udp bootps

Назначение: Указывает DHCP relay перенаправлять UDP-пакеты на порту.

Параметры: bootps: Перенаправление DHCP broadcast-пакетов на порту UDP 67.

Значение по умолчанию: Перенаправление выключено.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Адрес узла, на который перенаправляются пакеты задается командой **ip helper-address**.

Пример:

```
Switch(config)#ip forward-protocol udp boots
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip helper-address 192.168.1.5
```

13.2.2 ip helper-address

Синтаксис: ip helper-address {<ip-address>}

no ip helper-address {<ip-address>}

Назначение: Указывает IP-адрес назначения для функции DHCP Relay.

Параметры: <ip-address>: IP-адрес назначения.

Значение по умолчанию: IP-адрес назначения не задан.

Режим конфигурирования: Режим конфигурирования интерфейса.

Описание: IP-адрес назначения взаимосвязан с UDP-портом, т.о. механизм DHCP Relay перенаправляет UDP-пакеты только с указанного порта на указанный IP-адрес назначения, а не все пакеты на все DHCP-сервера.

13.3 Команды для настройки DHCPv6

13.3.1 clear ipv6 dhcp binding

Синтаксис: clear ipv6 dhcp binding [<ipv6-address>] [pd <ipv6-prefix | prefix-length>]

Назначение: Позволяет удалить запись привязки указанного аппаратного IPv6-адреса или все такие записи.

Параметры: <ipv6-address>: IPv6-адрес записи привязки; <ipv6-prefix | prefix-length>: IPv6-префикс записи привязки.

Режим конфигурирования: Привилегированный режим.

Описание: Для просмотра привязок IP-адресов к аппаратным DHCP-адресам клиентов можно использовать команду “show ipv6 dhcp binding” .

Если DHCP-сервер получил информацию о том, что DHCPv6-клиент по некоторым причинам не использует присвоенный IP-адрес до того, как истекает срок жизни адреса, то DHCP-сервер не удаляет автоматически информацию привязки. Администратор системы может использовать эту команду для удаления такой привязки IP-адреса к аппаратному адресу клиента вручную. Если параметры не указаны, то все записи автоматической привязки будут удалены, а соответствующие адреса пула DHCP – перераспределены.

Пример: Удалить все записи привязок IPv6-адресов к аппаратным адресам.
Switch#clear ipv6 dhcp binding

См. также: show ipv6 dhcp binding

13.3.2 clear ipv6 dhcp server statistics

Синтаксис: clear ipv6 dhcp server statistics

Назначение: Позволяет удалить статистику DHCPv6-сервера. Очищает счетчик DHCPv6-сервера.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Используя команду “show ipv6 dhcp server statistics” на экран можно вывести статистику DHCPv6-сервера. Выводится также сводная статистическая информация. С помощью команды “clear ipv6 dhcp server statistics” можно сбросить счетчик DHCPv6-сервера.

Пример: Переустановить счетчики DHCP-сервера.
Switch#clear ipv6 dhcp server statistics

13.3.3 debug ipv6 dhcp client packet

Синтаксис: debug ipv6 dhcp client {event | packet}

no debug ipv6 dhcp client {event | packet}

Назначение: Включает дебаг для DHCPv6 prefix delegation.

Параметры: event: дебаг событий; packet: дебаг пакетов DHCPv6.

Режим конфигурирования: Привилегированный режим.

Пример:
Switch# debug ipv6 dhcp client packet

13.3.4 debug ipv6 dhcp detail

Синтаксис: debug ipv6 dhcp detail

no debug ipv6 dhcp detail

Назначение: Включает дебаг для всех отправленных и полученных пакетов DHCPv6.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#debug ipv6 dhcp detail
```

13.3.5 debug ipv6 dhcp detail

Синтаксис: debug ipv6 dhcp relay packet

no debug ipv6 dhcp relay packet

Назначение: Включает дебаг пакетов для DHCPv6 Relay функции.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#debug ipv6 dhcp relay packet
```

13.3.6 debug ipv6 dhcp server

Синтаксис: debug ipv6 dhcp server {event | packet}

no debug ipv6 dhcp server {event | packet}

Назначение: Включает дебаг для DHCPv6-сервера.

Параметры: **event:** дебаг событий DHCPv6-сервера; **packet:** дебаг пакетов DHCPv6.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#debug ipv6 dhcp server packet
```

13.3.7 dns-server

Синтаксис: dns-server {<ipv6-address>}

no dns-server {<ipv6-address>}

Назначение: Позволяет задать DNS-серверы для DHCPv6-клиентов.

Параметры: <ipv6-address>: IPv6-адрес DNS-сервера.

Значение по умолчанию: DNS-сервер для DHCPv6-клиентов не задан.

Режим конфигурирования: Режим настройки пула адресов DHCPv6.

Описание: Может быть задано до 3 адресов DNS-серверов.

Пример: Установить 2001:da8::1 в качестве адреса DNS-сервера для DHCPv6-клиентов.

```
Switch(dhcp-1-config)#dns-server 2001:da8::1
```

13.3.8 domain-name

Синтаксис: domain-name {<domain-name>}

no domain-name {<domain-name>}

Назначение: Позволяет задать доменное имя для DHCPv6-клиентов.

Параметры: <domain-name>: доменное имя, допустимая длина – не более 32 символов.

Режим конфигурирования: Режим настройки пула адресов DHCPv6.

Значение по умолчанию: Нет.

Описание: Позволяет задать доменное имя для клиента. Может быть задано до 3 доменных имен для каждого пула.

Пример: Задать "zelaх.ru" в качестве доменного имени DHCPv6-клиента.
Switch(dhcp-1-config)#domain-name zelaх.ru

13.3.9 excluded-address

Синтаксис: excluded-address {<ipv6-address>}

no excluded-address {<ipv6-address>}

Назначение: Позволяет исключить адрес из тех, которые распределяются динамически. Отмена команды **no excluded-address** {<ipv6-address>} отменяет эту настройку.

Параметры: <ipv6-address>: IPv6-адрес, который будет исключен из раздачи.

Значение по умолчанию: Адреса не исключаются.

Режим конфигурирования: Режим настройки пула адресов DHCPv6.

Описание: Эта команда позволяет исключить один адрес из числа адресов, распределяемых динамически.

Пример: Зарезервировать адрес 2001:da8:123::1, исключить его из числа адресов, распределяемых динамически.
Switch(dhcpv6-test-config)#excluded-address 2001:da8:123::1

13.3.10 ipv6 address

Синтаксис: ipv6 address <prefix-name> <ipv6-prefix/prefix-length>

no ipv6 address <prefix-name> <ipv6-prefix/prefix-length>

Назначение: Позволяет сконфигурировать интерфейс для использования префикса при назначении адреса.

Параметры: <prefix-name>: строка длиной не более 32 символов; <ipv6-prefix | prefix-length>: оставшаяся часть IPv6-адреса, исключая префикс адреса и его длину.

Режим конфигурирования: Режим настройки интерфейса.

Значение по умолчанию: Глобальный адрес не задан.

Описание: IPv6-адреса состоит из двух частей: <prefix-name> и <ipv6-prefix/prefix-length>.

Пример: Назначение адреса 2001:da8:221:2008::2008 с использованием префикса test-prefix равного 2001:da8:221::/48.
Switch(Config-if-Vlan1)#ipv6 address test-prefix 0:0:0:2008::2008/64

13.3.11 ipv6 dhcp client pd

Синтаксис: ipv6 dhcp client pd <prefix-name> [rapid-commit]

no ipv6 dhcp client pd

Назначение: Позволяет сконфигурировать клиент назначения префикса на интерфейсе.

Параметры: <prefix-name>: строка длиной не более 32 символов, которая указывает имя префикса; **rapid-commit**: при указании данной опции, сервер назначения префикса будет отвечать клиенту непосредственно сообщением REPLY.

Режим конфигурирования: Режим настройки интерфейса.

Значение по умолчанию: Клиент назначения префикса выключен.

Описание: Данная команда используется для настройки клиента назначения префикса на интерфейсе. В данном режиме интерфейс будет посылать пакеты SOLICIT для того, чтобы получить префикс адреса с сервера. Эта команда является взаимоисключающей с командами **ipv6 dhcp server** и **ipv6 dhcp relay destination**.

Пример:
Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit

13.3.12 ipv6 dhcp client pd hint

Синтаксис: `ipv6 dhcp client pd hint <prefix | prefix-length>`

`no ipv6 dhcp client pd hint <prefix | prefix-length>`

Назначение: Позволяет назначить требуемый клиентом префикс и его длину.

Параметры: `<prefix | prefix-length>`: требуемый клиентом префикс и его длина.

Режим конфигурирования: Режим настройки интерфейса.

Значение по умолчанию: Не задан.

Описание: Система назначает префикс и его длину на интерфейсе для клиента.

Пример:

```
Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48
```

13.3.13 ipv6 dhcp pool

Синтаксис: `ipv6 dhcp pool <poolname>`

`no ipv6 dhcp pool <poolname>`

Назначение: Позволяет создать DHCPv6 пул адресов.

Параметры: `<poolname>`: имя пула адресов, длина не более 32 символов.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: DHCPv6 пул не создан.

Описание: Данная команда позволяет войти в режим конфигурирования DHCPv6-пула в котором можно настроить соответствующие параметры, такие как префикс адреса, адреса DNS, имя домена.

Пример:

```
Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48
```

13.3.14 ipv6 dhcp relay destination

Синтаксис: `ipv6 dhcp relay destination [[<ipv6-address>] [interface {<interface-name> | vlan <1-4096>}]] }`

`no ipv6 dhcp relay destination { [<ipv6-address>] [interface {<interface-name> | vlan <1-4096>}] }`

Назначение: Позволяет сконфигурировать адрес, куда механизм DHCPv6 relay будет перенаправлять DHCPv6-запросы от клиентов.

Параметры: `<ipv6-address>`: IPv6-адрес назначения; `<interface-name>`: имя интерфейса. Если `<ipv6-address>` является глобальным unicast-адресом, то параметр `<interface-name>` не должен быть использован. Если задан только параметр `<interface-name>`, то будет использоваться мультикаст адрес для всех DHCPv6-серверов ALL_DHCP_Servers (FF05::1:3).

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: DHCPv6 пул не создан.

Описание: Данная команда необходима для указания IPv6-адреса назначения, который будет использоваться при перенаправлении DHCPv6-запросов. Адрес должен быть адресов DHCPv6-сервера или DHCPv6-relay устройства.

Пример:

```
Switch(Config-if-Vlan1)#ipv6 dhcp relay destination 2001:da8::1
```

13.3.15 ipv6 dhcp server

Синтаксис: `ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint]`

`no ipv6 dhcp server <poolname>`

Назначение: Команда для конфигурирования пул адресов, который будет выделен DHCPv6-сервером через указанный интерфейс.

Параметры: **<poolname>**: имя пула адресов, длина не более 32 символов; **rapid-commit**: при указании данной опции, сервер назначения префикса будет отвечать клиенту непосредственно сообщением REPLY после получения сообщения SOLICIT. Если **preference** указан, то параметр **<value>** отвечает за приоритет DHCPv6-сервера. Допускаются значения от 0 до 255. 0 является значением по-умолчанию. Чем больше значение, тем выше приоритет. Если опция **allow-hint** указана, то ожидаемое клиентом значение будет добавлено в его request-пакет.

Режим конфигурирования: Режим настройки интерфейса.

Значение по умолчанию: DHCPv6 пул не создан.

Описание: На одном интерфейсе vlan может быть настроено много пулов DHCPv6.

Пример:

```
Switch(Config-if-Vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint
```

13.3.16 ipv6 general-prefix

Синтаксис: `ipv6 general-prefix <prefix-name> <ipv6-prefix/prefix-length>`

`no ipv6 general-prefix <prefix-name>`

Назначение: Команда для конфигурирования общего префикса адресов.

Параметры: **<prefix-name>**: строка длиной не более 32 символов; **<ipv6-prefix/prefix-length>**: оставшаяся часть IPv6-адреса, исключая префикс адреса и его длину.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Общий префикс не сконфигурирован.

Описание: Если IPv6-префикс задан, то при генерации IPv6-адреса будет использоваться указанный данной командой префикс. Сконфигурированный IPv6-префикс будет зарезервирован в пуле общих префиксов. Может быть сконфигурировано до 8 общих префиксов.

Пример:

```
Switch(config)#ipv6 general-prefix my-prefix 2001:da8:221::/48
```

13.3.17 ipv6 local pool

Синтаксис: `ipv6 local pool <poolname> <prefix/prefix-length> <assigned-length>`

`no ipv6 local pool <poolname>`

Назначение: Команда для конфигурирования пула для выделения префиксов адресов.

Параметры: **<poolname>**: имя пула адресов, длина не более 32 символов; **<ipv6-prefix/prefix-length>**: оставшаяся часть IPv6-адреса, исключая префикс адреса и его длину.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Пул не сконфигурирован.

Описание: Эта команда должна быть использована совместно с командой **prefix delegation pool** для выделения префикса адресов клиентам.

13.3.18 lifetime

Синтаксис: `lifetime {<valid-time> | infinity} {<preferred-time> | infinity}`

`no lifetime`

Назначение: Команда для конфигурирования времени жизни адресов и префиксов, выдаваемых DHCPv6-сервером.

Параметры: **<valid-time>** и **<preferred-time>**: действительное и предпочитаемое время жизни IPv6-адреса. Значение в диапазоне от 1 до 31536000 сек. **<preferred-time>** никогда не должно быть больше значения **<valid-time>**. Параметр **infinity** означает максимальное время жизни.

Режим конфигурирования: Режим конфигурирования DHCPv6-пула.

Значение по умолчанию: Для `<valid-time>` и `<preferred-time>` равно 2592000 сек. (30 дней) и 604800 сек. (7 дней) соответственно.

Описание: Если IPv6-префикс задан, то при генерации IPv6-адреса будет использоваться указанный данной командой префикс. Сконфигурированный IPv6-префикс будет зарезервирован в пуле общих префиксов. Может быть сконфигурировано до 8 общих префиксов.

Пример:

```
Switch(config)#lifetime 1000 600
```

13.3.19 network-address

Синтаксис: `network-address <ipv6-pool-start-address> {<ipv6-pool-end-address> | <prefix-length>} [eui-64]`

`no network-address`

Назначение: Команда для конфигурирования DHCPv6-пула.

Параметры: `<ipv6-pool-start-address>`: начальный адрес пула; `<ipv6-pool-end-address>`: конечный адрес пула; `<prefix-length>`: длина префикса, разрешенная в диапазоне от 3 до 128. Значение по-умолчанию 64. Если опция `eui-64` указана, то DHCPv6-сервер будет выдавать IPv6-адреса на основе eui-64 стандарта.

Режим конфигурирования: Режим конфигурирования DHCPv6-пула.

Значение по умолчанию: DHCPv6-пул не сконфигурирован..

Описание: Данная команда используется для конфигурирования пула адресов DHCPv6-сервера. Только один диапазон может быть сконфигурирован для каждого пула.

Пример:

```
Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200
```

13.3.20 prefix-delegation

Синтаксис: `prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>] [lifetime <valid-time> <preferred-time>]`

`no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]`

Назначение: Команда для конфигурирования выдачи определенного префикса указанному пользователю.

Параметры: `<ipv6-prefix/ prefix-length>`: длина префикса, выдаваемого клиенту; `<client-DUID>`: DUID клиента; DUID типа DUID-LLT и DUID-LL поддерживаются. DUID типа DUID-LLT должен быть из 14 символов; `<iaid>`: значение, которое будет добавлено в IA_PD поле клиентского запроса; `<valid-time>` и `<preferred-time>`: действительное и предпочитаемое время жизни IPv6-адреса. Значение в диапазоне от 1 до 31536000 сек. `<preferred-time>` никогда не должно быть больше значения `<valid-time>`

Режим конфигурирования: Режим конфигурирования DHCPv6-пула.

Значение по умолчанию: Отключено.

Описание: Данная команда используется для конфигурирования префикса адреса для выдвчи указанному клиенту. Максимум 8 префиксов может быть сконфигурировано для каждого пула адресов.

Пример: Назначить адрес 2001:da8::/48 клиенту с DUID 0001000600000005000BBFAA2408 и IAID 12.

```
Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48  
0001000600000005000BBFAA2408 12
```

13.3.21 prefix-delegation pool

Синтаксис: `prefix-delegation pool <poolname> [lifetime <valid-time> <preferred-time>]`

`no prefix-delegation pool <poolname>`

Назначение: Команда для конфигурирования имени пула назначения префикса, используемого DHCPv6-пулом.

Параметры: **<poolname>**: имя пула префиксов адресов, длина не более 32 символов; **<valid-time>** и **<preferred-time>**: действительное и предпочитаемое время жизни IPv6-адреса. Значение в диапазоне от 1 до 31536000 сек. **<preferred-time>** никогда не должно быть больше значения **<valid-time>**, для **<valid-time>** и **<preferred-time>** равно 2592000 сек. (30 дней) и 604800 сек. (7 дней) соответственно.

Режим конфигурирования: Режим конфигурирования DHCPv6-пула.

Значение по умолчанию: Не сконфигурировано.

Описание: Данная команда используется для конфигурирования имени пула префикса адреса для выдвчи указанному клиенту. Команда может быть использована совместно с командой **ipv6 local pool**. Для пула адресов только один пул назначения префиксов может быть привязан.

Пример:

```
Switch(dhcp-1-config)#prefix-delegation pool abc
```

13.3.22 service dhcpv6

Синтаксис: **service dhcpv6**

no service dhcpv6

Назначение: Включает службу DHCPv6. Отмена команды **no service dhcpv6** выключает службу DHCPv6.

Параметры: Нет.

Значение по умолчанию: Служба DHCPv6 выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: В службу DHCPv6 входят DHCPv6-сервер, DHCPv6-relay и DHCPv6-назначение префиксов. Только когда служба DHCPv6 включена глобально, остальные функции могут быть настроены на портах.

Пример: Включить DHCPv6-сервер.

```
Switch(config)#service dhcpv6
```

13.3.23 show ipv6 dhcp

Синтаксис: **show ipv6 dhcp**

Назначение: Отображает состояние службы DHCPv6 и DUID.

Режим конфигурирования: Привилегированный режим.

Описание: Отображает состояние службы DHCPv6 и DUID. Поддерживает только тип DUID-LLT.

Пример:

```
Switch#show ipv6 dhcp
DHCPv6 is enabled
DUID is <00010006000000005001A81112233>
```

13.3.24 show ipv6 dhcp binding

Синтаксис: **show ipv6 dhcp binding [<ipv6-address> | pd <ipv6-prefix | prefix-length> | count]**

Назначение: Отображает привязки адресов и префиксов службы DHCPv6.

Параметры: **<ipv6-address>**: IPv6-адрес; **count**: количество отображаемых DHCPv6-привязок.

Режим конфигурирования: Привилегированный режим.

Описание: Отображает все привязки адресов и префиксов DHCPv6, включая тип, DUID, IAID, префикс и т.д.

Пример: Включить DHCPv6-сервер.

```
Switch#show ipv6 dhcp binding
Client: iatype IANA, iaaid 0x0e001d92
```

```
DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
IANA leased address: 2001:da8::10
Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
Lease obtained at %Jan 01 01:34:44 1970
Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)
```

The number of DHCPv6 bindings is 1

13.3.25 show ipv6 dhcp interface

Синтаксис: `show ipv6 dhcp interface [<interface-name>]`

Назначение: Отображает информацию DHCPv6 для интерфейса.

Параметры: `<interface-name>`: название и номер интерфейса, если интерфейс не указан, то будет выведена информация обо всех интерфейсах.

Режим конфигурирования: Привилегированный режим.

Описание: Отображает информация DHCPv6 для интерфейса, включая настройки в режиме порта и другую требуемую информацию.

Пример:

```
Switch#show ipv6 dhcp interface vlan10
Vlan10 is in server mode
Using pool: poolv6
Preference value: 20
Rapid-Commit is disabled
```

13.3.26 show ipv6 dhcp local pool

Синтаксис: `show ipv6 dhcp local pool`

Назначение: Отображает информацию для DHCPv6 пула префиксов.

Режим конфигурирования: Привилегированный режим.

Описание: Отображает информация для DHCPv6 пула префиксов, включая имя пула префиксов, префикс и длину префикса, количество назначенных префиксов.

Пример:

```
Switch#show ipv6 dhcp pool binding
```

13.3.27 show ipv6 dhcp pool

Синтаксис: `show ipv6 dhcp pool [<poolname>]`

Назначение: Отображает информацию для DHCPv6 пула адресов.

Параметры: `<poolname>`: имя пула префиксов адресов, сконфигурированного на данный момент, длина не более 32 символов;

Режим конфигурирования: Привилегированный режим.

Описание: Отображает информация о настройке DHCPv6 пула адресов, включая имя пула префиксов, префикс, исключаемые адреса, настройку DNS и т.д.

Пример:

```
Switch#show ipv6 dhcp pool poolv6
```

13.3.28 show ipv6 dhcp statistics

Синтаксис: `show ipv6 dhcp statistics`

Назначение: Отображает статистику по всем типам DHCPv6 пакетов для DHCPv6-сервера.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show ipv6 dhcp server statistics
Address pools          1
Active bindings       0
```

```
Expired bindings          0
Malformed message       0
```

```
Message                  Recieved
DHCP6SOLICIT            0
DHCP6ADVERTISE          0
DHCP6REQUEST            0
DHCP6REPLY              0
DHCP6RENEW              0
DHCP6REBIND             0
DHCP6RELEASE            0
DHCP6DECLINE            0
DHCP6CONFIRM            0
DHCP6RECONFIGURE        0
DHCP6INFORMREQ          0
DHCP6RELAYFORW          0
DHCP6RELAYREPLY         0
```

```
Message                  Send
DHCP6SOLICIT            0
DHCP6ADVERTISE          0
DHCP6REQUEST            0
DHCP6REPLY              0
DHCP6RENEW              0
DHCP6REBIND             0
DHCP6RELEASE            0
DHCP6DECLINE            0
DHCP6CONFIRM            0
DHCP6RECONFIGURE        0
DHCP6INFORMREQ          0
DHCP6RELAYFORW          0
DHCP6RELAYREPLY         0
```

13.3.29 show ipv6 general-prefix

Синтаксис: `show ipv6 general-prefix`

Назначение: Отображает информацию общую для префикса IPv6-пула.

Режим конфигурирования: Привилегированный режим.

Описание: Отображает информацию общую для префикса IPv6-пула, включая количество префиксов в общем пуле префиксов, имя каждого префикса и значение префикса.

Пример:

```
Switch#show ipv6 general-prefix
```

13.4 Команды для настройки протокола DHCP Snooping

13.4.1 debug ip dhcp snooping packet interface

Синтаксис: `debug ip dhcp snooping packet interface {[ethernet] <InterfaceName>}`

`no debug ip dhcp snooping packet {[ethernet] <InterfaceName>}`

Назначение: Эта команда используется для включения отладки DHCP SNOOPING и просмотра информации DHCP SNOOPING по приему пакетов.

Параметры: <InterfaceName>: имя интерфейса.

Режим конфигурирования: Привилегированный режим.

Описание: Выводит информацию сообщений DHCP SNOOPING, принятых от конкретного порта.

13.4.2 debug ip dhcp snooping packet

Синтаксис: `debug ip dhcp snooping packet`

no debug ip dhcp snooping packet

Назначение: Эта команда используется для включения отладки DHCP SNOOPING. Позволяет отслеживать процесс обработки сообщений.

Режим конфигурирования: Привилегированный режим.

Описание: Отладочная информация позволяет отслеживать, как DHCP SNOOPING обрабатывает сообщения: добавляет сообщения оповещения, информацию о привязках, передает сообщения DHCP, добавляет или удаляет option 82 и т. д.

13.4.3 debug ip dhcp snooping update

Синтаксис: debug ip dhcp snooping update

no debug ip dhcp snooping update

Назначение: Эта команда используется для включения отладки DHCP SNOOPING и просмотра информации о связи между DHCP SNOOPING и helper-сервером.

Режим конфигурирования: Привилегированный режим.

Описание: Команда выводит на дисплей информацию о сообщениях, принятых и посланных DHCP SNOOPING и helper-сервером.

13.4.4 debug ip dhcp snooping event

Синтаксис: debug ip dhcp snooping event

no debug ip dhcp snooping event

Назначение: Эта команда используется для включения режима отладки DHCP SNOOPING. Позволяет отслеживать состояние задач DHCP SNOOPING.

Режим конфигурирования: Привилегированный режим

Описание: Эта команда, в основном, используется для вывода на дисплей информации о состоянии задач DHCP SNOOPING проверки данных привязки, действий, применяемых к порту и т. д.

13.4.5 debug ip dhcp snooping binding

Синтаксис: debug ip dhcp snooping binding

no debug ip dhcp snooping binding

Назначение: Эта команда включает сообщения отладки DHCP SNOOPING, касающиеся привязок.

Режим конфигурирования: Привилегированный режим

Описание: При DHCP snooping позволяет вывести на дисплей сообщения отладки для привязок agr, dot1x и привязок пользователей.

13.4.6 ip dhcp snooping

Синтаксис: ip dhcp snooping enable

no ip dhcp snooping enable

Назначение: Включает функцию DHCP Snooping.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: Протокол DHCP Snooping не включен.

Описание: Когда эта функция включена, будут контролироваться все пакеты DHCP-сервера для небезопасных портов.

Пример: Включает функцию DHCP Snooping.
Switch(config)#ip dhcp snooping enable

13.4.7 ip dhcp snooping binding

Синтаксис: ip dhcp snooping binding enable

no ip dhcp snooping binding enable

Назначение: Включает функцию привязки DHCP Snooping.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: Привязки DHCP Snooping не включены.

Описание: Когда эта функция включена, будет сохраняться информация о привязках, назначенных DHCP-сервером всем безопасным портам. Функция привязки DHCP SNOOPING может быть включена только после того, как будет включена функция dhcp snooping.

Пример: Включить функцию привязки DHCP Snooping.
switch(config)#ip dhcp snooping binding enable

См. также: ip dhcp snooping enable

13.4.8 ip dhcp snooping binding user

Синтаксис: ip dhcp snooping binding user <mac> address <ipaddress> <mask> vlan <vid> interface [Ethernet] <ifname>

no ip dhcp snooping binding user <mac> interface [Ethernet] <ifname>

Назначение: Позволяет настроить статическую привязку.

Параметры: <mac>: MAC-адрес пользователя со статической привязкой, индекс пользователя с привязкой.

<ipaddress> <mask>: IP-адрес и маска пользователя со статической привязкой;

<vid>: Номер VLAN ID, которой принадлежит пользователь со статической привязкой;

<ifname>: Интерфейс доступа пользователя со статической привязкой.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: DHCP Snooping не имеет списка статических привязок.

Описание: С пользователями, имеющими статическую привязку, DHCP SNOOPING обращается также, как и с теми пользователями, привязки которых получены динамически, в частности, разрешены следующие операции: уведомление DOT1X для пользователей, работающих под управлением DOT1X, прямое добавление пользователей в список безопасных пользователей, добавление в список привязок ARP.

Для пользователей со статической привязкой срок жизни адресов бесконечен, они имеют более высокий приоритет, чем пользователи с динамической привязкой. Пользователи со статической привязкой включаются только после того, как будет включена функция привязки DHCP SNOOPING.

Пример: Настроить пользователей со статической привязкой.
Switch(config)#ip dhcp snooping binding user 00-03-0f-12-34-56 address 192.168.1.16 255.255.255.0 interface Ethernet 0/0/16

См. также: ip dhcp snooping binding enable

13.4.9 ip dhcp snooping binding arp

Синтаксис: ip dhcp snooping binding arp

no ip dhcp snooping binding arp

Назначение: Включает функцию привязки ARP для DHCP Snooping.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: функция привязки ARP для DHCP Snooping не включена.

Описание: Когда эта функция включена, DHCP Snooping будет добавлять привязки (в соответствии с их информацией) в список привязок ARP. Функция привязки ARP будет включена только после включения функции привязки в глобальном режиме конфигурирования. Элементы списка привязок ARP – это статические привязки без настроек резервирования, они добавляются непосредственно в список NEIGHBOUR (соседи). Приоритет элементов списка привязок ARP меньше, чем у статических привязок ARP, заданных администратором, они могут быть заменены статическими привязками ARP. Однако если какие-либо статические привязки ARP будут удалены из списка, элементы списка привязок ARP не будут восстановлены до тех пор пока DHCP Snooping повторно не захватит информацию привязок. Добавление привязок в список ARP используется для предотвращения их подмены атакующим ложным ARP. В то же время для статических привязок в списке не требуется повторной аутентификации, что позволяет предотвратить неуспешные повторные аутентификации ARP при атаках, обусловленных сканированием ARP.

Функция привязки ARP может быть включена только после того, как будет включена функция привязки DHCP Snooping.

Пример: Включить функцию привязки ARP для DHCP Snooping.
Switch(config)#ip dhcp snooping binding arp

См. также: ip dhcp snooping binding enable

13.4.10 ip dhcp snooping binding dot1x

Синтаксис: ip dhcp snooping binding dot1x

no ip dhcp snooping binding dot1x

Назначение: Включает функцию привязки DOT1X для DHCP Snooping.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Настройки по умолчанию: Функция привязки DOT1X выключена на всех портах.

Описание: Когда эта функция включена, DHCP Snooping будет уведомлять модуль DOT1X о захваченной информации привязок для пользователей, осуществляющих управление DOT1X. Эта команда является взаимоисключающей с командой ip dhcp snooping binding user-control. Функция привязки ARP может быть включена только после того, как будет включена функция привязки DHCP Snooping.

Пример: Включить функцию привязки DOT1X на порту ethernet0/0/1.
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet 0/0/1)#ip dhcp snooping binding dot1x

См. также:

Команда	Описание
ip dhcp snooping binding enable	Позволяет включить или выключить функцию привязки dhcp snooping
ip dhcp snooping binding user-control	Позволяет включить функцию привязки пользователя

13.4.11 ip dhcp snooping binding user-control

Синтаксис: ip dhcp snooping binding user-control

no ip dhcp snooping binding user-control

Назначение: Позволяет включить функцию привязки пользователя.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Настройки по умолчанию: Функция привязки пользователя выключена на всех портах.

Описание: Когда эта функция включена, DHCP Snooping будет считать, что вся захваченная информация о привязках относится к безопасным пользователям, которым разрешен доступ ко всем ресурсам. Эта команда является взаимоисключающей с командой ip dhcp snooping binding dot1x.

Функция привязки ARP может быть включена только после того, как будет включена функция привязки DHCP SNOOPING.

Пример: Включить функцию привязки USER на порту ethernet0/0/1.

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet 0/0/1)# ip dhcp snooping binding user-control
```

См. также:

Команда	Описание
<code>ip dhcp snooping binding enable</code>	Позволяет включить или выключить функцию привязки dhcp snooping
<code>ip dhcp snooping binding dot1x</code>	Включает функцию привязки DOT1X для DHCP Snooping

13.4.12 ip dhcp snooping binding user-control max-user

Синтаксис: `ip dhcp snooping binding user-control max-user <number>`

`no ip dhcp snooping binding user-control max-user`

Назначение: Позволяет задать максимальное число пользователей, которым разрешен доступ к порту, когда включена функция DHCP Snooping для привязки пользователей. Отмена команды `no ip dhcp snooping binding user-control max-user` восстанавливает настройки, заданные по умолчанию.

Параметры: `<number>`: максимальное число пользователей, которым разрешен доступ к порту, в пределах от 0 до 1024.

Режим конфигурирования: Режим настройки интерфейсов.

Настройки по умолчанию: Максимальное число пользователей, которым разрешен доступ, на каждом порту равно 1024.

Описание: Команда позволяет задать максимальное число безопасных пользователей в соответствии с информацией привязок, при этом для порта предварительно должна быть выполнена команда `ip dhcp snooping binding user-control`. По умолчанию, число пользователей равно 1024.

Так как аппаратные ресурсы коммутатора ограничены, реальное число безопасных пользователей зависит от количества ресурсов. Если этой командой установлено большое максимальное число пользователей, DHCP Snooping в соответствии с информацией привязок перераспределит ресурсы аппаратуры так, что большая их часть будет выделена безопасным пользователям, а оставшая часть – небезопасным (если на них достаточно ресурсов). Если новое введенное максимальное число пользователей будет меньше, DHCP Snooping вновь перераспределит ресурсы в соответствии с изменившейся информацией привязок. Когда число привязок станет предельно допустимым, новые DHCP-привязки для безопасных пользователей выделяться не будут, они не будут также выделяться для доступа через коммутатор к другим сетевым ресурсам.

Примеры: Включить функцию для привязки пользователей DHCP Snooping на порту ethernet0/0/1, задать максимальное число пользователей при доступе к порту Ethernet0/0/1 равным 5.

```
Switch(Config-If-Ethernet0/0/1)# ip dhcp snooping binding user-control max-user 5
```

См. также: `ip dhcp snooping binding user-control`

13.4.13 ip dhcp snooping trust

Синтаксис: `ip dhcp snooping trust`

`no ip dhcp snooping trust`

Назначение: Позволяет установить или удалить атрибуты безопасности DHCP Snooping для порта.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Настройки по умолчанию: Все порты считаются небезопасными.

Описание: Эта команда работоспособна только в том случае, если DHCP Snooping включено в глобальном режиме конфигурирования. Когда порт превращается из небезопасного в безопасный, оригинальная оборонительная операция порта будет автоматически удалена, будут очищены и все записи из архива записей безопасности (за исключением системных сообщений).

Пример: Задать порт ethernet 0/0/1, как безопасный порт DHCP Snooping.

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet 0/0/1)#ip dhcp snooping trust
```

13.4.14 ip dhcp snooping action

Синтаксис: ip dhcp snooping action {shutdown | blackhole} [recovery <second>]

no ip dhcp snooping action

Назначение: Позволяет задать или удалить оборонительную операцию, выполняемую при атаке на порт.

Параметры: **shutdown:** Когда порт обнаруживает фальшивый DHCP-сервер, порт выключается. Когда порт обнаруживает фальшивый DHCP-сервер, vid и MAC-адрес фальшивого пакета будут использованы для блокирования трафика с этого MAC-адреса.

recovery: Пользователи могут задать выполнение восстановления после автоматического выполнения оборонительной операции (не выключая порты и не удаляя соответствующую блокировку).

second: Пользователи могут задать период времени (в секундах) между выполнением оборонительной операции и восстановлением. Диапазон значений 10—3600 секунд.

Режим конфигурирования: Режим настройки интерфейсов.

Настройки по умолчанию: Оборонительная операция не задана.

Описание: Эта команда работоспособна только в том случае, если DHCP Snooping включено в глобальном режиме конфигурирования. Безопасный порт не будет обнаруживать фальшивый DHCP-сервер, поэтому соответствующая оборонительная операция никогда не будет выполнена. Когда состояние порта изменяется с небезопасного на безопасный, оборонительная операция порта автоматически удаляется.

Пример: На порту ethernet0/0/1 задать оборонительную операцию DHCP Snooping «blackhole» (блокирование трафика по MAC-адресу источника), время восстановления 30 секунд.

```
Switch(config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#ip dhcp snooping action blackhole recovery 30
```

13.4.15 ip dhcp snooping action MaxNum

Синтаксис: ip dhcp snooping action {<maxNum> | default}

Назначение: Позволяет задать число выполняемых оборонительных операций.

Параметры: **<maxNum>:** число оборонительных операций на каждом порту, в пределах 1-200, по умолчанию 10.

default: Восстанавливает значение, заданное по умолчанию.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: 10.

Описание: Позволяет задать максимальное число оборонительных операций, чтобы не растрчивать вычислительные ресурсы при атаках на коммутатор. Если число сообщений сигнализации больше установленного значения, будет принудительно восстановлена оборонительная операция, которая была выполнена раньше всех.

Пример: Задать число оборонительных операций порта 100.

```
switch(config)#ip dhcp snooping action maxnum 100
```

13.4.16 ip dhcp snooping limit-rate

Синтаксис: ip dhcp snooping limit-rate <pps>

no ip dhcp snooping limit-rate

Назначение: Позволяет задать предельную скорость поступления сообщений DHCP.

Параметры: **<pps>**: Число сообщений DHCP, передаваемых в минуту, в пределах от 0 до 100. По умолчанию задано 100.

0 означает, что сообщения DHCP передаваться не будут.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: 100.

Описание: Когда DHCP snooping включено, коммутатор осуществляет мониторинг всех сообщений DHCP и с помощью ПО выполняет их передачу. Производительность ПО зависит от типа коммутатора, от текущей нагрузки на него и т. д. Для коммутатора ZES-2026 предельная скорость передачи сообщений составляет 50pps.

Пример: Задать скорость передачи сообщений 50pps.
`switch(config)#ip dhcp snooping limit-rate 50`

13.4.17 ip dhcp snooping information enable

Синтаксис: `ip dhcp snooping information enable`

`no ip dhcp snooping information enable`

Назначение: Эта команда позволяет включить функцию option 82 DHCP Snooping. Отмена команды `no ip dhcp snooping information enable` выключает эту функцию.

Параметры: Нет.

Настройки по умолчанию: Функция option 82 DHCP Snooping выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда позволяет при DHCP Snooping добавить стандартную информацию option 82 в запросные сообщения DHCP и передать их. Если принято сообщение запроса DHCP с option 82, DHCP Snooping заменит эти опции сообщения своими опциями. Если принято сообщение ответа DHCP с option 82, DHCP Snooping выбросит эти опции из сообщения и передаст его. Описываемая команда и команда `ip dhcp snooping option82 enable` являются взаимоисключающими.

Примеры: Включить функцию коммутатора option 82 DHCP Snooping.
`Switch(config)#ip dhcp snooping enable`
`Switch(config)#ip dhcp snooping binding enable`
`Switch(config)#ip dhcp snooping information enable`

13.4.18 ip dhcp snooping information option

Синтаксис: `ip dhcp snooping information option subscriber-id format {ascii | hex}`

`no ip dhcp snooping information option`

Назначение: Эта команда позволяет выбрать формат представления данных в полях option 82 DHCP Snooping.

Параметры: **ascii**: текстовый формат поля; **hex**: шестнадцатиричный формат представления, в котором каждое поле имеет фиксированную длину.

Настройки по умолчанию: ascii.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда позволяет выбрать формат представления данных в полях DHCP Snooping. В формате **ascii** option1 в option 82 (опция Circuit ID) представляет собой стандартное имя vlan + имя физического порта, например, "vlan1+ethernet1/12". Опция option2 в option 82 (ID удаленного устройства) является MAC-адресом CPU коммутатора, например, "00030f023301". В формате **hex** опция Circuit ID имеет следующее представление:

Тип	Длина	Тип Circuit id	Длина				
1	8	0	6	VLAN	Slot	Module	Port
1 байт	1 байт	1 байт	1 байт	2 байта	1 байт	1 байт	2 байта

Примеры:

```
Switch(config)#ip dhcp snooping information option subscriber-id format hex
```

13.4.19 enable trustview key

Синтаксис: enable trustview key

Назначение: Позволяет настроить ключ шифрования по алгоритму DES для частных пакетов. Кроме того, эта команда включает на коммутаторе шифрование частных пакетов и использование хэш-функции. Отмена команды **no enable trustview key** выключает шифрование.

Параметры: **<password>**: символьная строка длиной не более 16 символов (ключ шифра). 0 означает, что пароли шифроваться не будут, 7 – будут шифроваться.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: функция выключена.

Описание: Коммутатор связывается с системой управления TrustView с помощью частных протоколов. По умолчанию эти пакеты не шифруются. Во избежание перехвата, можно задать шифрование этих пакетов. Одновременно с этим, на сервере TrustView должны быть установлены те же пароли.

Пример: Включить шифрование частных сообщений, включить использование для них хэш-функции.

```
Switch(config)#enable trustview key 0 zes
```

13.4.20 ip user private packet version two

Синтаксис: ip user private packet version two

no ip user private packet version two

Назначение: Команда позволяет установить на коммутаторе версию 2 частных пакетов для связи с trustview.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: На коммутаторе установлена версия 1 частных пакетов для связи с DCBI.

Описание: Если применяется управление доступом DCBI, то для связи с DCBI-сервером на коммутаторе должно быть установлено использование частного протокола версии 1. Однако, если применяется ПО TrustView, должна применяться версия 2.

Пример: Задать на коммутаторе использование частных пакетов версии 2 для связи с системой ZES фоновое управление безопасностью коммутатора.

```
Switch(config)#ip user private packet version two
```

См. также: ip user helper-address

13.4.21 ip user helper-address

Синтаксис: ip user helper-address <svr_addr> [port <udp_port>] source <src_addr> [secondary]

no ip user helper-address [secondary]

Назначение: Позволяет задать адрес и порт HELPER-сервера.

Параметры: <svr_addr>: IP-адрес HELPER-сервера.

udp_port: Порт UDP HELPER-сервера, в пределах 1-65535, значение по умолчанию 9119.

src_addr: IP-адрес локального управления коммутатором;

secondary: Указывает, является ли этот адрес сервера вторичным или нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: Адрес HELPER-сервера не задан.

Описание: DHCP SNOOPING будет посылать контролируемую информацию привязок на HELPER-сервер для ее сохранения. Если запуск коммутатора произошел со сбоями, коммутатор может восстановить данные привязок с HELPER-сервера. Функция HELPER-сервера обычно интегрирована в пакет DCBI. DHCP SNOOPING и HELPER-сервер используют для связи протокол UDP и гарантируют прибытие данных, переданных повторно. Кроме того, HELPER-сервер может использоваться для отправки с сервера данных DOT1X-пользователя. Подробнее об этом см. в главе «Настройка dot1x».

Допускается два адреса HELPER-сервера, в первую очередь DHCP SNOOPING будет пытаться подключиться к первичному серверу. Только в том случае, если первичный сервер недоступен, коммутатор с HELPER-сервером будет пытаться подключиться к вторичному серверу.

Адрес источника является действующим IP-адресом управления коммутатором, если он будет изменен, эта настройка должна быть своевременно обновлена.

Пример: Задать для порта как значения по умолчанию: IP-адрес локального управления 100.1.1.1, адрес первичного HELPER-сервера 100.1.1.100.

```
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 100.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1
```

13.4.22 show trustview status

Синтаксис: show trustview status

Назначение: Позволяет вывести на дисплей все виды информации о частных пакетах, посылаемых и принимаемых коммутатором от TrustView (система фоновое управления безопасностью).

Параметры: Нет.

Режим конфигурирования: Привилегированный режим

Значение по умолчанию: Нет.

Описание: Команда используется для вывода на дисплей отладочных сообщений, характеризующих связь между коммутатором и TrustView-сервером, например, версию протокола уведомления, согласование шифров, общедоступные ресурсы, число сообщений о принудительном завершении регистрации (log-off), число принудительно завершенных сообщений обновления информации учета сервисов.

Пример:

```
Switch#show trustview status
Primary TrustView Server 200.101.0.9:9119
TrustView version2 message inform succeeded
TrustView inform free resource succeeded
TrustView inform web redirect address succeeded
TrustView inform user binding data succeeded
```

13.4.23 show ip dhcp snooping

Синтаксис: show ip dhcp snooping [interface [ethernet] <interfaceName>]

Назначение: Позволяет вывести на дисплей информацию о текущих настройках dhcp snooping, либо об оборонительной операции для указанного порта.

Параметры: <interfaceName>: Имя указанного порта.

Режим конфигурирования: Привилегированный режим

Настройки по умолчанию: Нет.

Описание: Если порт не указан, на дисплей выводятся текущие настройки dhcp snooping, в противном случае, отображаются записи об оборонительных операциях для указанного порта.

Пример:

```
switch#show ip dhcp snooping
DHCP Snooping is enabled
DHCP Snooping binding arp: disabled
DHCP Snooping maxnum of action info:10
DHCP Snooping limit rate: 100(pps), switch ID: 0003.0F12.3456
DHCP Snooping dropped packets: 0, discarded packets: 0
DHCP Snooping alarm count: 0, binding count: 0,
expired binding: 0, request binding: 0
```

interface	trust	action	recovery	alarm num	bind num
Ethernet0/0/1	untrust	none	0	0	0
Ethernet0/0/2	untrust	none	0	0	0
Ethernet0/0/3	untrust	none	0	0	0
Ethernet0/0/4	untrust	none	0	0	0
Ethernet0/0/5	untrust	none	0	0	0
Ethernet0/0/6	untrust	none	0	0	0
Ethernet0/0/7	untrust	none	0	0	0
Ethernet0/0/8	untrust	none	0	0	0
Ethernet0/0/9	untrust	none	0	0	0
Ethernet0/0/10	untrust	none	0	0	0
Ethernet0/0/11	trust	none	0	0	0
Ethernet0/0/12	untrust	none	0	0	0
Ethernet0/0/13	untrust	none	0	0	0
Ethernet0/0/14	untrust	none	0	0	0
Ethernet0/0/15	untrust	none	0	0	0
Ethernet0/0/16	untrust	none	0	0	0
Ethernet0/0/17	untrust	none	0	0	0
Ethernet0/0/18	untrust	none	0	0	0
Ethernet0/0/19	untrust	none	0	0	0
Ethernet0/0/20	untrust	none	0	0	0
Ethernet0/0/21	untrust	none	0	0	0
Ethernet0/0/22	untrust	none	0	0	0
Ethernet0/0/23	untrust	none	0	0	0
Ethernet0/0/24	untrust	none	0	0	0
Ethernet0/0/25	untrust	none	0	0	0
Ethernet0/0/26	untrust	none	0	0	0

Информация, отображаемая на дисплее	Описание
DHCP Snooping is enable	Включено или выключено DHCP Snooping в глобальном режиме конфигурирования.
DHCP Snooping binding arp	Включена или выключена функция привязки ARP.
DHCP Snooping maxnum of action info	Максимальное число оборонительных операций порта
DHCP Snooping limit rate switch ID	Предельно допустимое число принятых пакетов ID коммутатора, используемый для его идентификации, обычно используется MAC-адрес CPU.
DHCP Snooping dropped packets	Число отброшенных сообщений после того как число принятых DHCP-сообщений превысило установленное предельно допустимое число.
discarded packets	Число отброшенных пакетов, обусловленное сбоями связи в системе. Это может происходить, если CPU коммутатора занят обработкой задач DHCP SNOOPING и не успевает обрабатывать принятые DHCP-сообщения
DHCP Snooping alarm count: binding count	Число сообщений сигнализации.
expired binding	Число привязок, которые уже устарели, но пока не удалены. Причина того, что эти привязки не были удалены немедленно состоит в том, что коммутатору необходимо было передать эту информацию на helper –сервер, однако helper –сервер к этому моменту еще не прислал подтверждения о ее получении.
request binding interface	Число пакетов с запросами (REQUEST) Имя порта
trust	Атрибут безопасности порта
action	Автоматическая оборонительная операция порта
recovery	Автоматическое время восстановления порта
alarm num	Число записей в истории событий автоматического выполнения оборонительных операций в порту.
bind num interface	Число привязок для порта. Имя порта
trust attribute	Атрибуты безопасности порта
action	Автоматическая оборонительная операция порта
recovery interval	Интервал восстановления автоматической оборонительной операции порта
maxnum of alarm info	Максимальное число автоматически выполняемых оборонительных операций, которое может быть зарегистрировано портом
binding dot1x	Включена или выключена функция привязки dot1x на порту.
binding user	Включена или выключена функция привязки пользователей в порту.
Alarm info	Число сообщений сигнализации.
Binding info	Число сообщений привязки.
Expired Binding	Информация о привязках, срок жизни которых истек.
Request Binding	Информация о запросах (REQUEST).

```
Switch#show ip dhcp snooping interface ethernet 0/0/1
```

```
interface Ethernet0/0/1 user config:
trust attribute: untrust
action: none
binding dot1x: disabled
binding user: disabled
recovery interval:0(s)
```

Driver user number 0 : Max user number 1024

Alarm info: 0

Binding info: 0

Static Binding info: 0

Static Binding info from shell: 0

Static Binding info from server: 0

flag: D - Dynamic ; U - already upload server ;

S - static binding info from shell; R - static binding info from server;

O - dhcp ack has option82; X - notify dot1x ok;

L - notify driver ok; E - notify dot1x error

Expired Binding: 0

Request Binding: 0

Информация, отображаемая на дисплее	Описание
interface	Имя порта
trust attribute	Атрибуты безопасности порта
action	Автоматическая оборонительная операция порта
recovery interval	Интервал восстановления автоматической оборонительной операции порта
maxnum of alarm info	Максимальное число автоматически выполняемых оборонительных операций, которое может быть зарегистрировано портом
binding dot1x	Включена или выключена функция привязки dot1x на порту.
binding user	Включена или выключена функция привязки пользователей в порту.
Alarm info	Число сообщений сигнализации.
Binding info	Число сообщений привязки.
Expired Binding	Информация о привязках, срок жизни которых истек.
Request Binding	Информация о запросах (REQUEST).

13.4.24 show ip dhcp snooping binding all

Синтаксис: show ip dhcp snooping binding all

Назначение: Позволяет вывести на дисплей информацию о созданных привязках DHCP snooping.

Режим конфигурирования: Привилегированный режим

Настройки по умолчанию: Нет.

Описание: Выводимая информация для каждой записи содержит MAC-адрес, IP-адрес, порт, идентификатор vlan и флаг состояния привязки.

Пример:

```
switch#show ip dhcp snooping binding all
ip dhcp snooping static binding count:1169, dynamic binding count:0
```

```
MAC                IP address          Interface           Vlan ID  Flag
-----
00-00-00-00-11-11  192.168.40.1       Ethernet0/0/1       1        S
00-00-00-00-00-10  192.168.40.10     Ethernet0/0/2       1        D
```

14 Настройка Multicast-протокола IPv4

14.1 Команды настройки фильтров доступа (DCSCM)

14.1.1 access-list (управление multicast-назначением)

Синтаксис: `access-list <6000-7999> {deny | permit} ip {{<source> <source-wildcard>} | {host <source-host-ip>} | any-source} {{<destination> <destination-wildcard>} | {host-destination <destination-host-ip>}|any-destination}`

`no access-list <6000-7999> {deny | permit} ip {{<source> <source-wildcard>} | {host <source-host-ip>} | any} {{<destination> <destination-wildcard>} | {host-destination <destination-host-ip>} | any-destination}`

Назначение: Позволяет настроить список доступа для управления назначением группового трафика. Команда `no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}}{host <source-host-ip>}|any} {{<destination> <destination-wildcard>}}{host-destination <destination-host-ip>}|any-destination}` удаляет список доступа.

Параметры: `<6000-7999>`: Номера списка доступа для управления назначением.

`{deny|permit}`: Разрешить или запретить.

`<source>`: Адрес группового источника.

`<source-wildcard>`: Символ подстановки (*) адреса группового источника.

`<source-host-ip>`: Адрес хоста группового источника.

`<destination>`: Адрес назначения группового трафика.

`<destination-wildcard>`: Символ подстановки (*) адреса назначения группового трафика.

`<destination-host-ip>`: Адрес хоста назначения группового трафика.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Разделу списка доступа ACL назначения группового трафика присвоен специальный номер ACL – от 6000 до 7999. Эта команда используется для настройки соответствующих ACL. Для управления списком доступа ACL назначения (хоста, являющегося членом группы) необходимо только задать IP-адрес источника и IP-адрес назначения (групповой IP-адрес). Процедура настройки в основном такая же, как и для других списков доступа ACL. Символ подстановки (*) используется для настройки диапазона адресов, а также для указания адреса хоста, либо всех адресов. Имейте в виду, что опция "all address" (все адреса) соответствует групповому IP-адресу 224.0.0.0/4, а не 0.0.0.0/0, как в других списках доступа.

Пример:

```
Switch(config)#access-list 6000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0
0.0.0.255
Switch(config)#
```

14.1.2 access-list (управление multicast-источником)

Синтаксис: `access-list <5000-5099> {deny | permit} ip {{<source> <source-wildcard>} | {host <source-host-ip>} | any-source} {{<destination> <destination-wildcard>} | {host-destination <destination-host-ip>} | any-destination}`

`no access-list <5000-5099> {deny | permit} ip {{<source> <source-wildcard>} | {host <source-host-ip>} | any} {{<destination> <destination-wildcard>} | {host-destination <destination-host-ip>} | any-destination}`

Назначение: Позволяет настроить список доступа для управления источником группового трафика. Команда `no access-list<5000-5099> {deny|permit} ip {{<source> <source-wildcard>}}{host<source-host-ip>}|any-source} {{<destination><destination-wildcard>}}{host-destination <destination-host-ip>}|any-destination}` удаляет список доступа.

Параметры: <5000-5099>: Номера списка доступа для управления источником.

{deny|permit}: Разрешить или запретить.

<source>: Адрес группового источника.

<source-wildcard>: Символ подстановки (*) адреса группового источника.

<source-host-ip>: Адрес хоста группового источника.

<destination>: Адрес назначения группового трафика.

<destination-wildcard>: Символ подстановки (*) адреса назначения группового трафика.

<destination-host-ip>: Адрес хоста назначения группового трафика.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Разделу списка доступа ACL группового источника присвоены специальные номера ACL – от 5000 до 5099. Эта команда используется для настройки соответствующего раздела ACL. Для управления списком доступа ACL группового источника необходимо только задать IP-адрес источника и IP-адрес назначения (групповой IP-адрес). Процедура настройки в основном такая же, как и для других списков доступа ACL. Символ подстановки (*) используется для настройки диапазона адресов, а также для указания адреса хоста, либо всех адресов. Имейте в виду, что опция “all address” (все адреса) соответствует групповому IP-адресу 224.0.0.0/4, а не 0.0.0.0/0, как в других списках доступа.

Пример:

```
Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0
0.0.0.255
```

14.1.3 ip multicast destination-control

Синтаксис: ip multicast destination-control

no ip multicast destination-control

Назначение: В глобальном режиме конфигурирования включает управление назначением группового трафика. Отмена команды **no ip multicast destination-control** глобально выключает управление назначением группового трафика.

Параметры: Нет.

Значение по умолчанию: Функция выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Операции по настройке управления назначением группового трафика будут работать только в том случае, если такое управление включено в глобальном режиме конфигурирования. После ввода данной команды igmp snooping будет выполнять проверку на соответствие правилам, после чего, если принято сообщение IGMP REPORT, будет предпринята попытка добавления интерфейса.

Пример:

```
Switch(config)# ip multicast destination-control
```

14.1.4 ip multicast destination-control access-group

Синтаксис: ip multicast destination-control access-group <6000-7999>

no ip multicast destination-control access-group <6000-7999>

Назначение: Позволяет настроить список доступа для управления назначением на интерфейсе. Команда **no ip multicast destination-control access-group <6000-7999>** удаляет сделанные настройки.

Параметры: <6000-7999>: Номер списка доступа для управления назначением.

Значение по умолчанию: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Команда работает, только когда управление назначением групповых данных включено в глобальном режиме конфигурирования. Если оно включено и включен протокол IGMP-SPOOFING, при добавлении интерфейса к группе, он будет проверен на согласование с настройками списка доступа, при этом, если согласование достигнуто, интерфейс будет добавлен, в противном случае - не будет добавлен к группе.

Пример:

```
Switch(config)#inter e 0/0/4
Switch(Config-If-Ethernet 0/0/4)#ip multicast destination-control access-
group 6000
Switch (Config-If-Ethernet0/0/4)#
```

14.1.5 ip multicast destination-control access-group (sip)

Синтаксис: ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

Назначение: Позволяет настроить список доступа для управления назначением на указанном сегменте сети. Отмена команды **no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>** удаляет сделанные настройки.

Параметры: <IPADDRESS/M>: IP-адрес и длина маски.

<6000-7999>: Номер списка доступа для управления назначением.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда работает, только когда управление назначением групповых данных активировано в глобальном режиме конфигурирования. Если оно включено и включен протокол IGMP-SPOOFING, возможно добавление членов в группу. Если управление назначением групповых данных в сегменте сети, указанном в сообщении igmp-report настроено, то проверяется согласование со списком доступа, при этом, если согласование достигнуто, интерфейс добавляется в группу, если нет – не добавляется. Если до ввода этой команды была задана соответствующая группа или источник (выводимый командой ip igmp groups detail), предварительно необходимо в привилегированном режиме с помощью команды clear ip igmp groups уничтожить соответствующие группы.

Пример:

```
Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000
```

14.1.6 ip multicast destination-control access-group (vmac)

Синтаксис: ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999>

no ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999>

Назначение: Позволяет настроить список доступа для управления назначением на указанной сети vlan-mac. Отмена команды **no ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999>** удаляет сделанные настройки.

Параметры: <1-4094>: VLAN-ID;

<macaddr>: MAC-адрес источника, переданный в сообщении IGMP-REPORT в формате "xx-xx-xx-xx-xx-xx";

<6000-7999>: Номер списка доступа для управления назначением.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда работает, только когда управление назначением групповых данных включено в глобальном режиме конфигурирования. Если оно включено и включен протокол IGMP-SPOOFING, возможно добавление членов в группу. Если управление назначением групповых данных по MAC-адресу источника, полученного в сообщении igmp-report настроено, то проверяется согласование со списком доступа, при этом, если согласование достигнуто, новый член будет добавлен в группу.

Пример:

```
Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-  
group 6000
```

14.1.7 ip multicast policy

Синтаксис: `ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>`

`no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos`

Назначение: Позволяет настроить политику обслуживания группового трафика. Отмена команды `no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos` удаляет сделанные настройки.

Параметры: `<IPADDRESS/M>`: Групповой адрес источника, длина маски, адрес назначения, отдельная длина маски.

`<priority>`: Приоритет, в пределах от 0 до 7.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда позволяет изменить настройки, одновременно устанавливая один и тот же приоритет для указанного в ней потока групповых данных и типа обслуживания (TOS). Эта команда принимает параметры в виде `<IPADDRESS>`. Имейте в виду, что приоритет пакетов, переданных в режиме UNTAG (без меток), изменен не будет.

Пример:

```
Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7
```

14.1.8 ip multicast source-control

Синтаксис: `ip multicast source-control`

`no ip multicast source-control`

Назначение: В глобальном режиме конфигурирования включает управление групповым источником. Отмена команды `no ip multicast source-control` выключает (глобально) управление групповым источником.

Параметры: Нет.

Значение по умолчанию: Управление назначением группового трафика не включено.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Управление источником по списку доступа применяется к интерфейсу только тогда, когда управление групповым источником включено в глобальном режиме конфигурирования. По умолчанию, управление групповым источником в глобальном режиме конфигурирования не включено и списки доступа к управлению источником на интерфейсах не сконфигурированы. После ввода команды групповые данные, принятые от интерфейсов и не согласующиеся со списком доступа для группового источника, будут отброшены коммутатором. Вместе с тем, групповые данные, согласующиеся со списком доступа для группового источника, будут приняты коммутатором и переданы в соответствующие интерфейсы.

Пример:

```
Switch(config)#ip multicast source-control
```

14.1.9 ip multicast source-control access-group

Синтаксис: `ip multicast source-control access-group <5000-5099>`

`no ip multicast source-control access-group <5000-5099>`

Назначение: Позволяет настроить список доступа для управления групповым источником на интерфейсе. Отмена команды `no ip multicast source-control access-group <5000-5099>` удаляет сделанные настройки.

Параметры: `<5000-5099>`: Номера списка доступа для управления источником.

Значение по умолчанию: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Команда работает, только когда управление источником групповых данных включено в глобальном режиме конфигурирования. Если оно включено, групповые данные, полученные от интерфейса, будут проверены на согласование с настройками списка доступа. При этом если согласование достигнуто, сообщения будут приняты и переданы на соответствующие интерфейсы, в противном случае они будут отброшены.

Пример:

```
Switch (config)#interface ethernet0/0/4
Switch (Config-If-Ethernet0/0/4)#ip multicast source-control access-group
5000
```

14.1.10 multicast destination-control

Синтаксис: `multicast destination-control`

`no multicast destination-control`

Назначение: Позволяет в глобальном режиме конфигурирования настроить управление назначением multicast-трафиком протоколов IPv4 и IPv6. После ввода этой команды управление назначением multicast-трафика будет выполняться и для трафика протокола IPv4 и для трафика протокола IPv6 (одновременно). Отмена команды **no multicast destination-control** глобально выключает управление назначением группового трафика.

Параметры: Нет.

Значение по умолчанию: функция выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Только после того, как управление назначением multicast-трафика включено в глобальном режиме конфигурирования, станут работать остальные настройки управления назначением multicast-трафика: в портах начнут применяться списки доступа для назначения. После ввода данной команды `igmp snooping` будет выполнять проверку на соответствие правилам, после чего, если принято сообщение IGMP REPORT, будет предпринята попытка добавления интерфейса.

Пример:

```
switch(config)# multicast destination-control
```

14.1.11 show ip multicast destination-control

Синтаксис: `show ip multicast destination-control [detail]`

`show ip multicast destination-control interface <Interfacename> [detail]`

`show ip multicast destination-control host-address <ipaddress> [detail]`

`show ip multicast destination-control <vlan-id> <mac-address> [detail]`

Назначение: Выводит на дисплей настройки назначения группового трафика.

Параметры: **detail:** Задаёт, выводить ли детальную информацию.

<Interfacename>: Имя интерфейса, например, Ethernet 0/0/1 или ethernet 0/0/1, либо port-channel 1.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Команда выводит на дисплей настройки правил управления назначением группового трафика, в том числе (когда выбрана опция `detail`) детальную информацию о них, а также детальную информацию о списке доступа.

Пример:

```
Switch (config)#show ip multicast destination-control
ip multicast destination-control is enabled
ip multicast destination-control 11.0.0.0/8 access-group 6003
ip multicast destination-control 1 00-03-05-07-09-11 access-group 6001
multicast destination-control access-group 6000 used on interface
Ethernet0/0/13
Switch(config)#
```

14.1.12 show ip multicast destination-control access-list

Синтаксис: show ip multicast destination-control access-list

show ip multicast destination-control access-list <6000-7999>

Назначение: Позволяет вывести на дисплей настройки списка доступа ACL для управления назначением.

Параметры: <6000-7999>: идентификатор списка доступа (ACL ID).

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Команда выводит на дисплей настройки списка доступа ACL для управления назначением.

Пример:

```
Switch# sh ip multicast destination-control acc
access-list 6000 deny ip any any-destination
access-list 6000 deny ip any host-destination 224.1.1.1
access-list 6000 deny ip host 2.1.1.1 any-destination
access-list 6001 deny ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6002 permit ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6003 permit ip 2.1.1.0 0.0.0.255 225.0.0.0 0.255.255.255
```

14.1.13 show ip multicast policy

Синтаксис: show ip multicast policy

Назначение: Позволяет вывести на дисплей информацию о настройках политики обслуживания группового трафика.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Команда выводит на дисплей информацию о настройках политики обслуживания группового трафика.

Пример:

```
Switch#show ip multicast policy ip multicast-policy 10.1.1.0/24 225.0.0.0/8
cos 5
```

14.1.14 show ip multicast source-control

Синтаксис: show ip multicast source-control [detail]

show ip multicast source-control interface <Interfacename> [detail]

Назначение: Позволяет вывести на дисплей настройки управления групповым трафиком.

Параметры: detail: Задаёт, выводить ли детальную информацию.

<Interfacename>: Имя интерфейса, например, Ethernet 0/0/1 или ethernet 0/0/1.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Команда выводит на дисплей настройки правил управления групповым источником, в том числе (когда выбрана опция detail) детальную информацию о них, а также детальную информацию о списке доступа.

Пример:

```
Switch#show ip multicast source-control detail
ip multicast source-control is enabled
Interface Ethernet0/0/13 use multicast source control access-list 5000
access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255
```

14.1.15 show ip multicast source-control access-list

Синтаксис: show ip multicast source-control access-list

show ip multicast source-control access-list <5000-5099>

Назначение: Позволяет вывести на дисплей настройки списка доступа ACL для управления источником группового трафика.

Параметры: <5000-5099>: идентификатор списка доступа (ACL ID).

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим, глобальный режим конфигурирования

Описание: Команда выводит на дисплей настройки списка доступа ACL для управления источником группового трафика.

Пример:

```
Switch#sh ip multicast source-control access-list
access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255
```

14.2 Команды настройки IGMP Snooping

14.2.1 clear ip igmp snooping vlan

Синтаксис: clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]

Назначение: Удаляет запись о группе в указанном vlan.

Параметры: <1-4094>: номер vlan; A.B.C.D: IP-адрес группы.

Режим конфигурирования: Привилегированный режим.

Описание: Используйте команду **show ip igmp snooping vlan** для контроля удаления записи о группе.

Пример:

```
Switch#clear ip igmp snooping vlan 1 groups
```

14.2.2 clear ip igmp snooping vlan <1-4094> mrouter-port

Синтаксис: clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet IFNAME | IFNAME]

Назначение: Удаляет mrouter-порт в указанном vlan.

Параметры: <1-4094>: номер vlan; ethernet IFNAME: имя порта ethernet.

Режим конфигурирования: Привилегированный режим.

Описание: Используйте команду **show ip igmp snooping mrouter-port** для контроля удаления информации о mrouter.

Пример:

```
Switch#clear ip igmp snooping vlan 1 mrouter-port
```

14.2.3 debug igmp snooping {all | packet | event | timer | mfc}

Синтаксис: debug igmp snooping {all | packet | event | timer | mfc}

no debug igmp snooping {all | packet | event | timer | mfc}

Назначение: Включает вывод отладочных сообщений IGMP Snooping для коммутатора. Отмена команды **no debug igmp snooping {all | packet | event | timer | mfc}** выключает вывод отладочных сообщений.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Протокол IGMP Snooping не включен.

Описание: Команда используется для включения вывода отладочных сообщений IGMP Snooping для коммутатора, при выборе опции "packet" будут показаны сообщения пакетов данных IGMP коммутатора; при выборе опции "event" будут показаны сообщения о событиях; при выборе опции "time" будут показаны сообщения таймера; при выборе опции "mfc" будут показаны сообщения аппаратного уровня; при выборе опции "all" будут показаны все отладочные сообщения.

14.2.4 ip igmp snooping

Синтаксис: ip igmp snooping

no ip igmp snooping

Назначение: Включает функцию IGMP Snooping. Отмена команды **no ip igmp snooping** выключает эту функцию.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Протокол IGMP Snooping не включен.

Описание: Используйте эту команду для активации IGMP Snooping. После этого можно будет настроить работу IGMP snooping на каждом vlan.

Пример: Включить протокол IGMP Snooping.

```
Switch(config)#ip igmp snooping
```

14.2.5 ip igmp snooping vlan

Синтаксис: ip igmp snooping vlan <vlan-id>

no ip igmp snooping vlan <vlan-id>

Назначение: Включает для указанного VLAN функцию IGMP Snooping. Отмена команды **no ip igmp snooping vlan <vlan-id>** выключает функцию IGMP Snooping на указанном vlan.

Параметры: <vlan-id>: номер VLAN.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Протокол IGMP Snooping не включен.

Описание: Для того, чтобы настроить IGMP Snooping на указанном vlan, необходимо сначала активировать IGMP Snooping глобально.

Пример: Включить IGMP Snooping для VLAN 100 в глобальном режиме конфигурирования.

```
Switch(config)#ip igmp snooping vlan 100
```

14.2.6 ip igmp snooping vlan immediate-leave

Синтаксис: ip igmp snooping vlan <vlan-id> immediate-leave

no ip igmp snooping vlan <vlan-id> immediate-leave

Назначение: Включает для указанного VLAN функцию быстрого выхода (IGMP fast leave). Отмена команды **no ip igmp snooping vlan <vlan-id> immediate-leave** выключает функцию быстрого выхода IGMP.

Параметры: <vlan-id>: номер указанного VLAN, в пределах <1 — 4094>.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: функция выключена.

Описание: Включает функцию быстрого выхода IGMP Snooping для указанного vlan.

Пример: Включить для VLAN 100 функцию быстрого выхода (IGMP fast leave).

```
Switch(config)#ip igmp snooping vlan 100 immediate-leave
```

14.2.7 ip igmp snooping vlan l2-general-querier

Синтаксис: ip igmp snooping vlan <vlan-id> l2-general-querier

no ip igmp snooping vlan <vlan-id> l2-general-querier

Назначение: Устанавливает указанный vlan, как маршрутизатор уровня 2.

Параметры: vlan-id: номер VLAN, в пределах <1-4094>.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: vlan не является маршрутизатором IGMP Snooping уровня 2

Описание: Рекомендуется конфигурировать маршрутизатор уровня 2 на сегменте. Если функция IGMP Snooping ранее на этой vlan не была включена, после ввода этой команды она будет включена. Функция IGMP Snooping не будет выключена после выключения функции маршрутизатора уровня 2. Эта команда в основном используется для регулярной отправки общих запросов, помогающих осуществлять коммутацию внутри этого сегмента путем обучения портов mrouter.

Примечание: Существует три метода обучения mrouter при igmp snooping:

1. Порт принимает сообщения запросов IGMP.
2. Порт принимает пакеты группового протокола и поддерживает DVMRP, PIM.
3. Порт сконфигурирован статически.

14.2.8 ip igmp snooping vlan l2-general-querier-source

Синтаксис: ip igmp snooping vlan <vlanid> l2-general-query-source <A.B.C.D>

no ip igmp snooping vlan <vlanid> l2-general-query-source

Назначение: Позволяет задать адрес источника для маршрутизатора IGMP snooping уровня 2.

Параметры: <vlanid>: номер VLAN, в пределах <1 — 4094>.

<A.B.C.D>: адрес источника.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 0.0.0.0

Описание: Операционные системы Win2000/XP при запросе не поддерживают адрес 0.0.0.0, поэтому они не определяют адрес источника при запросе уровня 2. Клиент не будет посылать запрос (когда он у него возникает) и не будет принимать групповой трафик.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 l2-general-query-source 192.168.1.2
```

14.2.9 ip igmp snooping vlan l2-general-querier-version

Синтаксис: ip igmp snooping vlan <vlanid> l2-general-query-version <version>

Параметры: vlan-id: номер VLAN, в пределах <1 — 4094>.

version: Номер версии, в пределах <1 — 3>.

Назначение: Настройка протокола IGMP Snooping

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: версия 3.

Описание: Когда коммутатор работает в условиях, при которых поддерживаются только версии V1 или V2, vlan, который, является источником уровня 2, может быть найден по номеру версии, ему соответствующей. Команда позволяет задать номер версии.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 L2-general-query-version 2
```

14.2.10 ip igmp snooping vlan limit

Синтаксис: ip igmp snooping vlan <vlan-id> limit {group <g_limit> | source <s_limit>}

no ip igmp snooping vlan <vlan-id> limit

Назначение: Позволяет задать максимальное число групп для vlan и максимальное число источников, которые может иметь группа. Отмена команды **no ip igmp snooping vlan <vlan-id> limit** восстанавливает настройки, используемые по умолчанию.

Параметры: <vlan-id>: номер VLAN.

g_limit максимальное число создаваемых групп, в пределах <1 — 65535>;

s_limit: максимальное число членов группы для указанной VLAN с учетом ресурсов по включению в группу и исключению из нее, в пределах <1 — 65535>.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Не более 50 групп, в каждой группе может быть не более 40 источников.

Описание: Когда число вступивших в группу достигнет заданного предельного значения, новые запросы на вступление в группу будут отвергаться – это необходимо для предотвращения сетевых атак. Для того, чтобы эту команду можно было использовать, IGMP snooping должен быть включен на vlan. При вводе отрицательной формы команды (с “no”), будут восстановлены настройки по умолчанию, при этом они отличаются от настройки “no limit” (число вступающих в группу не ограничено). По соображениям безопасности в этой команде не следует использовать опцию “no limit”. Рекомендуется использовать настройку, заданную по умолчанию.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 limit group 300
```

14.2.11 ip igmp snooping vlan mrouter-port interface

Синтаксис: ip igmp snooping vlan <vlan-id> mrouter-port interface [<ethernet> | <ifname> | <port-channel>]

no ip igmp snooping vlan <vlan-id> mrouter-port interface [<ethernet> | <ifname> | <port-channel>]

Назначение: Позволяет настроить на vlan статический порт mrouter. Отмена команды **no ip igmp snooping vlan <vlan-id> mrouter-port interface [<ethernet> | <ifname> | <port-channel>]** отменяет эту настройку.

Параметры: vlan-id: Номер VLAN, в пределах <1-4094>.

ethernet: Имя Ethernet-порта.

ifname: Имя интерфейса.

port-channel: Агрегация порта.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Статический порт mrouter на vlan отсутствует.

Описание: Когда порт является статическим портом mrouter (и одновременно с этим – динамическим портом mrouter), он должен использоваться как статический порт mrouter.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet0/0/13
```

14.2.12 ip igmp snooping vlan mrpt

Синтаксис: ip igmp snooping vlan <vlan-id> mrpt <value>

no ip igmp snooping vlan <vlan-id> mrpt

Назначение: Позволяет задать срок жизни порта mrouter.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: Срок жизни порта mrouter , в пределах <1-65535> секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 255 секунд.

Описание: Эта команда корректна только для динамических портов mrouter. Для того, чтобы эту команду можно было использовать, на vlan должен быть включен IGMP snooping.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 mrpt 100
```

14.2.13 ip igmp snooping vlan report source-address

Синтаксис: ip igmp snooping vlan <vlan-id> report source-address <A.B.C.D>

no ip igmp snooping vlan <vlan-id> report source-address

Назначение: Позволяет задать IP-адрес источника, используемый при перенаправлении IGMP сообщений.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>; **A.B.C.D:** IP-адрес, может быть 0.0.0.0.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Адрес не задан.

Описание: IP-адрес, используемый при перенаправлении IGMP сообщений может быть 0.0.0.0. IP-адрес также может быть задан явно, если этого требуют вышестоящие устройства.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 report source-address 10.1.1.1
```

14.2.14 ip igmp snooping vlan static-group

Синтаксис: ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>

no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>

Назначение: Позволяет задать статическую группу на указанном порту vlan.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>; **A.B.C.D:** IP-адрес группы или источника; **port-channel:** агрегационный порт; **IFNAME:** имя интерфейса.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Статические группы не заданы.

Пример:

```
Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source 192.168.1.1 interface ethernet 0/0/1
```

14.2.15 ip igmp snooping vlan query-interval

Синтаксис: ip igmp snooping vlan <vlan-id> query-interval <value>

no ip igmp snooping vlan <vlan-id> query-interval

Назначение: Позволяет задать интервал отправки запросов.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: интервал выдачи запросов, в пределах <1-65535> секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 125 секунд.

Описание: Рекомендуется использовать настройку, заданную по умолчанию. По возможности согласуйте эту настройку с настройками IGMP, если протокол IGMP уровня 3 включен.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 query-interval 130
```

14.2.16 ip igmp snooping vlan query-mrsp

Синтаксис: ip igmp snooping vlan <vlan-id> query-mrsp <value>

no ip igmp snooping vlan <vlan-id> query-mrsp

Назначение: Позволяет настроить максимальный интервал времени ожидания ответа. Отмена команды **no ip igmp snooping vlan <vlan-id> query-mrsp** восстанавливает настройки, используемые по умолчанию.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: максимальный интервал времени ожидания ответа в пределах <1-25> секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 10 секунд.

Описание: Рекомендуется использовать настройку, заданную по умолчанию. По возможности согласуйте эту настройку с настройками IGMP, если протокол IGMP уровня 3 включен.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 query-mrsp 18
```

14.2.17 ip igmp snooping vlan query-robustness

Синтаксис: ip igmp snooping vlan <vlan-id> query-robustness <value>

no ip igmp snooping vlan <vlan-id> query-robustness

Назначение: Позволяет задать надежность запроса. Отмена команды **no ip igmp snooping vlan <vlan-id> query-robustness** восстанавливает значение, используемое по умолчанию.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: Надежность запросов, в пределах <2 — 10>.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Надежность запросов равна 2.

Описание: Рекомендуется использовать настройку, заданную по умолчанию. По возможности согласуйте эту настройку с настройками IGMP, если протокол IGMP уровня 3 включен.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 query-robustness 3
```

14.2.18 ip igmp snooping vlan suppression-query-time

Синтаксис: ip igmp snooping vlan <vlan-id> suppression-query-time <value>

no ip igmp snooping vlan <vlan-id> suppression-query-time

Назначение: Позволяет задать время подавления запроса. Отмена команды **no ip igmp snooping vlan <vlan-id> suppression-query-time** восстанавливает значение, используемое по умолчанию.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: время подавления запроса, в пределах <1 — 65535> секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 255 секунд.

Описание: Эта команда может быть выдана только для маршрутизатора уровня 2. Команда `Suppression-query-time` устанавливает период, в течение которого устанавливается состояние подавления, в котором маршрутизатор включается, когда он принимает запрос от IGMP уровня 3 в сегментах.

Пример:

```
Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270
```

14.2.19 show ip igmp snooping

Синтаксис: `show ip igmp snooping [vlan <vlan-id>]`

Параметры: `<vlan-id>`: номер vlan, для которого на дисплей выводится информация IGMP Snooping.

Режим конфигурирования: Привилегированный режим.

Описание: Если номер vlan не указан, на дисплей будет выведена следующая информация: включен или нет протокол `igmp snooping` в глобальном режиме конфигурирования; на каких vlan включена функция маршрутизатора уровня 2. Если номер vlan указан, на дисплей будут выведены детальные сообщения IGMP для этой vlan.

Пример:

Вывести на дисплей сводную информацию IGMP Snooping коммутатора.

```
Switch(config)#show ip igmp snooping
Global igmp snooping status: Enabled
L3 multicasting: running
Igmp snooping is turned on for vlan 1(querier)
Igmp snooping is turned on for vlan 2
```

Информация, отображаемая на дисплее	Описание
Global igmp snooping status	Включен ли <code>igmp snooping</code> в глобальном режиме конфигурирования коммутатора.
L3 multicasting	Включен ли <code>multicast</code> -протокол уровня 3 коммутатора.
Igmp snooping is turned on for vlan 1(querier)	На каких vlan коммутатора включена функция <code>igmp snooping</code> коммутатора и какие из них являются маршрутизаторами уровня 2.

Вывести на дисплей детальную информацию IGMP Snooping для vlan1.

```
Switch#show ip igmp snooping vlan 1
Igmp snooping information for vlan 1
Igmp snooping L2 general querier :Yes(COULD_QUERY)
Igmp snooping query-interval :125(s)
Igmp snooping max reponse time :10(s)
Igmp snooping robustness :2
Igmp snooping mrouter port keep-alive time :255(s)
Igmp snooping query-suppression time :255(s)
IGMP Snooping Connect Group Membership Note: *-All Source, (S)- Include
Source, [S]-Exclude Source Groups Sources Ports Exptime System Level
238.1.1.1 (192.168.0.1) Ethernet1/8 00:04:14 V2 (192.168.0.2) Ethernet1/8
00:04:14 V2
Igmp snooping vlan 1 mrouter port Note: "!"-static mrouter port !Ethernet1/2
```

Информация, отображаемая на дисплее	Описание
Igmp snooping L2 general querier	Включена ли для vlan функция маршрутизатора уровня 2, состояние маршрутизатора: Запросы разрешены или подавлены.
Igmp snooping query-interval	Интервал запроса, установленный на vlan

Igmp snooping max reponse time	Максимальное время ответа vlan
Igmp snooping robustness	Надежность vlan
Igmp snooping mrouter port keep-alive time	Срок жизни порта mrouter на vlan
Igmp snooping query-suppression time	Интервал времени подавления запросов vlan, когда она работает в качестве маршрутизатора уровня 2
IGMP Snooping Connect Group Membership	Группа vlan, соответствие между портом и (S,G).
Igmp snooping vlan 1 mrouter port	Порт mrouter vlan (статический и динамический).

15 Настройка Multicast-протокола IPv6

15.1 Команды настройки DCSCM протокола IPv6

15.1.1 ipv6 access-list (управление multicast-источником с ipv6-адресом)

Синтаксис: `ipv6 access-list <8000-8099> {deny | permit} {{<source/M>} | {host-source <source-host-ip>} | any-source} {{<destination/M>} | {host-destination <destination-host-ip>} | any-destination}`

`no ipv6 access-list <8000-8099> {deny | permit} {{<source/M>} | {host-source <source-host-ip>} | any-source} {{<destination/M>} | {host-destination <destination-host-ip>} | any-destination}`

Назначение: Позволяет настроить список доступа для управления IPv6-источником multicast-трафика. Отмена команды `no ipv6 access-list <8000-8099> {deny | permit} {{<source/M>} | {host-source <source-host-ip>} | any-source} {{<destination/M>} | {host-destination <destination-host-ip>} | any-destination}` удаляет список доступа.

Параметры: `<8000-8099>`: Номера списка доступа для управления источником.

`{deny | permit}`: Разрешить или запретить.

`<source/M>`: Адрес multicast-источника и длина маски.

`<source-host-ip>`: Адрес хоста источника multicast-трафика.

`<destination/M>`: Адрес назначения multicast-трафика и длина маски.

`<destination-host-ip>`: Адрес хоста назначения multicast-трафика.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Разделу списка доступа ACL IPv6 multicast - источника присвоен специальный номер ACL — от 8000 до 8099. Эта команда используется для настройки соответствующего раздела списка доступа ACL. Для управления списком доступа ACL IPv6 multicast -источника необходимо задать IPv6-адрес источника и IPv6-адрес назначения (групповой IPv6-адрес). Процедура настройки в основном такая же, как и для других списков доступа ACL. Для настройки диапазона адресов используется длина маски, либо можно указать адреса хостов или все адреса. Имейте в виду, что опция "all address" (все адреса) соответствует групповому IPv6-адресу ff::/8.

Пример:

```
Switch(config)#ipv6 access-list 8000 permit fe80::203:228a/64 ff1e::1/64
```

15.1.2 ipv6 access-list (управление назначением multicast-трафика)

Синтаксис: `ipv6 access-list <9000-10999> {deny | permit} {{<source/M>} | {host-source <source-host-ip>} | any-source} {{<destination/M>} | {host-destination <destination-host-ip>} | any-destination}`

`no ipv6 access-list <9000-10999> {deny | permit} {{<source/M>} | {host-source <source-host-ip>} | any-source} {{<destination/M>} | {host-destination <destination-host-ip>} | any-destination}`

Назначение: Позволяет настроить список доступа для управления IPv6-назначением multicast-трафика. Отмена команды `no ipv6 access-list <9000-10999> {deny|permit} {{<source/M>} | {host-source <source-host-ip>} | any-source} {{<destination/M>} | {host-destination <destination-host-ip>} | any-destination}` удаляет список доступа.

Параметры: `<9000-10999>`: Номера списка доступа для управления назначением.

`{deny|permit}`: Разрешить или запретить.

`<source/M>`: Адрес multicast-источника и длина маски.

`<source-host-ip>`: Адрес хоста multicast-источника.

<destination/M>: Адрес назначения multicast-трафика и длина маски.

<destination-host-ip>: Адрес хоста назначения multicast-трафика.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Разделу списка доступа ACL IPv6 multicast - назначения присвоен специальный номер ACL — от 9000 до 10999. Эта команда используется для настройки соответствующего раздела списка доступа ACL. Для управления списком доступа ACL IPv6 multicast -источника необходимо задать IPv6-адрес источника и IPv6-адрес назначения (групповой IPv6-адрес). Процедура настройки в основном такая же, как и для других списков доступа ACL. Для настройки диапазона адресов используется длина маски, либо можно указать адреса хостов или все адреса, которыми необходимо управлять. Имейте в виду, что опция “all address” (все адреса) соответствует групповому IPv6-адресу ff::/8.

Пример:

```
Switch(config)#ipv6 access-list 9000 permit fe80::203:228a/64 ffe::1/64
```

15.1.3 ipv6 multicast destination-control access-group

Синтаксис: `ipv6 multicast destination-control access-group <9000-10999>`

`no ipv6 multicast destination-control access-group <9000-10999>`

Назначение: Позволяет настроить список доступа для управления IPv6-назначением multicast-трафика на интерфейсе. Отмена команды: “no ipv6 multicast destination-control access-group <9000-10999>” удаляет сделанные настройки.

Параметры: <9000-10999>: Номера списка доступа для управления назначением.

Значение по умолчанию: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Команда работает, когда управление IPv6-назначением multicast - данных включено в глобальном режиме конфигурирования. Если оно включено и включен протокол MLD-SPOOPING, при добавлении интерфейса к multicast-группе он будет проверен на согласование с настройками списка доступа, при этом, если согласование достигнуто, интерфейс будет добавлен, в противном случае интерфейс не будет добавлен к группе.

Пример:

```
Switch(config)#inter ethernet 0/0/4
Switch(Config-If-Ethernet0/0/4)#ipv6 multicast destination-control access-
group 9000
Switch(Config-If-Ethernet0/0/4)#
```

15.1.4 ipv6 multicast destination-control access-group (sip)

Синтаксис: `ipv6 multicast destination-control <IPADDRESS/M> access-group <9000-10999>`

`no ipv6 multicast destination-control <IPADDRESS/M> access-group <9000-10999>`

Назначение: Позволяет настроить список доступа для управления назначением multicast-трафика в указанном сегменте сети. Отмена команды `no ipv6 multicast destination-control <IPADDRESS/M> access-group<9000-10999>` удаляет сделанные настройки.

Параметры: <IPADDRESS/M>: IP-адрес и длина маски.

<9000-10999>: Номер списка доступа для управления назначением.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда работает, только когда управление назначением multicast-данных включено в глобальном режиме конфигурирования. Если оно включено и включен протокол MLD-SPOOPING или MLD, возможно добавление членов в multicast-группу. Если управление назначением multicast-данных в сегменте сети, указанном в сообщении MLD-REPORT настроено, то проверяется согласование со списком доступа, при этом: если согласование достигнуто,

интерфейс добавляется в группу, если нет – не добавляется. Если до ввода этой команды была задана соответствующая группа или источник (выводимая командой `show ipv6 mld groups detail`), предварительно необходимо в привилегированном режиме с помощью команды `clear ipv6 mld group` уничтожить соответствующие группы.

Пример:

```
Switch(config)#ipv6 multicast destination-control 2008::8/64 access-group 9000
```

15.1.5 ipv6 multicast destination-control access-group (vmac)

Синтаксис: `ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10999>`

`no ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10999>`

Назначение: Позволяет настроить список доступа для управления IPv6-назначением multicast-трафика на указанной сети vlan-mac. Отмена команды `no ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10999>` удаляет сделанные настройки.

Параметры: `<1-4094>`: VLAN-ID;

`<macaddr>`: MAC-адрес источника, переданный в сообщении MLD-REPORT в формате "xx-xx-xx-xx-xx";

`<9000-10999>`: Номер списка доступа для управления назначением.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда работает, когда управление IPv6-назначением multicast - данных включено в глобальном режиме конфигурирования. Если оно включено и включен протокол MLD-SPOOFING, при добавлении интерфейса к multicast-группе он будет проверен на согласование с настройками списка доступа, при этом, если согласование достигнуто, интерфейс будет добавлен, в противном случае интерфейс не будет добавлен к группе.

Пример:

```
Switch(config)#ipv6 multicast destination-control 1 00-01-03-05-07-09 access-group 9000
```

15.1.6 ipv6 multicast policy

Синтаксис: `ipv6 multicast policy <IPADDRSRC/M> <IPADDRGRP/M> cos <priority>`

`no ipv6 multicast policy <IPADDRSRC/M> <IPADDRGRP/M> cos`

Назначение: Позволяет настроить политику обслуживания IPv6 multicast-трафика. Отмена команды `no ipv6 multicast policy <IPADDRSRC/M> <IPADDRGRP/M> cos` удаляет сделанные настройки.

Параметры: `<IPADDRESS/M>`: IPv6-адрес multicast-источника и длина маски.

`<IPADDRESS/M>`: IPv6 multicast-адрес источника, длина маски multicast-адреса.

`<priority>`: Диапазон приоритетов: `<0-7>`.

Значение по умолчанию: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда позволяет изменить настройки, одновременно устанавливая один и тот же приоритет для указанных в ней потока multicast-данных и типа обслуживания (TOS). Имейте в виду, что приоритет пакетов, переданных в режиме UNTAG (без меток), изменен не будет.

Пример:

```
Switch(config)#ipv6 multicast policy 2008::1/64 ff1e::3/64 cos 4
```

15.1.7 ipv6 multicast source-control

Синтаксис: `ipv6 multicast source-control`

no ipv6 multicast source-control

Назначение: Позволяет включить управление IPv6-источником multicast-трафика в глобальном режиме конфигурирования. Отмена команды **no ipv6 multicast source-control** выключает управление IPv6-источником multicast-трафика в глобальном режиме конфигурирования.

Параметры: Нет.

Значение по умолчанию: функция выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Списки управления источником в портах будут работать только в том случае, если управление IPv6-источником multicast-трафика включено в глобальном режиме конфигурирования. После ввода этой команды, IPv6 multicast-данные, принятые всеми портами коммутатора будут отбрасываться, если они не согласуются с каким-либо элементом списка управления multicast-источником. Будут приниматься и передаваться только multicast-данные, для которых достигнуто согласование (определена операция PERMIT).

Пример:

```
Switch(config)#ipv6 multicast source-control
```

15.1.8 ipv6 multicast source-control access-group

Синтаксис: **ipv6 multicast source-control access-group <8000-8099>**

no ipv6 multicast source-control access-group <8000-8099>

Назначение: Позволяет настроить список доступа для управления IPv6-источником multicast-трафика на интерфейсе. Отмена команды **no ipv6 multicast source-control access-group <8000-8099>** удаляет сделанные настройки.

Параметры: **<8000-8099>**: Номера списка доступа для управления источником.

Значение по умолчанию: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Описание: Эта команда будет работать только в том случае, если управление IPv6-источником multicast-трафика включено в глобальном режиме конфигурирования. После ввода данной команды все IPv6 multicast-сообщения приходящие из интерфейса будут проверяться на согласование со списком доступа. Будут приниматься и передаваться только multicast-данные, для которых достигнуто согласование, остальные multicast-данные будут отброшены.

Пример:

```
Switch(Config-If-Ethernet0/0/4)#ipv6 multicast source-control access-group  
8000
```

15.1.9 multicast destination-control

Синтаксис: **multicast destination-control**

no multicast destination-control

Назначение: Позволяет в глобальном режиме конфигурирования настроить управление назначением multicast-трафиком протоколов IPv4 и IPv6. После ввода этой команды управление назначением multicast-трафика будет выполняться и для трафика протокола IPv4 и для трафика протокола IPv6 (одновременно). Отмена команды **no multicast destination-control** глобально выключает управление назначением группового трафика.

Параметры: Нет.

Значение по умолчанию: функция выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Только после того, как управление назначением multicast-трафика включено в глобальном режиме конфигурирования, станут работать остальные настройки управления назначением multicast-трафика: в портах начнут применяться списки доступа для назначения. После ввода команды и выполнения вышеупомянутой проверки — при IGMP-SNOOPING, MLD-

SNOOPING и IGMP, MLD, когда принято сообщение с отчетом IGMP REPORT и MLD-REPORT, будет предпринята попытка добавления интерфейсов.

Пример:

```
Switch(config)# multicast destination-control
```

15.1.10 show ipv6 multicast destination-control

Синтаксис: `show ipv6 multicast destination-control [detail]`

`show ipv6 multicast destination-control interface <Interfacename> [detail]`

`show ipv6 multicast destination-control host-address <ipv6addr> [detail]`

`show ipv6 multicast destination-control <vlan-id> <mac> [detail]`

Назначение: Позволяет вывести на дисплей настройки управления назначением IPv6 multicast-трафика.

Параметры: **detail:** Задаёт, выводить ли детальную информацию.

<Interfacename>: имя интерфейса.

<ipv6addr>: IPv6-адрес.

<vlan-id>: VLAN-ID;

<mac>: MAC-адрес.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей сконфигурированные правила управления назначением multicast-трафика. Если задана опция detail, будет выведена подробная информация об используемом списке управления доступом.

Пример:

```
switch(config)#show ipv6 multicast destination-control
ipv6 multicast destination-control is enabled
ipv6 multicast destination-control 2003::1/64
access-group 9003 ipv6 multicast destination-control 1 00-03-05-07-09-11
access-group 9001 multicast destination-control access-group 6000 used on
interface Ethernet0/0/13
```

15.1.11 show ipv6 multicast destination-control access-list

Синтаксис: `show ipv6 multicast destination-control access-list`

`show ip multicast destination-control access-list <9000-10999>`

Назначение: Позволяет вывести на дисплей сконфигурированный список управления назначением IPv6 multicast-трафика.

Параметры: **<9000-10999>:** идентификатор списка доступа (ACL ID).

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда выводит на дисплей сконфигурированный список управления назначением IPv6 multicast-трафика.

Пример:

```
switch# show ipv6 multicast destination-control acc
ipv6 access-list 9000 permit 2003::2/64 ffla::3/64
ipv6 access-list 9000 deny 2008::1/64 ffla::1/64
ipv6 access-list 9000 permit any-source any-destination
ipv6 access-list 9001 deny any-source host-destination ffla::1
ipv6 access-list 9001 permit any-source any-destination
```

15.1.12 show ipv6 multicast policy

Синтаксис: show ipv6 multicast policy

Назначение: Позволяет вывести на дисплей настройки политик обслуживания IPv6 multicast-трафика.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Выводит на дисплей настройки политики обслуживания IPv6 multicast-трафика.

Пример:

```
Switch#show ipv6 multicast policy
ipv6 multicast-policy 2003::2/64 ffile::3/64 cos 5
```

15.1.13 show ipv6 multicast source-control

Синтаксис: show ipv6 multicast source-control [detail]

show ipv6 multicast source-control interface <Interfacename> [detail]

Назначение: Позволяет вывести на дисплей настройки управления источником IPv6 multicast-трафика.

Параметры: **detail:** Задаёт, выводить ли детальную информацию.

<Interfacename>: имя порта.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей сконфигурированные правила управления источником multicast-трафика. Если задана опция detail, будет выведена подробная информация об используемом списке управления доступом.

Пример:

```
Switch#show ipv6 multicast source-control detail
Ipv6 multicast source-control is enabled Interface Ethernet 0/0/1 use
multicast source control access-list 8000
ipv6 access-list 8000 permit 2003::2/64 ffile::3/64
ipv6 access-list 8000 deny 2008::1/64 ffile::1/64
ipv6 access-list 8000 permit any-source any-destination
```

15.1.14 show ipv6 multicast source-control access-list

Синтаксис: show ipv6 multicast source-control access-list

show ipv6 multicast source-control access-list <8000-8099>

Назначение: Позволяет вывести на дисплей сконфигурированный список управления источником IPv6 multicast-трафика.

Параметры: **<8000-8099>:** идентификатор списка доступа (ACL ID).

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда выводит на дисплей сконфигурированный список управления источником IPv6 multicast-трафика.

Пример:

```
switch#sh ipv6 multicast source-control access-list
ipv6 access-list 8000 permit 2003::2/64 ffile::3/64
ipv6 access-list 8000 deny 2008::1/64 ffile::1/64
```

15.2 Команды для настройки MLD Snooping

15.2.1 clear ipv6 mld snooping vlan

Синтаксис: `clear ipv6 mld snooping vlan vlan <1-4094> groups [X:X::X:X]`

Назначение: Удаляет запись о группе в указанном vlan.

Параметры: `<1-4094>`: номер vlan; `X:X::X:X`: адрес группы.

Режим конфигурирования: Привилегированный режим.

Описание: Используйте команду `show ipv6 mld snooping vlan <1-4094>` для контроля удаления записи о группе.

Пример: Удалить все группы.

```
Switch#clear ipv6 mld snooping vlan 1 groups
```

15.2.2 clear ipv6 mld snooping vlan <1-4094> mrouter-port

Синтаксис: `clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet IFNAME | IFNAME]`

Назначение: Удаляет mrouter-порт в указанном vlan.

Параметры: `<1-4094>`: номер vlan; `ethernet IFNAME`: имя порта ethernet.

Режим конфигурирования: Привилегированный режим.

Описание: Используйте команду `show ipv6 mld snooping mrouter-port` для контроля удаления информации о mrouter.

Пример: Удалить mrouter-порт в vlan 1.

```
Switch#clear ipv6 mld snooping vlan 1 mrouter-port
```

15.2.3 debug mld snooping {all | packet | event | timer | mfc}

Синтаксис: `debug mld snooping {all | packet | event | timer | mfc}`

`no debug mld snooping {all | packet | event | timer | mfc}`

Назначение: Позволяет включить на коммутаторе режим отладки протокола MLD Snooping. Отмена команды `no debug mld snooping {all | packet | event | timer | mfc}` выключает режим отладки протокола MLD Snooping.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Режим отладки протокола MLD Snooping не включен.

Описание: Команда используется для включения режима отладки протокола MLD Snooping. В режиме отладки на дисплей выводится информация о различных MLD-пакетах, обработанных коммутатором: `event` (сообщения о событиях), `timer` (сообщения о таймерах), `mfc` (сообщения аппаратного уровня), `all` (все сообщения).

15.2.4 ipv6 mld snooping

Синтаксис: `ipv6 mld snooping`

`no ipv6 mld snooping`

Назначение: Включает функцию MLD Snooping. Отмена команды `no ipv6 mld snooping` выключает функцию MLD Snooping.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: функция MLD Snooping выключена.

Описание: Позволяет включить в глобальном режиме конфигурирования функцию MLD Snooping.

Пример: Включить функцию MLD Snooping в глобальном режиме конфигурирования.

```
Switch (config)#ipv6 mld snooping
```

15.2.5 ipv6 mld snooping vlan

Синтаксис: `ipv6 mld snooping vlan <vlan-id>`

`no ipv6 mld snooping vlan <vlan-id>`

Назначение: Включает MLD Snooping в указанной VLAN. Отмена команды `no ipv6 mld snooping vlan <vlan-id>` выключает MLD Snooping в указанной VLAN.

Параметры: `<vlan-id>`: идентификатор VLAN, в пределах <1-4094>.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: функция MLD Snooping в VLAN выключена.

Описание: Для того, чтобы настроить MLD Snooping на указанной vlan, необходимо сначала включить MLD Snooping в глобальном режиме конфигурирования.

Пример: Включить MLD snooping в VLAN 100 в глобальном режиме конфигурирования.

```
Switch (config)#ipv6 mld snooping vlan 100
```

15.2.6 ipv6 mld snooping vlan immediate-leave

Синтаксис: `ipv6 mld snooping vlan <vlan-id> immediate-leave`

`no ipv6 mld snooping vlan <vlan-id> immediate-leave`

Назначение: Включает функцию быстрого выхода протокола MLD для указанной vlan. Отмена команды `no ipv6 mld snooping vlan <vlan-id> immediate-leave` выключает функцию временного выхода протокола MLD.

Параметры: `<vlan-id>`: идентификатор VLAN, в пределах <1-4094>.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Функция быстрого выхода протокола MLD выключена.

Описание: Команда включения функции быстрого выхода протокола MLD ускоряет процесс освобождения порта multicast – группой, при этом указанной группе запрос не посылается, а просто непосредственно удаляется порт.

Пример: Включить для VLAN 100 функцию быстрого выхода протокола MLD.

```
Switch (config)#ipv6 mld snooping vlan 100 immediate-leave
```

15.2.7 ipv6 mld snooping vlan I2-general-querier

Синтаксис: `ipv6 mld snooping vlan < vlan-id > I2-general-querier`

`no ipv6 mld snooping vlan < vlan-id > I2-general-querier`

Назначение: Устанавливает указанный vlan, как маршрутизатор уровня 2.

Параметры: `vlan-id`: идентификатор VLAN, в пределах <1-4094>.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Vlan не является маршрутизатором уровня 2 для протокола MLD Snooping.

Описание: Рекомендуется конфигурировать маршрутизатор уровня 2 на сегменте. Если до ввода этой команды MLD snooping не включен для этой VLAN, то описываемая команда выполнена не будет. После выключения функции маршрутизатора уровня 2 протокол MLD вместе с ней выключен не будет. Основная задача этой команды – формирование периодических запросов, помогающих коммутатору сегмента обучить порт mrouter.

Примечание: При MLD Snooping имеется три способа обучения порта mrouter:

1. Порт принимает сообщения с запросами MLD.
2. Порт принимает пакеты multicast-протокола и поддерживает PIM.
3. С помощью статически сконфигурированного порта.

Пример: Использовать VLAN 100 как маршрутизатор уровня 2.

```
Switch (config)# ipv6 mld snooping vlan 100 I2-general-querier
```

15.2.8 ipv6 mld snooping vlan limit

Синтаксис: `ipv6 mld snooping vlan <vlan-id> limit {group <g_limit> | source <s_limit>}`

`no ipv6 mld snooping vlan <vlan-id> limit`

Назначение: Позволяет задать максимальное число групп MLD snooping, в которые может вступить хост, и максимальное число источников, которые может иметь группа.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

g_limit: <1-65535>, максимальное число групп, в которые может вступить хост.

s_limit: <1-65535>, максимальное число источников в группе, состоящих из источников внутри группы и внешних источников группы.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Не более 50 групп, в каждой группе может быть не более 40 источников.

Описание: Когда число вступивших в группу достигнет заданного предельного значения, новые запросы на вступление в группу будут отвергаться – это необходимо для предотвращения сетевых атак. Для того, чтобы эту команду можно было использовать, MLD snooping должен быть включен на vlan. При вводе отрицательной формы команды (с “no”), будут восстановлены настройки по умолчанию, при этом они отличаются от настройки “no limit” (число вступающих в группу не ограничено). По соображениям безопасности в этой команде не следует использовать опцию “no limit”. Если включен протокол MLD уровня 3, рекомендуется использовать настройку по умолчанию, при этом она, насколько возможно, должна соответствовать конфигурации протокола MLD.

Пример:

```
Switch(config)#ipv6 mld snooping vlan 2 limit group 300
```

15.2.9 ipv6 mld snooping vlan mrouter-port interface

Синтаксис: `ipv6 mld snooping vlan <vlan-id> mrouter-port interface [<ethernet>|<port-channel>] <ifname>`

`no ipv6 mld snooping vlan <vlan-id> mrouter-port interface [<ethernet>|<port-channel>] <ifname>`

Назначение: Позволяет задать статический порт mrouter для VLAN. Отмена команды `no ipv6 mld snooping vlan <vlan-id> mrouter-port interface [<ethernet>|<port-channel>] <ifname>` отменяет эту настройку.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

Ehernet: Имя Ethernet-порта.

Ifname: Имя интерфейса.

port-channel: Агрегированный порт.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Если в порту одновременно имеется и статический, и динамический порт mrouter, предпочтительнее использовать статический mrouter.

Пример:

```
Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet0/0/13
```

15.2.10 ipv6 mld snooping vlan mrpt

Синтаксис: `ipv6 mld snooping vlan <vlan-id> mrpt <value>`

`no ipv6 mld snooping vlan <vlan-id> mrpt`

Назначение: Позволяет задать срок жизни порта mrouter.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: срок жизни порта mrouter, в пределах <1-65535> секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 255 секунд.

Описание: Эта команда может быть применена к динамическому порту mrouter, но не к статическому. Для того, чтобы эту команду можно было использовать, на vlan должен быть включен протокол MLD snooping.

Пример:

```
Switch(config)#ipv6 mld snooping vlan 2 mrpt 100
```

15.2.11 ipv6 mld snooping vlan query-interval

Синтаксис: `ipv6 mld snooping vlan <vlan-id> query-interval <value>`

`no ipv6 mld snooping vlan <vlan-id> query-interval`

Назначение: Позволяет задать интервал отправки запросов.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: интервал отправки запросов, в пределах <1-65535> секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 125 секунд.

Описание: Если включен протокол MLD уровня 3, рекомендуется использовать настройку по умолчанию, при этом она, насколько возможно, должна соответствовать конфигурации протокола MLD.

Пример:

```
Switch(config)#ipv6 mld snooping vlan 2 query-interval 130
```

15.2.12 ipv6 mld snooping vlan query-mrsp

Синтаксис: `ipv6 mld snooping vlan <vlan-id> query-mrsp <value>`

`no ipv6 mld snooping vlan <vlan-id> query-mrsp`

Назначение: Позволяет настроить максимальный интервал времени ожидания ответа. Отмена команды `no ipv6 mld snooping vlan <vlan-id> query-mrsp` восстанавливает настройки, используемые по умолчанию.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: Значение максимального интервала времени ожидания ответа, пределах <1-25> секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 10 секунд.

Описание: Если включен протокол MLD уровня 3, рекомендуется использовать настройку по умолчанию, при этом она, насколько возможно, должна соответствовать конфигурации протокола MLD.

Пример:

```
Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18
```

15.2.13 ipv6 mld snooping vlan query-robustness

Синтаксис: `ipv6 mld snooping vlan <vlan-id> query-robustness <value>`

`no ipv6 mld snooping vlan <vlan-id> query-robustness`

Назначение: Позволяет задать надежность (robustness). Отмена команды `no ipv6 mld snooping vlan <vlan-id> query-robustness` восстанавливает настройки, используемые по умолчанию.

Параметры: **vlan-id:** Номер VLAN, в пределах <1-4094>.

value: Значение надежности, пределах <2-10>.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 2.

Описание: Если включен протокол MLD уровня 3, рекомендуется использовать настройку по умолчанию, при этом она, насколько возможно, должна соответствовать конфигурации протокола MLD.

Пример:

```
Switch(config)#ipv6 mld snooping vlan 2 query-robustness 3
```

15.2.14 ipv6 mld snooping vlan static-group

Синтаксис: `ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source < X:X::X:X>] interface [ethernet | port-channel] <IFNAME>`

no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source < X:X::X:X>] interface [ethernet | port-channel] <IFNAME>

Назначение: Позволяет задать в указанном порту VLAN статическую группу. Отмена команды `no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source < X:X::X:X>] interface [ethernet | port-channel] <IFNAME>` отменяет сделанные настройки.

Параметры: `vlan-id`: Номер VLAN, в пределах <1-4094>.

`X:X::X:X`: Адрес группы или источника.

`ethernet`: Имя Ethernet-порта.

`port-channel`: Агрегация порта.

`ifname`: Имя интерфейса.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Нет.

Описание: Когда группа является статической (но одновременно с этим – и динамической), с ней следует обращаться как со статической группой. Удалить статическую группу можно только с помощью ввода отрицательной формы этой команды (с `no`).

Пример:

```
Switch(config)#ip igmp snooping vlan 1 static-group ffile::15 source 2000::1  
interface ethernet 0/0/1
```

15.2.15 ipv6 mld snooping vlan suppression-query-time

Синтаксис: `ipv6 mld snooping vlan <vlan-id> suppression-query-time <value>`

no ipv6 mld snooping vlan <vlan-id> suppression-query-time

Назначение: Позволяет задать время подавления запроса. Отмена команды `no ipv6 mld snooping vlan <vlan-id> suppression-query-time` восстанавливает настройки, используемые по умолчанию.

Параметры: `vlan-id`: Номер VLAN, в пределах <1-4094>.

`value`: Значение времени подавления запроса, в пределах <1-65535> секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 255 секунд.

Описание: Эта команда может быть выдана только для маршрутизатора уровня 2. Время подавления запроса определяет интервал времени, в течение которого будут подавляться принятые в сегменте запросы маршрутизатора уровня 3 протокола MLD. Для использования этой команды необходимо, чтобы интервалы запросов разных коммутаторов одного и того же сегмента сети совпадали. Рекомендуется использовать настройку, заданную по умолчанию.

Пример:

```
Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270
```

15.2.16 show ipv6 mld snooping

Синтаксис: show ipv6 mld snooping [vlan <vlan-id>]

Параметры: <vlan-id>: номер VLAN, для которой надо вывести на дисплей сообщения MLD Snooping.

Режим конфигурирования: Привилегированный режим.

Описание: Если номер VLAN не указан, будет показан номер того VLAN, для которого включен протокол MLD snooping в глобальном режиме конфигурирования и multicast-протокол уровня 3, а также на котором включен протокол MLD Snooping и сконфигурирован маршрутизатор уровня 2. Если номер VLAN указан, на дисплей будет выведена подробная информация протокола MLD Snooping для этого VLAN.

Пример:

Вывести на дисплей сводную информацию для протокола MLD snooping коммутатора.

```
Switch(config)#show ipv6 mld snooping
Global mld snooping status: Enabled
L3 multicasting: running
Mld snooping is turned on for vlan 1(querier) Mld snooping is turned on for
vlan 2
```

Информация, отображаемая на дисплее	Описание
Global mld snooping status	Включен или нет протокол MLD Snooping в глобальном режиме конфигурирования
L3 multicasting	Включен или нет multicast-протокол уровня 3
Mld snooping is turned on for vlan 1(querier)	На какой VLAN коммутатора включен протокол MLD Snooping, является ли VLAN маршрутизатором уровня 2.

Вывести на дисплей подробную информацию для протокола MLD snooping интерфейса vlan1.

```
Switch#show ipv6 mld snooping vlan 1
Mld snooping information for vlan 1
Mld snooping L2 general querier :Yes(COULD_QUERY)
Mld snooping query-interval :125(s)
Mld snooping max reponse time :10(s)
Mld snooping robustness :2
Mld snooping mrouter port keep-alive time :255(s)
Mld snooping query-suppression time :255(s)
MLD Snooping Connect Group Membership Note: *-All Source, (S)- Include Source,
[S]-Exclude Source Groups Sources Ports Exptime System LevelFfile:::15
(2000::1) Ethernet1/8 00:04:14 V2
(2000::2) Ethernet1/8 00:04:14 V2
Mld snooping vlan 1 mrouter port Note: "!"-static mrouter port !Ethernet1/2
```

Информация, отображаемая на дисплее	Описание
Mld snooping L2 general querier	Включен или нет маршрутизатор уровня 2 на vlan. Состояние запросов маршрутизатора (подавлены или посылаются).
Mld snooping query-interval	Интервал отправки запросов в vlan
Mld snooping max reponse time	Максимальное время отклика для этого vlan
Mld snooping robustness	Надежность, заданная для vlan
Mld snooping mrouter port keep-alive time	Срок жизни динамического порта mrouter в этом vlan.
Mld snooping query-suppression time	Таймер vlan подавления запросов маршрутизатора уровня 2 (в состоянии подавления запросов).

MLD Snooping Connect Group Membership	Члены группы vlan, соответствие имен между портом и (S,G) .
Mld snooping vlan 1 mrouter port	Порт mrouter vlan (статический и динамический).

16 Команды для настройки групповой VLAN (multicast vlan)

16.1.1 multicast-vlan

Синтаксис: `multicast-vlan`

no multicast-vlan

Назначение: Включает на VLAN функцию групповой VLAN. Отмена команды **no multicast-vlan** выключает функцию групповой VLAN.

Параметры: Нет.

Режим конфигурирования: Режим настройки VLAN.

Значение по умолчанию: Функция групповой VLAN не включена.

Описание: Функция групповой VLAN не может быть включена для private VLAN. Для выключения на VLAN групповой функции VLAN, следует удалить ассоциативные связи между сетями VLAN пользователей и групповой VLAN. Имейте в виду, что с помощью этой команды не может быть сконфигурирована VLAN, назначаемая по умолчанию. На коммутаторе допускается только одна групповая VLAN.

Примеры:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)# multicast-vlan
```

16.1.2 multicast-vlan association

Синтаксис: `multicast-vlan association <vlan-list>`

no multicast-vlan association <vlan-list>

Назначение: Ассоциирует некоторые VLAN с групповой VLAN. Отмена команды **no multicast-vlan association <vlan-list>** отменяет ассоциированные связи.

Параметры: **<vlan-list>**: список идентификаторов VLAN ID, ассоциированных с групповой VLAN. Каждый VLAN может быть ассоциирован только с одним групповым VLAN, ассоциация будет успешной только в том случае, если VLAN, идентификатор которого (VLAN ID) указан в таблице, существует.

Режим конфигурирования: Режим настройки интерфейсов VLAN.

Значение по умолчанию: Группован VLAN не ассоциирован с каким-либо VLAN.

Описание: После того, как VLAN будет ассоциирован с групповым VLAN, если с порта этого VLAN приходит запрос на групповой трафик, групповые данные будут посылаться с групповой VLAN на этот порт, в результате трафик данных снизится. VLAN, ассоциированный с групповым VLAN, не должна быть private VLAN. После того, как включен групповой VLAN, обычный VLAN, кроме группового, может ассоциироваться только с другим обычным VLAN.

Примеры:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)# multicast-vlan association 3, 4
```

17 Команды для настройки списков доступа (ACL)

17.1.1 absolute-periodic/periodic

Синтаксис: [no] absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <start_time> to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <end_time>

[no] periodic {{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily|weekdays | weekend} <start_time> to <end_time>

Назначение: Позволяет задать временной диапазон действия различных команд на протяжении недели. Этот диапазон будет поддерживаться для каждой недели.

Параметры:

Monday	(Понедельник)
Tuesday	(Вторник)
Wednesday	(Среда)
Thursday	(Четверг)
Friday	(Пятница)
Saturday	(Суббота)
Sunday	(Воскресенье)

daily: (Ежедневно)

weekdays: (С понедельника по пятницу)

weekend: (В субботу и воскресенье)

start_time: время начала, ЧЧ:ММ:СС (часы: минуты: секунды)

end_time: время окончания, ЧЧ:ММ:СС (часы: минуты: секунды)

Примечание: Таймер временного диапазона имеет минутный отсчет, поэтому временные ошибки должны быть <= одной минуты.

Режим конфигурирования: режим настройки временного диапазона

Значение по умолчанию: Временной диапазон не задан.

Описание: Временной диапазон позволяет ввести периодическое выполнение команд по времени и дате. Команда позволяет задать определенный период времени выполнения команд, еженедельно для всех дней недели – с понедельника по субботу, а также в воскресенье.

С день1 чч:мм:сс по день2 чч:мм:сс или {[день1+день2+день3+день4+день5+день6+день7] | все выходные дни | выходные дни отдельно | ежедневно} чч:мм:сс дочч:мм:сс.

Примеры: Обеспечить действие настроек в период с 9:15:30 до 12:30:00 со Вторника по Субботу.

```
Switch(config)#time-range dc_timer
Switch(Config-Time-Range-dc_timer)#absolute-periodic Tuesday 9:15:30 to
Saturday
```

Обеспечить действие настроек в период с 14:30:00 по 16:45:00 в понедельник, среду, пятницу и воскресенье.

```
Switch(Config-Time-Range-dc_timer)#periodic Monday Wednesday Friday Sunday
14:30:00 to 16:45:00
```

17.1.2 absolute start

Синтаксис: [no] absolute start <start_time> <start_data> [end <end_time> <end_data>]

Назначение: Позволяет задать абсолютный временной диапазон по часам, встроенным в оборудование.

Параметры: **start_time:** Время начала, ЧЧ:ММ:СС (часы: минуты: секунды)

end_time: время окончания, ЧЧ:ММ:СС (часы: минуты: секунды)

start_data: Дата начала, формат: ГГГГ.ММ.ДД (год.месяц.день)

end_data: Дата окончания, формат: ГГГГ.ММ.ДД (год.месяц.день)

Примечание: Таймер временного диапазона имеет минутный отсчет, поэтому временные ошибки должны быть <= одной минуты.

Режим конфигурирования: Режим настройки временного диапазона

Значение по умолчанию: Временной диапазон не задан.

Описание: Если команда вводится несколько раз, абсолютное время и дата, соответствующие определенному году, месяцу, дню, часу и минуте начала временного диапазона не должны совпадать с ранее введенными датами и временем, в противном случае будут выполнены настройки, введенные последними.

Примеры: Обеспечить действие настроек с 6:00:00 по 13:30:00 с 1 октября 2004 года по 26 января 2005 года.

```
Switch(config)#Time-range zes_timer
```

```
Switch(Config-Time-Range-zes_timer)#absolute start 6:00:00 2004.10.1 end  
13:30:00 2005.1.26
```

17.1.3 access-list (ip extended)

Синтаксис: access-list <num> {deny | permit} icmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

access-list <num> {deny | permit} igmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

access-list <num> {deny | permit} tcp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } [s-port <sPort>] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [d-port <dPort>] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <prec>] [tos <tos>] [time-range <time-range-name>]

access-list <num> {deny | permit} udp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } [s-port <sPort>] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [d-port <dPort>] [precedence <prec>] [tos <tos>] [time-range <time-range-name>]

access-list <num> {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num> } {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [precedence <prec>] [tos <tos>] [time-range <time-range-name>]

no access-list <num>

Назначение: Позволяет создать нумерованное расширенное (extended) правило доступа для согласования с конкретным IP-протоколом, либо со всеми IP-протоколами. Если список доступа с таким номером не существует, то он будет создан.

Параметры: <num>: номер списка доступа, 100-299;

<protocol>: номер ip-протокола верхнего уровня, 0-255;

<slpAddr>: IP-адрес источника;

<sMask>: обратная маска IP-адреса источника;

<dIpAddr> : IP-адрес назначения;

<dMask>: обратная маска IP-адреса назначения, принимать во внимание - позиция 0, игнорировать - позиция 1;

<igmp-type>: тип igmp, 0-15;

<icmp-type>: тип icmp, 0-255;

<icmp-code>: номер протокола icmp, 0-255;

<prec>: приоритет IP, 0-7;

<tos>: тип обслуживания, 0-15;
<sPort>, номер порта источника, 0-65535;
<dPort>, номер порта назначения, 0-65535;
<time-range-name>: имя временного диапазона.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Списки доступа не настроены.

Описание: Когда пользователь в первый раз присваивает конкретный номер <num>, создается серийный номер списка, затем правила добавляются в этот ACL. Для списков доступа с номерами 200-299 могут быть заданы обратные маски IP-адресов, не являющиеся постоянными. <igmp-type> указывает тип пакета IGMP, характерные значения этого параметра: 17(0x11): IGMP QUERY packet 18(0x12): IGMP V1 REPORT packet 22(0x16): IGMP V2 REPORT packet 23(0x17): IGMP V2 LEAVE packet 34(0x22): IGMP V3 REPORT packet 19(0x13): DVMR packet 20(0x14): PIM V1 packet

Важные примечания: Приведенные типы пакетов могут содержать поля IP OPTION. Обычно IGMP-пакет содержит поля OPTION, однако в описываемой настройке эти поля использовать нельзя. Если необходимо настроить пакеты, содержащие поля OPTION, используйте те из них, для которых задана опция OFFSET.

Примеры: Создать нумерованный расширенный список доступа с серийным номером 110. Запретить прохождение пакетов icmp, разрешить прохождение пакетов udp с адресом назначения 192.168.0.1 и портом назначения 32.

```
Switch(config)#access-list 110 deny icmp any any-destination
Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-
port 32
```

17.1.4 access-list (ip standard)

Синтаксис: access-list <num> {deny | permit} {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}}

no access-list <num>

Назначение: Позволяет создать стандартный нумерованный список доступа для IP-адресов. Если список доступа существует, к нему будет добавлен список правил. Отмена команды no access-list <num> удаляет стандартный нумерованный список доступа для IP-адресов.

Параметры: <num>: номер списка доступа, 100-199;

<slpAddr>: IP-адрес источника;

<sMask> : обратная маска IP-адреса источника.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Списки доступа не настроены.

Описание: Когда пользователь в первый раз присваивает конкретный номер <num>, создается серийный номер списка, затем правила добавляются в этот ACL.

Примеры: Создать стандартный нумерованный список доступа для IP-адресов с серийным номером 20. Разрешить прохождение пакетов данных с адресом источника 10.1.1.0/24, запретить прохождение пакетов с адресом источника 10.1.1.0/16.

```
Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255
Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255
```

17.1.5 access-list (mac extended)

Синтаксис: access-list <num> {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [untagged-eth2|tagged-eth2| untagged-802-3 | tagged-802-3]

no access-list <num>

Назначение: Позволяет задать расширенное (extended) нумерованное правило ACL для MAC-адресов. Отмена команды **no access-list <num>** удаляет стандартное нумерованное правило ACL для MAC-адресов.

Параметры: **<num>**: номер списка доступа (десятичный), в пределах 1100-1199;

<deny>: если согласование с правилом достигнуто, то запретить доступ;

<permit>: если согласование с правилом достигнуто, то разрешить доступ;

<any-source-mac>: для любого адреса источника;

<any-destination-mac>: для любого адреса назначения;

<host_smac>, **<smac>**: MAC-адрес источника;

<smac-mask>: маска (обратная маска) MAC-адреса источника;

<host_dmac>, **<dmac>**: MAC-адрес назначения;

<dmac-mask>: маска (обратная маска) MAC-адреса назначения;

untagged-eth2: формат нетегированных пакетов Ethernet II;

tagged-eth2: формат тегированных пакетов Ethernet II;

untagged-802-3: формат нетегированных пакетов 802.3;

tagged-802-3: формат тегированных пакетов 802.3.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Список доступа не сконфигурирован.

Описание: Когда пользователь в первый раз присваивает конкретный номер <num>, создается серийный номер списка, затем правила добавляются в этот ACL.

Примеры: Разрешить прохождение кадров tagged-eth2 от источников с любыми MAC-адресами и любыми MAC-адресами назначения.

```
Switch(config)#access-list 1100 permit any-source-mac any-destination-mac
tagged-eth2
```

17.1.6 access-list (mac-ip extended)

Синтаксис: `access-list <num> {deny | permit} {any-source-mac | {host-source-mac<host_smac>} | {<smac><smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac><dmac-mask>}} icmp {{<source> <source-wildcard>} | any-source | {host-source<source-host-ip>}} {{<destination> <destination-wildcard>} | any-destination | {host-destination<destination-host-ip>}} [<icmp-type>] [<icmp-code>] [precedence <precedence>] [tos <tos>] [time-range <time-range-name>]`

`access-list <num> {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac><smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac><dmac-mask>}} igmp {{<source> <source-wildcard>} | any-source | {host-source <source-host-ip>}} {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>] [time-range <time-range-name>]`

`access-list <num> {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} tcp {{<source> <source-wildcard>} | any-source | {host-source <source-host-ip>}} [s-port <port1>] {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [d-port <port3>] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>] [time-range <time-range-name>]`

`access-list <num> {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} udp {{<source> <source-wildcard>} | any-source | {host-source <source-host-ip>}} [s-port <port1>] {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [d-port <port3>] [precedence <precedence>] [tos <tos>] [time-range <time-range-name>]`

```
access-list <num> {deny | permit} {any-source-mac | {host-source-mac <host_smac>} |
{<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac>
<dmac-mask>}} {eigrp | gre | igmp | ip | ipinip | ospf | {<protocol-num>}} {{<source> <source-
wildcard>} | any-source | {host-source <source-host-ip>}} {{<destination> <destination-wildcard>}
| any-destination | {host-destination <destination-host-ip>}} [precedence <precedence>] [tos
<tos>] [time-range <time-range-name>]
```

Назначение: Позволяет задать нумерованное расширенное правило списка доступа MAC-IP ACL. Отмена команды (с 'no') удаляет одно расширенное нумерованное правило списка доступа MAC-IP ACL.

Параметры: **num:** серийный номер списка доступа (десятичный), в пределах 3100-3299;

deny: если согласование с правилом достигнуто, то запретить доступ;

permit: если согласование с правилом достигнуто, то разрешить доступ;

any-source-mac: любой MAC-адрес источника;

any-destination-mac: любой MAC-адрес назначения;

host_smac, smac: MAC-адрес источника;

smac-mask: маска (обратная маска) MAC-адреса источника;

host_dmac, dmas : MAC-адрес назначения;

dmac-mask: маска (обратная маска) MAC-адреса назначения;

protocol: номер протокола, имя протокола или IP-протокол. Может быть одним из ключевых слов: eigrp, gre, icmp, igmp, igmp, ip, ipinip, ospf, tcp или udp, либо целым числом в пределах 0-255, являющимся номером IP-протокола. Для согласования со всеми Интернет-протоколами (включая ICMP, TCP и UDP) используйте суффикс 'ip'.

source-host-ip: IP-адрес источника, сети-источника или хоста-источника доставляемого пакета. 32-битные числа, представленные в десятичном формате с точками;

host-source: означает, что IP-адрес является адресом хоста источника, в противном случае IP-адрес будет считаться адресом сети;

source-wildcard: IP-адрес в обратном порядке. 32-битные числа, представленные в десятичном формате с 4 точками-разделителями, обратная маска;

destination-host-ip, номер назначения сети назначения, либо хоста, на который доставляются пакеты. 32-битные числа, представленные в десятичном формате с точками;

host: означает, что адрес является адресом хоста назначения, в противном случае считается IP-адресом сети;

destination-wildcard: маска назначения. 32-битные числа, представленные в десятичном формате с 4 точками-разделителями, обратная маска;

s-port (опция): означает необходимость согласования с портом источником при TCP/UDP;

port1 (опция): номер интерфейса источника при TCP/UDP, целое число в пределах 0-65535;

d-port (опция): Означает необходимость согласования с интерфейсом назначения при TCP/UDP;

port3 (опция): Номер интерфейса назначения при TCP/UDP, целое число в пределах 0 — 65535;

[ack] [fin] [psh] [rst] [urg] [syn] (опции): только для протокола TCP, порядок следования тегов не важен. Флаги поля flags заголовка TCP;

precedence (опция): пакеты могут фильтроваться по приоритетам (целое число в пределах 0-7);

tos (опция): пакеты могут фильтроваться по типу обслуживания (целое число в пределах 0-15);

icmp-type (опция): ICMP-пакеты могут фильтроваться по типу пакета (целое число в пределах 0-255);

icmp-code (опция): ICMP-пакеты могут фильтроваться по коду пакета (целое число в пределах 0-255);

igmp-type (опция): IGMP-пакеты могут фильтроваться по имени IGMP-пакета или по типу пакета (целое число в пределах 0-255);

<time-range-name>: имя временного диапазона.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Список доступа не сконфигурирован.

Описание: Когда пользователь в первый раз присваивает конкретный номер <num>, создается серийный номер списка, затем правила добавляются в этот ACL. Для списков доступа с номерами 3200-3299 могут быть заданы обратные маски IP-адресов, не являющиеся постоянными.

Пример: Разрешить прохождение TCP-пакетов с MAC-адресом источника 00-12-34-45-XX-XX, с любым MAC-адресом назначения, IP-адресом источника 100.1.1.0 0.255.255.255, портом источника 100 и интерфейсом назначения 40000.

```
Switch(config)#access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF
any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination d-
port 40000
```

17.1.7 access-list (mac standard)

Синтаксис: `access-list <num> {deny | permit} {any-source-mac | {host-source-mac <host_smac> } | {<smac> <smac-mask> } }`

no access-list <num>

Назначение: Позволяет задать стандартное нумерованное правило ACL для MAC-адресов. Отмена команды **no access-list <num>** удаляет стандартное нумерованное правило ACL для MAC-адресов.

Параметры: **<num>**: номер списка доступа (десятичный), в пределах 700-799;

deny: если согласование с правилом достигнуто, то запретить доступ;

permit: если согласование с правилом достигнуто, то разрешить доступ;

<host_smac>, **<sumac>** : MAC-адрес источника;

<sumac-mask>: маска (обратная маска) MAC-адреса источника

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Список доступа не задан.

Описание: Когда пользователь в первый раз присваивает конкретный номер <num>, создается серийный номер списка, затем правила добавляются в этот ACL.

Пример: Настроить коммутатор таким образом, чтобы осуществлялась передача пакетов от 00-00-xx-xx-00-01 и была запрещена передача пакетов от 00-00-00-xx-00-ab.

```
Switch(config)#access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00
Switch(config)#access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00
```

17.1.8 clear access-group statistic

Синтаксис: `clear access-group statistic [ethernet <interface-name>]`

Назначение: Очищает статистику пакетов на указанном интерфейсе.

Параметры: **<interface-name>**: имя интерфейса.

Режим конфигурирования: Привилегированный режим

Значение по умолчанию: Нет.

Пример: Очистить статистику пакетов на интерфейсе.

```
Switch#clear access-group statistic
```

17.1.9 firewall

Синтаксис: `firewall {enable | disable}`

Назначение: Включает или выключает межсетевой экран.

Параметры: **enable:** включить межсетевой экран;

disable: выключить межсетевой экран.

Значение по умолчанию: Межсетевой экран не используется.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Правила доступа могут быть заданы и при включенном, и при выключенном межсетевом экране. Однако только когда межсетевой экран включен, правила могут быть использованы для конкретного порта и направления передачи в нем. Когда межсетевой экран выключен, все списки доступа ACL, привязанные к портам, удалены.

Примеры: Включить межсетевой экран.

```
Switch(config)#firewall enable
```

17.1.10 firewall default

Синтаксис: **firewall default {permit | deny [ipv4 | ipv6 | all]}**

Назначение: Позволяет настроить операции межсетевого экрана, выполняемые по умолчанию.

Параметры: **permit:** разрешить прохождение пакетов данных;

deny [ipv4 | ipv6 | all] позволяет запретить прохождение пакетов ipv4 или ipv6-данных, либо всех пакетов данных. Если задано значение по умолчанию deny, то ранее использовавшееся значение permit будет отменено.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Permit (Разрешить).

Описание: Эта команда влияет только на IP-пакеты, входящие через порт, в других ситуациях через коммутатор могут проходить все пакеты.

Примеры: Настроить операцию, выполняемую межсетевым экраном по умолчанию – разрешить прохождение пакетов.

```
Switch(config)#firewall default permit
```

17.1.11 ip access extended

Синтаксис: **ip access extended <name>**

no ip access extended <name>

Назначение: Позволяет создать расширенный список доступа для IP-адресов и присвоить ему имя. Отмена команды **no ip access extended <name>** удаляет расширенный список доступа вместе со всем его содержимым.

Параметры: **<name>:** имя списка доступа. **<name>** — строка, содержащая 1 — 32 символа (но не числовой строкой).

Режим конфигурирования: Глобальный режим конфигурирования

Значение по умолчанию: Список доступа не задан.

Описание: Когда эта команда вводится впервые, создается пустой список доступа.

Пример: Создать расширенный список доступа для IP-адресов с именем tcpFlow.

```
Switch(config)#ip access-list extended tcpFlow
```

17.1.12 ip access standard

Синтаксис: **ip access standard <name>**

no ip access standard <name>

Назначение: Позволяет создать стандартный список доступа для IP-адресов и присвоить ему имя. Отмена команды **no ip access standard <name>** удаляет список доступа вместе со всем его содержимым.

Параметры: <name>: имя списка доступа. <name> — строка, содержащая 1 — 32 символа (но не числовой строкой).

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Список доступа не задан.

Описание: Когда эта команда вводится впервые, создается пустой список доступа.

Пример: Создать стандартный список доступа для IP-адресов с именем ipFlow.

```
Switch(config)#ip access-list standard ipFlow
```

17.1.13 ipv6 access-list

Синтаксис: `ipv6 access-list <num-std> {deny | permit} {<slPv6Prefix/sPrefixlen> | any-source | {host-source <slPv6Addr>}}`

`ipv6 access-list <num-ext> {deny | permit} icmp {{ <slPv6Prefix/sPrefixlen> } | any-source | {host-source <slPv6Addr> }} { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]`

`ipv6 access-list <num-ext> {deny | permit} tcp {{<slPv6Prefix/<sPrefixlen>} | any-source | {host-source <slPv6Addr>}} [s-port <sPort>] {{<dIPv6Prefix/<dPrefixlen>} | any-destination | {host-destination <dIPv6Addr>}} [dPort <dPort>] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <flowlabel>][time-range <time-range-name>]`

`ipv6 access-list <num-ext> {deny | permit} udp {{<slPv6Prefix/<sPrefixlen>} | any-source | {host-source <slPv6Addr>}} [s-port <sPort>] {{<dIPv6Prefix/<dPrefixlen>} | any-destination | {host-destination <dIPv6Addr>}} [dPort <dPort>] [dscp <dscp>] [flow-label <flowlabel>][time-range <time-range-name>]`

`ipv6 access-list <num-ext> {deny | permit} <next-header> {<slPv6Prefix/sPrefixlen> | any-source | {host-source <slPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]`

`no ipv6 access-list {<num-std> | <num-ext>}`

Назначение: Позволяет создать стандартный нумерованный список доступа для IP-адресов. Если список доступа уже существует, в него будет добавлено правило. Отмена команды `no access-list {<num-std>|<num-ext>}` удаляет стандартный нумерованный список доступа для IP-адресов.

Параметры: <num-std>: номер списка доступа, в пределах от 500 до 599;

<num-ext>: номер списка доступа, в пределах от 600 до 699;

<slPv6Prefix>: префикс ipv6-адреса источника;

<sPrefixlen>: длина префикса ipv6-адреса источника, в пределах от 1 до 128;

<slPv6Addr>: ipv6-адрес источника;

<dIPv6Prefix>: префикс ipv6-адреса назначения;

<dPrefixlen>: длина префикса ipv6-адреса назначения, в пределах от 1 до 128;

<dIPv6Addr>: ipv6-адрес назначения;

<icmp-type>: тип icmp, 0-255;

<icmp-code>: код протокола icmp;

<dscp>: приоритет IPv6, в пределах от 0 до 63.

<flowlabel>: значение тега потока, в пределах от 0 до 1048575;

syn, ack, urg, rst, fin, psh, tcp: положение метки;

<sPort>: номер порта источника, 0-65535;

<dPort>: номер порта назначения, 0-65535;

<next-header>: следующий заголовок IPv6, в пределах от 0 до 255;

<time-range-name>: имя временного диапазона.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Список доступа не задан.

Описание: Команда позволяет создать стандартный список доступа по IPv6-адресам. При последующих настройках, новые правила будут добавляться к уже существующим.

Примеры: Создать нумерованный стандартный список доступа 520, разрешающий пакетам от назначения 2003:1:2:3::1/64 проходить через сеть и запрещающий проходить через нее пакетам от источника с адресом 2003:1:2::1/48.

```
Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64
Switch (config)#ipv6 access-list 520 deny 2003:1:2::1/48
```

17.1.14 ipv6 access-list standard

Синтаксис: `ipv6 access-list standard <name>`

no ipv6 access-list standard <name>

Назначение: Позволяет создать стандартный список доступа для IPv6-адресов на основе имен. Отмена команды **no ipv6 access-list standard<name>** удаляет стандартный список доступа для IPv6-адресов на основе имен (удаляет все его элементы).

Параметры: **<name>**: имя списка доступа, символьная строка длиной от 1 до 32 символов.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Список доступа не задан.

Описание: Когда эта команда вводится впервые, создается пустой список доступа.

Пример: Создать стандартный список доступа для IPv6-адресов с именем "ip6Flow".
`Switch(config)#ipv6 access-list standard ip6Flow`

17.1.15 ipv6 access-list extended

Синтаксис: `ipv6 access-list extended <name>`

no ipv6 access-list extended <name>

Назначение: Позволяет создать расширенный список доступа для IPv6-адресов на основе имен. Отмена команды **no ipv6 access-list extended<name>** удаляет список доступа вместе со всем его содержимым.

Параметры: **<name>**: имя списка доступа, символьная строка длиной от 1 до 32 символов.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: IP-адрес не задан.

Описание: Когда эта команда вводится впервые, создается пустой список доступа.

Пример: Создать расширенный список доступа для IPv6-адресов с именем "tcpFlow".
`Switch (config)#ipv6 access-list extended tcpFlow`

17.1.16 {ip | ipv6 | mac | mac-ip} access-group

Синтаксис: `{ip | ipv6 | mac | mac-ip} access-group <name> {in} [traffic-statistic]`

no {ip | mac} access-group <name> {in}

Назначение: Позволяет применить список доступа для требуемого направления передачи порта, имеет опцию, по которой в правило ACL может быть добавлен счетчик статистики. Отмена команды **no {ip | mac} access-group <name> {in}** удаляет список доступа, привязанный к порту.

Параметры: **<name>**: имя списка доступа, символьная строка длиной от 1 до 32 символов.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: К входу порта списки доступа не привязаны.

Описание: К входу порта может быть привязано правило доступа.

Всего имеется четыре вида полей заголовка пакетов: MAC ACL, IP ACL. В некоторых случаях режим ACL-фильтрации (по операциям permit и deny) приводит к конфликтам (так как

пакеты могут согласовываться с несколькими типами данных в восьми ACL). В каждом списке ACL точные приоритеты задаются на основе результирующей достоверности. Когда фильтрация приводит к конфликту, можно задать финальный режим работы фильтра на основе приоритетов.

При привязке ACL к порту имеются некоторые ограничения:

К каждому порту может быть привязан MAC-IP ACL, IP ACL, IPv6 ACL и MAC ACL.

При привязке к порту двух ACL, когда пакетные данные согласуются с несколькими ACL одновременно, приоритеты списков ACL образуют следующую последовательность (от высшего приоритета к низшему): IPv6 ACL, MAC-IP ACL, MAC ACL, IP ACL (все для входящих пакетов).

Пример: Привязать список доступа AAA к входящему направлению порта.

```
Switch(Config-If-Ethernet0/0/5)#ip access-group aaa in
```

17.1.17 mac access extended

Синтаксис: `mac-access-list extended <name>`

`no mac-access-list extended <name>`

Назначение: Позволяет создать список доступа ACL с именем (для MAC-адресов), либо войти в режим настройки списков доступа. Отмена команды `no mac-access-list extended <name>` удаляет этот список доступа ACL.

Параметры: `<name>`: имя списка доступа, не должно содержать пробелов и кавычек, должно начинаться с буквы, длина имени не должна превышать 32 символов (одноименные заглавные и строчные буквы считаются разными символами).

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Списки доступа не сконфигурированы.

Описание: После первого выполнения этой команды создается список доступа с пустым именем, элементы списка отсутствуют.

Примеры: Создать MAC ACL с именем `mac_acl`.

```
Switch(config)# mac-access-list extended mac_acl
Switch(Config-Mac-Ext-Nacl-mac_acl)#
```

17.1.18 mac-ip access extended

Синтаксис: `mac-ip-access-list extended <name>`

`no mac-ip-access-list extended <name>`

Назначение: Позволяет создать список доступа ACL с именем (для MAC-IP-адресов), либо войти в режим настройки списков доступа. Отмена команды `no mac-ip-access-list extended <name>` удаляет этот список доступа ACL.

Параметры: `<name>`: имя списка доступа, не должно содержать пробелов и кавычек, должно начинаться с буквы, длина имени не должна превышать 32 символов (одноименные заглавные и строчные буквы считаются разными символами).

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Именованные списки доступа для MAC-IP-адресов отсутствуют.

Описание: Когда эта команда вводится впервые, создается пустой список доступа.

Примеры: Создать MAC-IP ACL с именем `mac_acl`.

```
Switch(config)# mac-ip-access-list extended macip_acl
Switch(Config-MacIp-Ext-Nacl-macip_acl)#
```

17.1.19 permit | deny (ip extended)

Синтаксис: `[no] {deny | permit} icmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>]`

```
[no] {deny | permit} igmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}}
{{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>]
[precedence <prec>] [tos <tos>][time-range<time-range-name>]
```

```
[no] {deny | permit} tcp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } }
[s-port <sPort> ] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [d-port
<dPort> ] [ack+fin+psh+rst+urg+syn] [precedence <prec> ] [tos <tos> ][time-range <time-range-
name> ]
```

```
[no] {deny | permit} udp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } }
[s-port <sPort> ] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [d-port
<dPort> ] [precedence <prec> ] [tos <tos> ][time-range <time-range-name> ]
```

```
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | < protocol-num >} {{<slpAddr>
<sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-
destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>]
```

Назначение: Позволяет создать имя расширенного правила доступа для IP-адресов для согласования с конкретным IP-протоколом или со всеми IP-протоколами.

Параметры: <slpAddr>: IP-адрес источника;

<sMask>: обратная маска IP-адреса источника;

<dIpAddr>: IP-адрес назначения;

<dMask>: обратная маска IP-адреса назначения, принимать во внимание - позиция 0, игнорировать - позиция 1;

<igmp-type>: тип igmp, 0-15;

<icmp-type>: тип icmp, 0-255;

<icmp-code>: номер протокола icmp, 0-255;

<prec>: приоритет IP, 0-7;

<tos>: тип обслуживания, 0-15;

<sPort>: номер порта источника, 0-65535;

<dPort>: номер порта назначения, 0-65535;

<time-range-name>: имя временного диапазона.

Режим конфигурирования: Режим настройки именованного расширенного списка доступа для IP-адресов.

Значение по умолчанию: Список доступа не задан.

Примеры: Создать расширенный список доступа. Запретить прохождение пакетов icmp, разрешить прохождение пакетов udp с адресом назначения 192.168.0.1 и портом назначения 32.

```
Switch(config)#access-list ip extended udpFlow
Switch(Config-IP-Ext-Nacl-udpFlow)#deny igmp any any-destination
Switch(Config-IP-Ext-Nacl-udpFlow)#permit udp any host-destination
192.168.0.1 d-port 32
```

17.1.20 permit | deny (ip standard)

Синтаксис: {deny | permit} {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}}

no {deny | permit} {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}}

Назначение: Позволяет создать стандартное именованное правило доступа для IP-адресов. Отмена команды no {deny | permit} {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} удаляет соответствующее правило доступа для IP-адресов.

Параметры: <slpAddr>: IP-адрес источника;

<sMask>: обратная маска IP-адреса источника;

Режим конфигурирования: Режим настройки именованного расширенного списка доступа для IP-адресов. Значение по умолчанию: Список доступа не задан.

Пример: Разрешить прохождение пакетов от источника с адресом 10.1.1.0/24, запретить прохождение пакетов от источника с адресом 10.1.1.0/16.

```
Switch(config)# access-list ip standard ipFlow
Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255
```

17.1.21 permit | deny (ipv6 extended)

Синтаксис: [no] {deny|permit} icmp {{<slIPv6Prefix/sPrefixlen> | any | {host<slIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination<dIPv6Addr>}} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <flowlabel>] [time-range <time-range-name>]

[no] {deny | permit} tcp {<slIPv6Prefix/sPrefixlen> | any-source | {host-source <slIPv6Addr>}} [s-port <sPort>] {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [d-port <dPort>] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <fl>] [time-range <time-range-name>]

[no] {deny | permit} udp {<slIPv6Prefix/sPrefixlen> | any-source | {host-source <slIPv6Addr>}} [s-port <sPort>] {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [d-port <dPort>] [dscp <dscp>] [flow-label <fl>] [time-range <time-range-name>]

[no] {deny | permit} <next-header> {<slIPv6Prefix/sPrefixlen> | any-source | {host-source <slIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range <time-range-name>]

[no] {deny | permit} {<slIPv6Prefix/sPrefixlen> | any-source | {host-source <slIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]

Назначение: Позволяет создать расширенный список доступа для IPv6-адресов для согласования с конкретным IPv6-протоколом.

Параметры: <slIPv6Addr>: ipv6-адрес источника;

<sPrefixlen>: длина префикса IPv6-адреса, в пределах от 1 до 128;

<dIPv6Addr>: ipv6-адрес назначения;

<dPrefixlen>: длина префикса IPv6-адреса, в пределах от 1 до 128;

<igmp-type>: тип IGMP;

<icmp-type>: тип icmp;

<icmp-code>: номер протокола icmp;

<dscp>: приоритет IPv6, в пределах от 0 до 63;

<flowlabel>: значение метки потока, в пределах от 0 до 1048575;

syn, ack, urg, rst, fin, psh, tcp: позиция метки;

<sPort>: номер порта источника, в пределах от 0 до 65535;

<dPort>: номер порта назначения, в пределах от 0 до 65535;

<next-header>: следующий заголовок IPv6.

<time-range-name>: имя временного диапазона.

Режим конфигурирования: Режим работы с именованными расширенными списками доступа.

Значение по умолчанию: Список доступа не задан.

Пример: Создать расширенный список доступа с именем udpFlow, запретить прохождение пакетов igmp и разрешить прохождение пакетов udp с адресом назначения 2001:1:2:3::1 и портом назначения 32.

```
Switch(config)#ipv6 access-list extended udpFlow
Switch(Config-IPv6-Ext-Nacl-udpFlow)#deny igmp any any-destination
Switch(Config-IPv6-Ext-Nacl-udpFlow)#permit udp any-source host-destination
2001:1:2:3::1 dPort 32
```

17.1.22 permit | deny (ipv6 standard)

Синтаксис: [no] {deny | permit} {{<slIPv6Prefix/sPrefixlen>} | any-source | {host-source <slIPv6Addr>}}

Назначение: Позволяет создать стандартное IPv6-правило управления доступом. Отмена команды `no {deny | permit} {{<slIPv6Prefix/sPrefixlen>} | any-source | {host-source <slIPv6Addr>}}` удаляет стандартное IPv6-правило управления доступом.

Параметры: <slIPv6Prefix>: префикс ipv6-адреса источника;

<sPrefixlen>: длина префикса IPv6-адреса, в пределах от 1 до 128;

<slIPv6Addr>: ipv6-адрес источника.

Режим конфигурирования: Режим настройки IPv6-списков доступа.

Значение по умолчанию: Список доступа не задан.

Пример: Разрешить прохождение пакетов от источника с адресом 2001:1:2:3::1/64, запретить прохождение пакетов от источника с адресом 2001:1:2:3::1/48.

```
Switch(config)#ipv6 access-list standard ipv6Flow
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48
```

17.1.23 permit | deny (mac extended)

Синтаксис: [no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype <protocol> [<protocol-mask>]]]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [ethertype <protocol> [<protocol-mask>]]]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [vlanId <vid-value> [<vid-mask>]] [ethertype <protocol> [<protocol-mask>]]]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [untagged-eth2 [ethertype <protocol> [<protocol-mask>]]]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [untagged-802-3]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [tagged-eth2 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype <protocol> [<protocol-mask>]]]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [tagged-802-3 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]]]

Назначение: Позволяет задать именованное расширенное правило списка доступа ACL для MAC-адресов. Отмена команды (с 'no') удаляет это расширенное правило списка доступа ACL.

Параметры: any-source-mac: Любой источник MAC-адреса;

any-destination-mac: Любое назначение MAC-адреса;

host_smac, smac: MAC-адрес источника;

smac-mask: маска (обратная маска) MAC-адреса источника;

host_dmac, dmac: MAC-адрес назначения;

dmac-mask: маска (обратная маска) MAC-адреса назначения;

untagged-eth2: формат нетегированных пакетов Ethernet II;

tagged-eth2: формат тегированных пакетов Ethernet II;

untagged-802-3: формат нетегированных пакетов 802.3;

tagged-802-3: формат тегированных пакетов 802.3;

cos-val: Значение cos, 0-7;

cos-bitmask: Маска протокола, 0-7; обратная маска, биты маски берутся последовательно.

vid-value: Номер vlan, 1-4094;

vid-bitmask: Маска VLAN, 0-4095; обратная маска, биты маски берутся последовательно.

protocol: Номер конкретного Ethernet-протокола, 1536-65535;

protocol-bitmask: Маска протокола, 0-65535; обратная маска, биты маски берутся последовательно.

Примечание: «Биты маски берутся последовательно» означает – биты, имеющие значения, начинаются слева, к ним могут добавляться справа биты, не оказывающие эффекта. Например, формат одного байта обратной маски: 00001111b; формат маски 11110000; недопустимая комбинация битов: 00010011.

Режим конфигурирования: Режим настройки именованного расширенного списка доступа для MAC-адресов

Значение по умолчанию: Список доступа не задан.

Пример: Запретить передачу пакетных данных 802.3 от источника с MAC-адресом 00-12-11-23-XX-XX.

```
Switch(config)# mac-access-list extended macExt
Switch(Config-Mac-Ext-Nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac untagged-802-3
Switch(Config-Mac-Ext-Nacl-macExt)# deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any tagged-802
```

17.1.24 permit | deny (mac-ip extended)

Синтаксис: [no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac><dmac-mask>}} icmp {{<source> <source-wildcard>} | any-source | {host-source <source-host-ip>}} {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [*<icmp-type>*] [*<icmp-code>*] [*precedence <precedence>*] [*tos <tos>*] [*time-range <time-range-name>*]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} igmp {{<source> <source-wildcard>} | any-source | {host-source <source-host-ip>}} {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [*<igmp-type>*] [*precedence <precedence>*] [*tos <tos>*] [*time-range <time-range-name>*]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} tcp {{<source> <source-wildcard>} | any-source | {host-source <source-host-ip>}} [*s-port <port1>*] {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [*d-port <port3>*] [*ack + fin + psh + rst + urg + syn*] [*precedence <precedence>*] [*tos <tos>*] [*time-range <time-range-name>*]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} udp {{<source> <source-wildcard>} | any-source | {host-source <source-host-ip>}} [*s-port <port1>*] {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [*d-port <port3>*] [*precedence <precedence>*] [*tos <tos>*] [*time-range <time-range-name>*]

[no] {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} {eigrp | gre | igmp | ip | ipinip | ospf | {<protocol-num>}} {{<source> <source-wildcard>} | any-source | {host-source <source-host-ip>}} {{<destination> <destination-wildcard>} | any-destination

| {host-destination <destination-host-ip>}} [precedence <precedence>] [tos <tos>] [time-range<time-range-name>]

Назначение: Позволяет задать именованное расширенное MAC-IP правило списка доступа ACL. Отмена команды (с 'No') удаляет одно расширенное нумерованное MAC-IP правило списка доступа ACL.

Параметры: **num:** серийный номер списка доступа (десятичный), в пределах 3100-3199;

deny: если согласование с правилом достигнуто, то запретить доступ;

permit: если согласование с правилом достигнуто, то разрешить доступ;

any-source-mac: любой MAC-адрес источника;

any-destination-mac: любой MAC-адрес назначения;

host_smac, smac: MAC-адрес источника;

smac-mask: маска (обратная маска) MAC-адреса источника;

host_dmac, dmas: MAC-адрес назначения;

dmac-mask: маска (обратная маска) MAC-адреса назначения;

protocol: номер протокола, имя протокола или IP-протокол. Может быть одним из ключевых слов: eigrp, gre, icmp, igmp, igmp, ip, ipinip, ospf, tcp или udp, либо целым числом в пределах 0-255, являющимся номером протокола IP. Для согласования со всеми Интернет-протоколами (включая ICMP, TCP и UDP) используйте суффикс 'ip', в списке, приведенном ниже:

source-host-ip: номер источника сети-источника или хоста-источника доставляемого пакета. 32-битные числа, представленные в десятичном формате с точками;

host-source: означает, что IP-адрес является адресом хоста источника, в противном случае IP-адрес будет считаться адресом сети;

source-wildcard: IP-адрес в обратном порядке. 32-битные числа, представленные в десятичном формате с 4 точками-разделителями, обратная маска;

destination-host-ip, номер назначения сети назначения, либо хоста, на который доставляются пакеты. 32-битные числа, представленные в десятичном формате с точками;

host-destination: означает, что адрес является адресом хоста назначения, в противном случае считается IP-адресом сети;

destination-wildcard: Маска назначения. | 32-битные числа, представленные в десятичном формате с 4 точками-разделителями, обратная маска;

s-port (опция): означает необходимость согласования с портом источником при TCP/UDP;

port1 (опция): номер интерфейса источника при TCP/UDP, целое число в пределах 0-65535;

d-port (опция): означает необходимость согласования с интерфейсом назначения при TCP/UDP;

port3 (опция): номер интерфейса назначения при TCP/UDP, целое число в пределах 0-65535;

[ack] [fin] [psh] [rst] [urg] [syn], (опции): только для протокола TCP, порядок следования тегов не важен. Когда данные TCP дают информацию о том, что сконфигурированы соответствующие позиции, то включается инициализация данных отчета TCP для формирования согласования (когда присутствует соединение);

precedence (опция): пакеты могут фильтроваться по приоритетам (целое число в пределах 0-7);

tos (опция): пакеты могут фильтроваться по типу обслуживания (целое число в пределах 0-15);

icmp-type (опция): ICMP-пакеты могут фильтроваться по типу пакета (целое число в пределах 0-255);

icmp-code (опция): ICMP-пакеты могут фильтроваться по коду пакета (целое число в пределах 0-255);

igmp-type (опция): IGMP-пакеты могут фильтроваться по имени IGMP-пакета или по типу пакета (целое число в пределах 0-255);

<time-range-name>: имя временного диапазона.

Режим конфигурирования: Режим настройки расширенного списка доступа для MAC-IP-адресов

Значение по умолчанию: Список доступа не задан.

Примеры: Запретить прохождение пакетов UDP с любыми MAC-адресами источника и назначения, любыми IP-адресами источника и назначения, портом источника 100 и портом назначения 40000.

```
Switch (config)# access-list 3100 deny any-source-mac any-destination-mac udp any s-port 100 any-destination d-port 40000
```

17.1.25 show access-lists

Синтаксис: show access-lists [<num> | <acl-name>]

Назначение: Выводит информации о созданных списках доступа.

Параметры: **<acl-name>**: имя конкретного списка доступа ACL (символьная строка);

<num>: номер конкретного списка доступа ACL.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Если спискам доступа ACL имена не присвоены, на дисплей будет выведена информация обо всех ACL. Для каждого списка будет выведено число раз его использования.

Примеры:

```
Switch#show access-lists
access-list 10(used 0 time(s))
access-list 10 deny any-source
access-list 100(used 1 time(s))
access-list 100 deny ip any any-destination
access-list 100 deny tcp any any-destination
access-list 1100(used 0 time(s))
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2
access-list 3100(used 0 time(s))
access-list 3100 deny any-source-mac any-destination-mac udp any s-port 100
any-destination d-port 40000
```

Информация, отображаемая на дисплее	Описание
access-list 10 (used 1 time(s))	ACL 10 использовался 1 раз
access-list 10 deny any	Правило в ACL 10
access-list 100 (used 1 time(s))	ACL 100 использовался 1 раз
access-list 100 deny ip any any-destination	Правило в ACL 100
access-list 100 deny tcp any any-destination	Правило в ACL 100
access-list 1100(used 0 time(s))	ACL 1100 использовался 1 раз
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2	Правило в ACL 1100
access-list 3100 permit any-source-mac any-destination-mac udp any s-port 100 any-destination d-port 40000	Правило в ACL 1100

17.1.26 show access-group

Синтаксис: show access-group [interface {ethernet IFNAME | vlan <1-4094 >}]

Назначение: Выводит на дисплей привязки списков доступа ACL к портам.

Параметры: **IFNAME:** имя интерфейса.

<1-4094>: идентификатор Vlan (Vlan ID).

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Если имена интерфейсу не заданы, будут показаны все списки ACL, привязанные к порту.

Пример:

```
Switch#show access-group
interface name: Ethernet 0/0/1
IP Ingress access-list used is 100, traffic-statistics Disable.
Interface VLAN 100:
Ethernet0/0/4: IP Ingress access-list used is 100, packet(s) number is 0.
Ethernet0/0/5: IP Ingress access-list used is 100, packet(s) number is 0.
Ethernet0/0/6: IP Ingress access-list used is 100, packet(s) number is 0.
```

Информация, отображаемая на дисплее	Описание
interface name: Ethernet 0/0/1	Привязки порта Ethernet0/0/1
interface VLAN 100	Привязки интерфейса VLAN 100
packet(s) number is 10	Число пакетов, согласующихся с этим ACL

17.1.27 show firewall

Синтаксис: show firewall

Назначение: Отображает настройку firewall.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch#show firewall
Firewall status: Enable.
Firewall default rule: Permit
```

Информация, отображаемая на дисплее	Описание
firewall is enable	Фильтрация пакетов включена
the default action of firewall is permit	По умолчанию функция фильтрации пакетов настроена на пропускание всех пакетов.

17.1.28 show ipv6 access-lists

Синтаксис: show ipv6 access-lists [<num> | <acl-name>]

Назначение: Выводит на дисплей настройки списка доступа ACL IPv6.

Параметры: **<num>:** номер конкретного списка доступа, в пределах от 500 до 699; номера с 500 до 599 закреплены за стандартными списками доступа IPv6 ACL, номера с 600 по 699 закреплены за расширенными списками доступа IPv6 ACL;

<acl-name>: имя конкретного списка доступа, символьная строка длиной от 1 до 16 символов.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Если спискам доступа ACL имена не присвоены, на дисплей будет выведена информация обо всех ACL. Для каждого списка будет выведено число раз его использования.

Пример:

```
Switch #show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
ipv6 access-list 500 deny any-source
ipv6 access-list 510(used 1 time(s))
ipv6 access-list 510 deny ip any any-destination
ipv6 access-list 510 deny tcp any any-destination
ipv6 access-list 520(used 1 time(s))
ipv6 access-list 520 permit ip any any-destination
```

17.1.29 show time-range

Синтаксис: show time-range <word>

Назначение: Выводит на дисплей информацию о настройках функции временного диапазона.

Параметры: word: имя, присвоенное временному диапазону, информация о котором должна быть выведена на дисплей

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Если имя временного диапазона не задано, на дисплей выводится информация о всех временных диапазонах.

Пример:

```
Switch#show time-range time-range
timer1 (inactive, used 0 times)
absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (inactive, used 0 times)
absolute-periodic Monday 0:0:0 to Friday 23:59:59
```

17.1.30 time-range

Синтаксис: [no] time-range <time_range_name>

Назначение: Позволяет присвоить имя временному диапазону и включает режим работы с временными диапазонами.

Параметры: time_range_name: Имя временного диапазона, должно начинаться с буквы, длина не более 16 символов.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Временной диапазон не задан.

Пример: Создать именованный временной диапазон (с именем zes_timer).

```
Switch(config)#Time-range zes_timer
```

18 Команды для настройки 802.1x

18.1.1 debug dot1x detail

Синтаксис: `debug dot1x detail {pkt-send | pkt-receive | internal | all | userbased | webbased } | dhcproption82based} interface [ethernet] <interface-name>`

`no debug dot1x detail {pkt-send | pkt-receive | internal | all | userbased | webbased} | dhcproption82based } interface [ethernet] <interface-name>`

Назначение: Включает вывод подробной отладочной информации dot1x. Отмена команды `no debug dot1x detail { pkt-send | pkt-receive | internal | all | userbased | webbased } |dhcproption82based }` interface [ethernet] <interface-name> прекращает вывод подробной отладочной информации dot1x.

Параметры:

pkt-send: детальная информация об отправленных пакетах;

pkt-receive: детальная информация о принятых пакетах;

internal: детальная внутренняя информация;

all: вывод всей детальной информации; аутентификация на основе пользователя;

webbased: аутентификация на основе Web-интерфейса;

dhcproption82based: информация об аутентификации на основе dhcproption82;

<interface-name>: имя интерфейса.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей детальную отладочную информацию dot1x, позволяющую проверить работу протокола Radius и определить причину сбоев (если таковые имеются).

Пример: Включить вывод детальной отладочной информации dot1x для интерфейса 0/0/1.
`Switch#debug dot1x detail all interface ethernet0/0/1`

18.1.2 debug dot1x error

Синтаксис: `debug dot1x error`

`no debug dot1x error`

Назначение: Включает вывод отладочной информации об ошибках dot1x. Отмена команды `no debug dot1x error` прекращает вывод этой отладочной информации.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей отладочную информацию об ошибках dot1x, позволяющую проверить работу протокола Radius и определить причину сбоев (если таковые имеются).

Пример:

`Switch#debug dot1x error`

18.1.3 debug dot1x fsm

Синтаксис: `debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>`

`no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>`

Назначение: Включает вывод отладочной информации о состоянии машины при dot1x. Отмена команды `no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>` прекращает вывод отладочной информации о состоянии машины.

Режим конфигурирования: Привилегированный режим.

Параметры: **all:** включает вывод отладочной информации о состоянии машины при dot1x;

aksm: включает вывод отладочной информации о состоянии машины передачи ключа аутентификатора;

asm: включает вывод отладочной информации о состоянии машины аутентификатора;

basrm: включает вывод отладочной информации о состоянии машины базы данных аутентификатора;

ratsm: включает вывод отладочной информации о состоянии таймера повторной аутентификации;

<interface-name>: имя интерфейса.

Описание: Команда позволяет вывести на дисплей отладочную информацию dot1x, позволяющую проверить процесс согласования параметров при dot1x и определить причину сбоев (если таковые имеются).

Пример: Включить вывод отладочной информации о состоянии машины при dot1x.

```
Switch#debug dot1x fsm asm interface ethernet0/0/1
```

18.1.4 debug dot1x packet

Синтаксис: `debug dot1x packet {all | receive | send} interface <interface-name>`

`no debug dot1x packet {all | receive | send} interface <interface-name>`

Назначение: Включает вывод отладочной информации о сообщениях dot1x. Отмена команды `no debug dot1x packet {all | receive | send} interface <interface-name>` прекращает вывод этой отладочной информации.

Режим конфигурирования: Привилегированный режим.

Параметры: **send:** отладочная информация dot1x об отправленных пакетах;

receive: отладочная информация dot1x о принятых пакетах;

all: отладочная информация dot1x о переданных и принятых пакетах;

<interface-name>: Имя интерфейса.

Описание: Команда позволяет вывести на дисплей отладочную информацию о сообщениях dot1x, проверить процесс согласования параметров при dot1x и определить причину сбоев (если таковые имеются).

Пример: Включить вывод отладочной информации о сообщениях dot1x;

```
Switch#debug dot1x packet all interface ethernet0/0/1
```

18.1.5 dot1x accept-mac

Синтаксис: `dot1x accept-mac <mac-address> [interface <interface-name>]`

`no dot1x accept-mac <mac-address> [interface <interface-name>]`

Назначение: Добавляет MAC-адрес в таблицу фильтруемых адресов dot1x. Если порт указан, адрес добавляется только для указанного порта. Если порт не указан, адрес добавляется ко всем портам. Отмена команды `no dot1x accept-mac <mac-address> [interface <interface-name>]` удаляет адрес из таблицы фильтруемых адресов dot1x.

Параметры: **<mac-address>:** MAC-адрес;

<interface-name>: имя интерфейса и номер порта.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Нет.

Описание: Функция фильтрации адресов dot1x работает с таблицей фильтруемых MAC-адресов. Она позволяет пользователю вручную добавлять фильтрующие dot1x-адреса в таблицу или удалять их из нее. Если порт указан в команде, то добавление адреса в таблицу выполняется только для этого порта. Если порт не указан, адрес добавляется для всех портов коммутатора. Когда функция фильтруемых dot1x-адресов включена, коммутатор будет фильтровать проходящих аутентификацию пользователей, используя MAC-адреса. Будут приниматься только запросы аутентификации, инициированные пользователями, имеющимися в таблице фильтруемых dot1x-адресов. Остальные запросы будут отвергаться.

Пример: Добавить MAC-адрес 00-01-34-34-2e-0a в таблицу фильтруемых адресов порта Ethernet 0/0/5.

```
Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 0/0/5
```

18.1.6 dot1x eap or enable

Синтаксис: dot1x eap or enable

no dot1x eap or enable

Назначение: Включает функцию передачи аутентификационных данных протокола EAP на коммутаторе. Отмена команды **no dot1x eap or enable** задает локальное окончание аутентификации.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Передача аутентификационных данных протокола EAP включена.

Описание: Коммутатор может быть соединен с RADIUS-сервером по протоколам Ethernet или PPP. Если между RADIUS-сервером и коммутатором существует Ethernet-соединение, коммутатору потребуется передача аутентификационной информации пользователя по протоколу EAP (аутентификация EAPoR). Если коммутатор подключен к RADIUS-серверу по PPP, коммутатор будет использовать локальное окончание аутентификации EAP (аутентификацию CHAP). В зависимости от соединения коммутатора с сервером аутентификации, коммутатор будет использовать различные методы аутентификации.

Пример: Включить на коммутаторе локальное окончание аутентификации EAP.

```
Switch(config)#no dot1x eap or enable
```

18.1.7 dot1x enable

Синтаксис: dot1x enable

no dot1x enable

Назначение: Включает функцию 802.1x на коммутаторе и портах. Отмена команды **no dot1x enable** выключает функцию 802.1x.

Режим конфигурирования: Глобальный режим конфигурирования, режим настройки интерфейсов.

Значение по умолчанию: Функция 802.1x не включена в глобальном режиме конфигурирования. Если функция 802.1x в глобальном режиме конфигурирования включена, по умолчанию она не будет включена для портов.

Описание: Для того, чтобы аутентификация 802.1x работала на соответствующих портах, она сначала должна быть включена в глобальном режиме конфигурирования.

Пример: Включить функцию 802.1x на коммутаторе, затем включить 802.1x для порта 0/0/12.

```
Switch(config)#dot1x enable
Switch(config)#interface ethernet 0/0/12
Switch(Config-If-Ethernet0/0/12)#dot1x enable
```

18.1.8 user-control limit

Синтаксис: user-control limit <count>

Назначение: В глобальном режиме конфигурирования позволяет задать максимальное число управляемых (безопасных) пользователей.

Режим конфигурирования: Глобальный режим конфигурирования.

Настройки по умолчанию: Максимальное число пользователей, поддерживаемое коммутатором, составляет 128.

Описание: Команда позволяет задать максимальное число пользователей, поддерживаемое коммутатором, в пределах от 1 до 200. Это число является предельно возможной суммой числа пользователей dot1x и числа безопасных пользователей, добавленных командой ip dhcp snooping binding user-control.

Пример: Задать в глобальном режиме конфигурирования максимальное число пользователей.

```
Switch(config)#user-control limit 100
```

18.1.9 dot1x guest-vlan

Синтаксис: dot1x guest-vlan <vlanid>

no dot1x guest-vlan

Назначение: Устанавливает для заданного порта гостевой vlan. Команда **no dot1x guest-vlan** используется для удаления гостевого vlan.

Параметры: <vlanid>: идентификатор заданного Vlan, диапазон значений от 1 до 4094.

Режим конфигурирования: Режим настройки интерфейсов.

Настройки по умолчанию: Функция 802.1x guest-vlan не включена на порту.

Описание: Устройство доступа будет добавлять порт в гостевой VLAN, если нет клиентского устройства, успешно прошедшего аутентификацию в течение некоторого достаточно короткого времени из-за несовершенства собственной системы аутентификации этого клиентского устройства. В гостевом VLAN пользователи могут получить программное обеспечение стандарта 802.1x для клиентского устройства, обновить систему клиентского устройства, либо обновить некоторые другие приложения (например, обновить антивирусное программное обеспечение, установить пакеты исправлений для операционной системы). Когда пользователь порта гостевого VLAN начинает аутентификацию, и она оканчивается неуспешно, порт будет оставаться в гостевом VLAN. Если аутентификация прошла успешно, возможны два результата:

1. сервер аутентификации присваивает значение Auto VLAN, что приводит к тому, что порт покидает гостевую сеть, чтобы войти в состав Auto VLAN. После того, как пользователь перейдет в автономный режим (offline), порт будет возвращен обратно заданному гостевому Vlan (снова закреплен за ним).
2. сервер аутентификации назначает Auto VLAN, и порт покидает гостевую VLAN, чтобы войти в состав Auto VLAN. После того, как пользователь перейдет в автономный режим (offline), порт будет возвращен обратно заданному гостевому VLAN (снова закреплен за ним).

Внимание: На разных портах могут быть установлены различные гостевые VLAN, однако на одном порту допускается только один гостевой VLAN.

Гостевой VLAN может работать только в том случае, если режим управления доступом основан на портах. Если режим управления доступом к порту основан на MAC-адресах или он пользовательский, гостевой VLAN может быть успешно установлен, но будет неработоспособен.

Пример: Установить Vlan 10 в качестве гостевого для порта Ethernet 0/0/3.

```
Switch(Config-If-Ethernet0/0/3)#dot1x guest-vlan 10
```

18.1.10 dot1x macfilter enable

Синтаксис: dot1x macfilter enable

no dot1x macfilter enable

Назначение: Включает функцию dot1x фильтрации адресов на коммутаторе. Отмена команды **no dot1x macfilter enable** выключает функцию фильтрации dot1x адресов.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Функция фильтрации dot1x адресов не включена.

Описание: Когда функция фильтруемых dot1x адресов включена, коммутатор будет фильтровать проходящих аутентификацию пользователей, используя MAC-адреса. Будет приниматься только запросы аутентификации, инициированные пользователями, имеющимися в таблице фильтруемых dot1x-адресов.

Пример: Включить на коммутаторе функцию фильтрации dot1x адресов.

```
Switch(config)#dot1x macfilter enable
```

18.1.11 dot1x max-req

Синтаксис: dot1x max-req <count>

no dot1x max-req

Назначение: Позволяет задать число запросов/кадров MD5, посылаемых перед тем, как коммутатор повторно инициирует аутентификацию при неполучении ответа от клиентской системы. Команда **no dot1x max-req** восстанавливает настройки, заданные по умолчанию.

Параметры: <count>: число раз повторных передач запроса EAP/ кадров MD5, в пределах от 1 до 10.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Задано максимальное число повторных передач, равное 2.

Описание: Рекомендуется использовать число повторных передач запроса EAP/кадров MD5, заданное по умолчанию.

Пример: Изменить максимальное число повторных передач запроса EAP/кадров MD5, установить его равным 5.

```
Switch(config)#dot1x max-req 5
```

18.1.12 dot1x user free-resource

Синтаксис: dot1x user free-resource <prefix> <mask>

no dot1x user free-resource

Назначение: Позволяет задать общедоступный ресурс 802.1x. Отмена команды **no dot1x user free-resource** удаляет доступ к общедоступному ресурсу.

Параметры: <prefix>: сегмент, в котором находится ограниченный ресурс;

<mask>: маска ограниченного ресурса;

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: общедоступный ресурс не задан.

Описание: Команда доступна только в том случае, если используется управление доступом на основе пользователей. Если используется такое управление доступом, команда позволяет установить ограниченный ресурс, к которому могут иметь доступ не аутентифицированные пользователи. При управлении доступом на основе портов и MAC-адресов, пользователи до окончания аутентификации не имеют доступа к ресурсам сети.

Для всей сети может быть задан только один общедоступный ресурс.

Пример: Задать сегмент с общедоступным ресурсом 1.1.1.0, маска 255.255.255.0.

```
Switch(Config)#dot1x user free-resource 1.1.1.0 255.255.255.0
```

18.1.13 dot1x max-user macbased

Синтаксис: dot1x max-user macbased <number>

no dot1x max-user macbased

Назначение: Позволяет задать максимальное число пользователей, которым разрешено подключаться к порту. Отмена команды **no dot1x max-user macbased** восстанавливает настройки, заданные по умолчанию.

Параметры: <number>: максимальное число пользователей, которым разрешено подключаться к порту, в пределах от 1 до 256.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Задано максимальное число пользователей, равное 1.

Описание: Эта команда доступна для портов, на которых используется управление доступом на основе MAC-адресов. Если номер аутентифицированного MAC-адреса больше числа адресов, разрешенных для пользователей, то пользователь с этим номером отвергается; пользователи с еще большими номерами также не получают доступа к сети.

Пример: Установить для порта 0/0/3 число разрешенных пользователей, равное 5.
Switch(Config-If-Ethernet0/0/3)#dot1x max-user macbased 5

18.1.14 dot1x max-user userbased

Синтаксис: dot1x max-user userbased <number>

no dot1x max-user userbased

Назначение: Позволяет задать максимальное число пользователей, которым разрешен доступ к указанному порту, при том, что используется режим управления доступом на основе пользователей. Отмена команды **no dot1x max-user userbased** восстанавливает настройки, заданные по умолчанию.

Параметры: <number>: максимальное число пользователей, которым будет разрешен доступ в сеть, в пределах от 1 до 256.

Режим команды: Режим настройки интерфейсов.

Настройки по умолчанию: Максимальное число пользователей, которым разрешен доступ, в каждом порту равно 10.

Описание: Эта команда будет работоспособна только тогда, когда на порту включен режим пользовательского управления доступом. Если число аутентифицированных пользователей превышает максимальное число пользователей, которым может быть разрешен доступ к указанному порту, то эти дополнительные пользователи не будут иметь доступа к сети.

Пример: Установить для порта 0/0/3 число разрешенных пользователей, равное 5.
Switch(Config-If-Ethernet0/0/3)#dot1x max-user userbased 5

18.1.15 dot1x port-control

Синтаксис: dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

Назначение: Позволяет задать состояние аутентификации 802.1x. Отмена команды **no dot1x port-control** восстанавливает настройки, используемые по умолчанию.

Параметры: **auto:** Включает аутентификацию 802.1x, состояние авторизации порта определяется информацией аутентификации, обмен которой идет между коммутатором и клиентской системой;

force-authorized: устанавливает для порта состояние авторизации, не аутентифицированным пользователям не разрешается проходить через порт;

force-unauthorized: для порта будет задан неавторизованный режим, коммутатор не будет выполнять аутентификацию клиентской системы, прохождение данных через порт запрещено.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Когда функция 802.1x включена для порта, по умолчанию установлено auto.

Описание: Если порту необходимо обеспечивать аутентификацию 802.1x для пользователя, режим аутентификации порта должен быть установлен на auto.

Пример: Установить на порту 1/1 режим аутентификации 802.1x.
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#dot1x port-control auto

18.1.16 dot1x port-method

Синтаксис: dot1x port-method {macbased | portbased | userbased advanced | dhcproption82based}

no dot1x port-method

Назначение: Устанавливает метод управления доступом к указанному интерфейсу. Отмена команды: "no dot1x port-method" восстанавливает метод управления доступом, использованный по умолчанию.

Параметры: **macbased:** устанавливает метод управления доступом на основе MAC-адресов;

portbased: устанавливает метод управления доступом на основе портов;

userbased: устанавливает метод управления доступом на основе пользователей. Этот метод имеет два вида - стандартное и расширенное управление доступом.

dhcpoption82based: устанавливает метод управления доступом на основе DHCP option82.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Метод управления доступом на основе пользователей (расширенное управление).

Описание: Команда используется для установки метода аутентификации dot1x для указанного порта. При управлении доступом на основе портов, допускается аутентификация только одного хоста. После аутентификации хосту будут доступны все сетевые ресурсы. При управлении доступом на основе MAC-адресов допускается аутентификация многих хостов, подключенных к одному и тому же порту. После аутентификации этим хостам будут доступны все сетевые ресурсы. Когда применяются методы управления доступом, упомянутые выше, не аутентифицированным хостам недоступны никакие сетевые ресурсы.

Если используется метод управления доступом на основе пользователей, пользователям могут быть доступны только ограниченные ресурсы сети. Метод управления доступом на основе пользователей имеет два вида – стандартное управление доступом и расширенное управление доступом. При стандартном управлении доступом, когда хост еще не аутентифицирован, он имеет неограниченный доступ к ограниченным ресурсам сети. При расширенном управлении доступом, когда хост еще не аутентифицирован, может осуществляться управление доступом к ограниченными ресурсам сети.

При методе управления доступом DHCP option 82, хостам, на которых функционирует ПО DHCP-клиентов, до и после аутентификации будут назначены разные IP-адреса, причем эти хосты будут иметь доступ к сетевым ресурсам при обоих IP-адресах. В этом режиме протокол DHCP назначает адреса в соответствии с информацией option 82. Когда хосты попытаются получить IP-адрес посредством DHCP, коммутатор добавит в конец запроса DHCP информацию option 82, соответствующую состоянию аутентификации хоста. Затем в соответствии с этой информацией DHCP-сервер назначит адреса. Одновременно с этим, на магистральном коммутаторе, подключенном к коммутатору доступа, может существовать список доступа ACL, управляющий доступом к сетевым ресурсам, которые могут быть доступны хосту.

Примечания: Для стандартного управления на основе пользователей сначала должны быть сконфигурированы общедоступные ресурсы 802.1x.

Пример: Включить стандартный метод управления доступом на основе портов на порту Ethernet0/0/4.

```
Switch(Config-If-Ethernet0/0/4)#dot1x port-method portbased
```

18.1.17 dot1x privateclient enable

Синтаксис: dot1x privateclient enable

no dot1x privateclient enable

Назначение: Включает на коммутаторе режим принудительной аутентификации клиента с использованием частного протокола аутентификации 802.1x, разработанного компанией Zelax. Отмена команды **no dot1x privateclient enable** выключает режим принудительной аутентификации клиента с использованием частного протокола аутентификации 802.1x, разработанного компанией Zelax и возобновляет использование стандартного протокола аутентификации 802.1x.

Синтаксис: Глобальный режим конфигурирования.

Значение по умолчанию: Частные сообщения 802.1x для клиента не включены.

Пример: Включить на коммутаторе режим принудительной аутентификации клиента с использованием частного протокола аутентификации 802.1x, разработанного компанией Zelax.

```
Switch(config)#dot1x privateclient enable
```

18.1.18 dot1x re-authenticate

Синтаксис: dot1x re-authenticate [interface <interface-name>]

Назначение: Включает повторную аутентификацию IEEE 802.1x реального времени на всех портах (не требующую ожидания), либо на указанном порту.

Параметры: <interface-name>: номер порта, если этот параметр отсутствует, то одно и то же значение параметра действует для всех портов.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Эта команда является командой глобального режима конфигурирования. Она позволяет коммутатору провести повторную аутентификацию клиента без ожидания истечения времени таймера повторной аутентификации. После выполнения аутентификации эта команда не работает.

Пример: Включить повторную аутентификацию реального времени на порту 0/0/8.
Switch(config)#dot1x re-authenticate interface ethernet 0/0/8

18.1.19 dot1x re-authentication

Синтаксис: dot1x re-authentication

no dot1x re-authentication

Назначение: Включает периодическую аутентификацию клиентской системы. Отмена команды **no dot1x re-authentication** выключает эту функцию.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Периодическая аутентификация клиентской системы не включена.

Описание: Когда включена периодическая аутентификация клиентской системы, коммутатор будет через регулярные интервалы времени выполнять повторную аутентификацию клиентской системы. Эта функция не рекомендуется для широкого использования.

Пример: Включить периодическую повторную аутентификацию аутентифицированных пользователей.
Switch(config)#dot1x re-authentication

18.1.20 dot1x timeout quiet-period

Синтаксис: dot1x timeout quiet-period <seconds>

no dot1x timeout quiet-period

Назначение: Позволяет задать время бездействия в порту при сбое аутентификации клиентской системы. Команда **no dot1x timeout quiet-period** восстанавливает значение, используемое по умолчанию.

Параметры: <seconds>: время бездействия на порту в секундах, в пределах от 1 до 65535 секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 10 секунд.

Описание: Рекомендуется использовать значение, заданное по умолчанию.

Пример: Установить время бездействия 120 секунд.
Switch(config)#dot1x timeout quiet-period 120

18.1.21 dot1x timeout re-authperiod

Синтаксис: dot1x timeout re-authperiod <seconds>

no dot1x timeout re-authperiod

Назначение: Позволяет задать интервал времени, по истечении которого выполняется повторная аутентификация клиентской системы. Команда **no dot1x timeout re-authperiod** восстанавливает настройки, используемые по умолчанию.

Параметры: **<seconds>**: интервал времени повторной аутентификации в секундах, в пределах от 1 до 65535 секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 3600 секунд.

Описание: Для того, чтобы стало возможно изменять интервал времени повторной аутентификации клиентской системы, предварительно должна быть включена повторная аутентификация dot1x. Если аутентификация не включена на коммутаторе, команда изменения интервала времени повторной аутентификации клиентской системы работать не будет.

Пример: Задать время повторной аутентификации 1200 секунд.
`Switch(config)#dot1x timeout re-authperiod 1200`

18.1.22 dot1x timeout tx-period

Синтаксис: `dot1x timeout tx-period <seconds>`

`no dot1x timeout tx-period`

Назначение: Позволяет задать интервал времени, по истечении которого клиентской системой выполняется повторная передача запроса/кадра идентичности EAP. Команда **no dot1x timeout tx-period** восстанавливает настройки, используемые по умолчанию.

Параметры: **<seconds>**: интервал времени повторной передачи кадров с запросами EAP в секундах, в пределах от 1 до 65535 секунд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 30 секунд.

Описание: Рекомендуется использовать значение, заданное по умолчанию.

Пример: Установить интервал времени повторной передачи кадров с запросами EAP 1200 секунд.
`Switch(config)#dot1x timeout tx-period 1200`

18.1.23 dot1x unicast enable

Синтаксис: `dot1x unicast enable`

`no dot1x unicast enable`

Назначение: Включает функцию прозрачной передачи unicast 802.1x.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Функция выключена.

Описание: Функция прозрачной передачи аутентификации 802.1x должна быть включена прежде, чем будет включена функцию прозрачной передачи unicast 802.1x.

Пример:

```
Switch(config)#dot1x enable
Switch(config)#dot1x unicast enable
Switch(config)#interface ethernet 0/0/1
Switch(Config-If-Ethernet0/0/1)#dot1x enable
```

18.1.24 show dot1x

Синтаксис: `show dot1x [interface <interface-list>]`

Назначение: Выводит на дисплей информацию о параметрах dot1x. Если заданы параметры, отображается информация о состоянии dot1x для соответствующего порта.

Параметры: **<interface-list>**: список портов. Если параметры не заданы, отображается информация для всех портов.

Режим конфигурирования: Привилегированный режим

Описание: Команда позволяет вывести на дисплей параметры и другую информацию протокола dot1x.

Пример: Вывести на дисплей информацию о глобальных параметрах dot1x коммутатора.

```
Switch#show dot1x
Global 802.1X Parameters
  free resource           :unknown
  reauth-enabled         :no
  reauth-period          :3600
  quiet-period           :10
  tx-period              :30
  max-req                :2
  authenticator mode     :active
```

```
Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
dot1x-privateclient Disable
dot1x-privateclient protect Disable
dot1x-unicast Disable
```

```
802.1X is enabled on port Ethernet0/0/3
Authentication Method:User based advanced
Max User Number:10
Notify trustview is 0
```

Информация, отображаемая на дисплее	Описание
Global 802.1x Parameters	Информация о глобальных параметрах 802.1x
reauth-enabled	Указывает, включена повторная аутентификация или нет
reauth-period	Интервал повторной аутентификации
quiet-period	Интервал бездействия
tx-period	Интервал повторной передачи EAP
max-req	Интервал повторной передачи пакета EAP
authenticator mode	Режим аутентификации коммутатора
Mac Filter	Включен фильтр адресов dot1x или нет
MacAccessList	Таблица фильтрующих адресов Dot1x
Dot1x-EAPoR	Метод аутентификации, используемый в коммутаторе (передача пакетов аутентификации EAP, локальное окончание EAP)
802.1x is enabled on ethernet Ethernet0/0/1	Указывает, включен или нет протокол dot1x для порта
Authentication Method:	Метод аутентификации порта (на основе MAC-адресов, на основе портов)

19 Команды для настройки управления доступом (AM)

19.1.1 am enable

Синтаксис: `am enable`

`no am enable`

Назначение: Включает или выключает функцию AM в глобальном режиме конфигурирования.

Параметры: Нет.

Значение по умолчанию: По умолчанию функция AM выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: При включении функции AM (access management — управление доступом), информация принятых пакетов IP или ARP (IP-адрес источника или IP-адрес источника + MAC-адрес источника) сравнивается с настройками аппаратных адресов в пуле адресов. При обнаружении совпадения пакет передается, в противном случае — отбрасывается.

Пример: Включить функцию AM на коммутаторе.

```
Switch(config)#am enable
```

Отключить функцию AM на коммутаторе.

```
Switch(config)#no am enable
```

19.1.2 am port

Синтаксис: `am port`

`no am port`

Назначение: Включает функцию AM для физических портов. Отмена команды `no am port` выключает функцию AM.

Параметры: Нет.

Значение по умолчанию: Функция AM выключена на всех портах.

Режим конфигурирования: Режим настройки интерфейсов.

Пример: Включить функцию AM на интерфейсе 0/0/3 коммутатора.

```
Switch(Config-If-Ethernet 0/0/3)#am port
```

Отключить функцию AM на интерфейсе 0/0/3 коммутатора.

```
Switch(Config-If-Ethernet 0/0/3)#no am port
```

19.1.3 am ip-pool

Синтаксис: `am ip-pool <ip-address> <num>`

`no am ip-pool <ip-address> <num>`

Назначение: Позволяет задать сегмент IP-адресов AM для интерфейса, разрешить или запретить передачу IP- или APR-сообщений от IP-источника в этом сегменте, которые могут передаваться через интерфейс.

Параметры: `<ip-address>`: начальный адрес сегмента адресов в пуле IP-адресов;

`<num>`: число последовательных адресов, следующих за начальным ip-адресом, не более 32.

Значение по умолчанию: IP-пул пуст.

Режим конфигурирования: Режим настройки интерфейсов.

Пример: Настроить Ethernet-интерфейс 0/0/3 таким образом, чтобы передавались все пакеты от 10 источников, адреса которых берутся последовательно, начинаться с адреса 10.10.10.1.

```
Switch(Config-If-Ethernet 0/0/3)#am ip-pool 10.10.10.1 10
```

19.1.4 am mac-ip-pool

Синтаксис: am mac-ip-pool <mac-address> <ip-address>

no am mac-ip-pool <mac-address> <ip-address>

Назначение: Позволяет задать АМ MAC-IP-адрес для интерфейса, разрешить или запретить передачу IP- или APR-сообщений от IP-источника в этом сегменте, которые могут передаваться через интерфейс.

Параметры: <mac-address>: MAC-адрес источника;

<ip-address>: IP-адрес источника пакетов, 32-разрядное двоичное число, представленное четырьмя десятичными числами.

Значение по умолчанию: MAC-IP-пул пуст.

Режим конфигурирования: Режим настройки интерфейсов.

Пример: Настроить коммутатор так, чтобы через интерфейс 0/0/3 передавались пакеты от источника с MAC-адресом 11-22-22-11-11-11 и от источника с IP-адресом 10.10.10.1.
Switch(Config-If-Ethernet0/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1

19.1.5 no am all

Синтаксис: no am all [ip-pool | mac-ip-pool]

Назначение: Удаляет все пользовательские настройки для таблиц MAC-IP-пула и IP-пула.

Параметры: ip-pool: пул IP-адресов.

mac-ip-pool: пул mac-ip-адресов.

Если команда введена без параметров, будут удалены оба пула адресов.

Значение по умолчанию: Оба пула адресов пусты.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Очистить все адреса в IP-пуле.

Switch(config)#no am all ip-pool

19.1.6 show am

Синтаксис: show am [interface <interface-name>]

Назначение: Позволяет вывести на дисплей настройки адресов АМ для текущего коммутатора.

Параметры: <interface-name>: имя интерфейса, настройки которого будут выведены на дисплей. Если команда введена без параметров, будут выведены настройки АМ для всех интерфейсов.

Режим конфигурирования: Привилегированный режим

Пример: Вывести на дисплей все настройки адресов АМ.

```
Switch#show am
AM is enabled
Interface Ethernet0/0/3    am interface    am ip-pool 30.10.10.1 20
Interface Ethernet0/0/5    am interface    am ip-pool 50.10.10.1 30    am mac-
ip-pool 00-02-04-06-08-09 20.10.10.5      am ip-pool 50.20.10.1 20
Interface Ethernet0/0/6    am interface
Interface Ethernet0/0/1    am interface    am ip-pool 10.10.10.1 20    am ip-
pool 10.20.10.1 20
```

20 Команды для настройки протокола TACACS+

20.1.1 tacacs-server authentication host

Синтаксис: `tacacs-server authentication host <ip-address> [port <port-number>] [timeout <seconds>] [key <string>] [primary]`

`no tacacs-server authentication host <ip-address>`

Назначение: Позволяет задать IP-адрес, номер порта прослушивания, значение таймера и строку ключа сервера TACACS+. Отмена команды `no tacacs-server authentication host <ip-address>` удаляет сервер аутентификации TACACS+.

Параметры: `<ip-address>`: IP-адрес сервера.

`<port-number>`: номер порта прослушивания сервера, в пределах от 0 до 65535. 0 означает, что прослушивание на сервере аутентификации не выполняется;

`<seconds>`: значение таймера аутентификации TACACS+ , в пределах от 1 до 60 секунд;

`key <string>`: строка ключа, длиной не более 16 символов;

`primary`: указывает, что сервер является первичным.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: аутентификация TACACS+ не включена в системе.

Описание: Эта команда используется для указания IP-адреса, номера порта, таймера и строки ключа сервера TACACS+, которые используются при аутентификации на коммутаторе. Параметр `port` определяет номер порта аутентификации, который должен совпадать с номером порта, указанным для сервера TACACS+ (по умолчанию равен 49). Параметры `key` и `timeout` используются для установки собственного ключа и таймера коммутатора. Если эти параметры не заданы, будут использованы таймер и ключ, заданные в глобальном режиме конфигурирования для `tacacs-сервера: timeout<секунд>` и `tacacs-server key <строка>`. С помощью этой команды можно сконфигурировать несколько TACACS+ серверов, связывающихся с коммутатором. Последовательность настройки такая же, как и для сервера аутентификации. Если для TACACS+ сервера задана опция `primary`, сервер будет первичным.

Пример: Задать адрес сервера аутентификации TACACS+ равным 192.168.1.2. Использовать ключ, заданный в глобальном режиме конфигурирования.
`Switch(config)#tacacs-server authentication host 192.168.1.2`

20.1.2 tacacs-server key

Синтаксис: `tacacs-server key <string>`

`no tacacs-server key`

Назначение: Позволяет задать ключ сервера TACACS+. Отмена команды `no tacacs-server key` удаляет ключ.

Параметры: `<string>`: символьная строка ключа сервера TACACS+, длина не более 16 символов.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Ключ используется для криптозащиты связи коммутатора с TACACS+-сервером. Заданный ключ должен соответствовать одному из ключей, установленных на TACACS+ сервере, в противном случае аутентификация будет выполняться некорректно. Для гарантии безопасности данных рекомендуется задавать ключ аутентификации сервера.

Пример: Установить в качестве ключа TACACS+-сервера аутентификации слово `test`.
`Switch(config)#tacacs-server key test`

20.1.3 tacacs-server nas-ipv4

Синтаксис: `tacacs-server nas-ipv4 <ip-address>`

`no tacacs-server nas-ipv4`

Назначение: Позволяет задать IP-адрес источника для TACACS+ пакетов, отправляемых коммутатором.

Параметры: <ip-address >: IP-адрес;

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: IP-адрес не задан.

Описание: Если IP-адрес источника для TACACS+ пакетов не задан, будет использоваться IP-адрес того интерфейса с которого отправляются пакеты.

Пример:

```
Switch(config)#tacacs-server nas-ipv4 192.168.2.254
```

20.1.4 tacacs-server timeout

Синтаксис: tacacs-server timeout <seconds>

no tacacs-server timeout

Назначение: Позволяет настроить для сервера TACACS+ время таймера. Команда **no tacacs-server timeout** восстанавливает настройки, используемые по умолчанию.

Параметры: <seconds>: значение таймера аутентификации TACACS+ , в пределах от 1 до 60 секунд;

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 3 с.

Описание: Команда позволяет задать время ожидания коммутатора окончания аутентификации на сервере TACACS+. После отправки на сервер TACACS+ пакета с запросом, коммутатор ожидает ответа сервера. Если в течение указанного периода времени ответ не принят, аутентификация считается безуспешной.

Пример: Установить таймер для tacacs+ сервера равным 30 секундам.

```
Switch(config)# tacacs-server timeout 30
```

20.1.5 debug tacacs-server

Синтаксис: debug tacacs-server

no debug tacacs-server

Назначение: Позволяет вывести на дисплей сообщения TACACS+. Отмена команды **no debug tacacs-server** прекращает вывод на дисплей отладочных сообщений TACACS+.

Режим конфигурирования: Привилегированный режим.

Параметры: Нет.

Описание: Позволяет включить вывод на дисплей сообщений TACACS+ для контроля согласования параметров при протоколе TACACS+, что помогает установить причину сбоев.

Пример: Включить вывод на дисплей сообщений протокола TACACS+.

```
Switch#debug tacacs-server
```

21 Команды для настройки протокола RADIUS

21.1.1 aaa enable

Синтаксис: `aaa enable`

no `aaa enable`

Назначение: Включает функцию аутентификации AAA на коммутаторе. Отмена команды **no aaa enable** выключает функцию аутентификации AAA.

Режим конфигурирования: Глобальный режим конфигурирования.

Параметры: Нет.

Значение по умолчанию: AAA аутентификация не включена.

Описание: Для того, чтобы аутентификация AAA работала, надо включить на коммутаторе аутентификацию IEEE 802.1x.

Пример: Включить функцию AAA коммутатора.
`Switch(config)#aaa enable`

21.1.2 aaa-accounting enable

Синтаксис: `aaa-accounting enable`

no `aaa-accounting enable`

Назначение: Включает на коммутаторе функцию AAA accounting. Команда **no aaa-accounting enable** выключает функцию AAA accounting.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: AAA accounting не включена.

Описание: Когда AAA accounting (учет сетевых сервисов) включен в коммутаторе, они будут учитываться на основе трафика или времени подключения аутентифицированного пользователя к порту. В момент начала учета сетевых ресурсов коммутатор пошлет на RADIUS-сервер, учитывающий сетевые сервисы, сообщение «учет сетевых сервисов начат». Далее, через каждые 5 секунд на RADIUS-сервер, учитывающий сетевые сервисы для онлайн-пользователя, будет поступать пакет учета сетевых сервисов. В момент окончания учета сетевых сервисов на RADIUS-сервер, учитывающий сетевые сервисы, будет отправлено сообщение «учет сетевых сервисов прекращен».

Примечание: Коммутатор посылает сообщение «пользователь в автономном режиме» на RADIUS-сервер, учитывающий сетевые сервисы, только в том случае, если учет сетевых сервисов включен. Сообщение «пользователь в автономном режиме» не будет послано на RADIUS-сервер аутентификации.

Пример: Включить функцию учета стоимости AAA на коммутаторе.
`Switch(config)#aaa-accounting enable`

21.1.3 aaa-accounting update

Синтаксис: `aaa-accounting update {enable | disable}`

Назначение: Включает или выключает обновление информации учета сетевых сервисов при AAA.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Обновление информации учета сетевых сервисов при AAA включено.

Описание: Если учет сетевых сервисов при AAA включен, коммутатор будет периодически посылать сообщения учета сетевых сервисов по каждому онлайн-пользователю на сервер учета сетевых сервисов.

Пример: Выключить обновление информации учета сетевых сервисов при AAA на коммутаторе.

```
Switch(config) #aaa-accounting update disable
```

21.1.4 debug aaa packet

Синтаксис: `debug aaa packet {send | receive | all} interface {ethernet <interface-number> | <interface-name>}`

`no debug aaa packet {send | receive | all} interface {ethernet <interface-number> | <interface-name>}`

Назначение: Включает вывод информации о приеме и отправке пакетов AAA. Отмена команды `no debug aaa packet {send|receive|all} interface{ethernet <interface-number> | <interface-name>}` прекращает вывод информации о приеме и отправке пакетов AAA.

Параметры: `send`: отправленные пакеты;

`receive`: принятые пакеты;

`all`: отправленные и принятые пакеты;

`<interface-number>`: номер интерфейса.

`<interface-name>`: имя интерфейса.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей отладочную информацию о сообщениях AAA, проверить сообщения, принятые и посланные протоколом Radius и определить причину сбоев (если таковые имеются).

Пример: Включить вывод отладочной информации о принятых и посланных пакетах AAA для Ethernet-интерфейса 0/0/1.

```
Switch#debug aaa packet all interface Ethernet 0/0/1
```

21.1.5 debug aaa detail attribute

Синтаксис: `debug aaa detail attribute interface {ethernet <interface-number> | <interface-name>}`

`no debug aaa detail attribute interface {ethernet <interface-number> | <interface-name>}`

Назначение: Включает вывод подробной отладочной информации AAA об атрибутах Radius. Отмена команды `no debug aaa detail attribute interface {ethernet <interface-number> | <interface-name>}` прекращает вывод подробной отладочной информации.

Параметры: `<interface-number>`: номер интерфейса.

`<interface-name>`: имя интерфейса.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей детальную отладочную информацию AAA об атрибутах Radius, позволяющую проверить работу протокола Radius и определить причину сбоев (если таковые имеются).

Пример: Включить вывод на дисплей детальной отладочной информации AAA об атрибутах Radius для интерфейса 0/0/1.

```
Switch#debug detail attribute interface Ethernet 0/0/1
```

21.1.6 debug aaa detail connection

Синтаксис: `debug aaa detail connection`

`no debug aaa detail connection`

Назначение: Включает вывод подробной отладочной информации AAA о соединении. Отмена команды `no debug aaa detail connection` прекращает вывод подробной отладочной информации.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей детальную отладочную информацию AAA о соединении, позволяющую проверить работу протокола AAA и определить причину сбоев (если таковые имеются).

Пример: Включить вывод на дисплей детальной отладочной информации AAA о соединении.

```
Switch#debug aaa detail connection
```

21.1.7 debug aaa detail event

Синтаксис: `debug aaa detail event`

`no debug detail event`

Назначение: Включает вывод отладочной информации AAA о событиях. Отмена команды `no debug detail event` прекращает вывод этой отладочной информации.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей отладочную информацию AAA о событиях, позволяющую проверить работу протокола Radius и определить причину сбоев (если таковые имеются).

Пример: Включить вывод отладочной информации AAA о событиях.

```
Switch#debug aaa detail event
```

21.1.8 debug aaa error

Синтаксис: `debug aaa error`

`no debug error`

Назначение: Включает вывод отладочной информации об ошибках AAA. Отмена команды `no debug error` прекращает вывод этой отладочной информации.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей отладочную информацию AAA об ошибках, позволяющую проверить работу протокола Radius и определить причину сбоев (если таковые имеются).

Пример: Включить вывод отладочной информации об ошибках AAA.

```
Switch#debug aaa error
```

21.1.9 radius nas-ipv4

Синтаксис: `radius nas-ipv4 <ip-address>`

`no radius nas-ipv4`

Назначение: Позволяет задать IP-адрес источника для пакетов RADIUS, посылаемых коммутатором. Отмена команды `no radius nas-ipv4` удаляет эту настройку.

Параметры: `<ip-address>`: IP-адрес источника пакетов RADIUS, должен быть корректным unicast-IP-адресом.

Значение по умолчанию: IP-адрес источника пакетов RADIUS не задан. В качестве IP-адреса источника пакетов RADIUS используется IP-адрес интерфейса, с которого посылаются пакеты RADIUS.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: IP-адрес источника должен принадлежать одному из IP-интерфейсов коммутатора. В противном случае в ответ на пакет RADIUS, посланный коммутатором придет сообщение об ошибке привязки IP-адреса. Рекомендуется использовать в качестве IP-адреса источника IP-адрес интерфейса петли. Это позволяет избежать отбрасывания пакетов на сервере RADIUS, когда интерфейсы выключены.

Пример: Задать IP-адрес источника пакетов RADIUS равным 192.168.2.254.

```
Switch#radius nas-ipv4 192.168.2.254
```

21.1.10 radius nas-ipv6

Синтаксис: `radius nas-ipv6 <ipv6-address>`

`no radius nas-ipv6`

Назначение: Позволяет задать IPv6-адрес источника для пакетов RADIUS, посылаемых коммутатором. Отмена команды `no radius nas-ipv6` удаляет эту настройку.

Параметры: `<ipv6-address>`: IPv6-адрес источника пакетов RADIUS, должен быть корректным unicast-IPv6-адресом.

Значение по умолчанию: IPv6-адрес источника пакетов RADIUS не задан. В качестве IPv6-адреса источника пакетов RADIUS используется IPv6-адрес интерфейса, с которого посылаются пакеты RADIUS.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: IPv6-адрес источника должен принадлежать одному из IPv6-интерфейсов коммутатора. В противном случае в ответ на пакет RADIUS, посланный коммутатором придет сообщение об ошибке привязки IPv6-адреса. Рекомендуется использовать в качестве IPv6-адреса источника IPv6-адрес интерфейса петли. Это позволяет избежать отбрасывания пакетов на сервере RADIUS, когда интерфейсы выключены.

Пример: Задать IPv6-адрес источника пакетов RADIUS равным 2001:da8:456::1.

```
Switch#radius nas-ipv6 2001:da8:456::1
```

21.1.11 radius-server accounting host

Синтаксис: `radius-server accounting host {<ipv4-address> | <ipv6-address>} [port <port-number>] [primary]`

`no radius-server accounting host {<ipv4-address> | <ipv6-address>}`

Назначение: Позволяет задать IPv4/IPv6-адрес и номер порта слушания для сервера учета сетевых сервисов RADIUS. Отмена команды `no radius-server accounting host {<ipv4-address>|<ipv6-address>}` удаляет RADIUS-сервер учета сетевых сервисов.

Параметры: `<ipv4-address> | <ipv6-address>`: IPv4 или IPv6 -адрес сервера;

`<port-number>`: номер порта прослушивания сервера, в пределах от 0 до 65535;

primary: первичный сервер. Могут быть настроены и сделаны доступными несколько RADIUS-серверов. Если параметр `primary` не задан, поиск RADIUS-серверов будет выполнен в порядке, заданном настройками; в противном случае первым будет использован RADIUS-сервер, указанный в параметре `primary`.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: RADIUS-сервер учета сетевых сервисов не настроен.

Описание: Эта команда используется для указания IPv4/IPv6 -адреса и номера порта для указанного RADIUS-сервера учета сетевых сервисов. Может быть введено несколько команд с разными настройками. В параметре `<port-number>` задается номер порта, он должен совпадать с номером порта учета сетевых сервисов RADIUS-сервера, по умолчанию 1813. Если задан номер порта 0, номер порта учета сетевых сервисов будет сгенерирован случайным образом, что может привести к неправильной настройке. Эту команду можно использовать несколько раз для настройки нескольких RADIUS-серверов, связывающихся с коммутатором. Коммутатор будет посылать пакеты учета стоимости на все настроенные серверы учета сетевых сервисов. Все серверы учета сетевых сервисов могут дублировать друг друга. Если задан параметр `primary`, то первичным RADIUS-сервером будет сервер, указанный в этом параметре.

Пример: Установить RADIUS-сервер учета сетевых сервисов с IP-адресом 100.100.100.60 как первичный сервер, номер порта учета стоимости 3000.

```
Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary
```

21.1.12 radius-server authentication host

Синтаксис: `radius-server authentication host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key <string>] [primary] [access-mode {dot1x | telnet}]`

`no radius-server authentication host {<ipv4-address> | <ipv6-address>}`

Назначение: Позволяет задать IP-адрес RADIUS-сервера, номер порта прослушивания, секретный ключ, является ли сервер первичным или нет, режим доступа. Отмена команды `no radius-server authentication host <IPaddress>` удаляет RADIUS-сервер.

Параметры: `<ipv4-address> | <ipv6-address>`: IPv4 или IPv6 -адрес сервера;

`<port-number>`: номер порта прослушивания сервера, в пределах от 0 до 65535;

0 означает, что сервер аутентификации использоваться не будет.

`<string>`: строка секретного ключа;

`primary`: первичный сервер.

Могут быть настроены и сделаны доступными несколько RADIUS-серверов. Если параметр `primary` не задан, поиск RADIUS-серверов будет выполнен в порядке, заданном настройками, в противном случае, первым будет использован RADIUS-сервер, указанный в параметре `primary`.

`access-mode {dot1x | telnet}`: текущий RADIUS-сервер будет использовать только для аутентификации 802.1x или telnet, все службы могут по умолчанию использовать текущий RADIUS-сервер.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: RADIUS-сервер аутентификации не настроен.

Описание: Эта команда используется для указания IPv4/IPv6 -адреса и номера порта для указанного RADIUS-сервера аутентификации коммутатора. Может быть введено несколько команд с разными настройками. В параметре `port` задается номер порта аутентификации, он должен совпадать с номером порта аутентификации RADIUS-сервера, номер порта по умолчанию: 1812. Если задан номер порта 0, заданный сервер считается не аутентифицирующим. Эта команда может быть введена несколько раз для настройки нескольких RADIUS-серверов, связывающихся с коммутатором. Выбор сервера аутентификации производится в соответствии с приоритетами, заданными при настройке. После ответа первого сервера (не важно при этом была аутентификация успешной или нет), коммутатор не будет посылать на следующий сервер запрос на аутентификацию. Если задан параметр `primary`, то первичным RADIUS-сервером будет сервер, указанный в этом параметре. Если для текущего RADIUS-сервера строка ключа не задана, будет использоваться ключ шифра, заданный командой `radius-server key <string>` в глобальном режиме конфигурирования. Кроме того, можно задать, чтобы текущий RADIUS-сервер использовался только для аутентификации 802.1x или telnet с опцией режима доступа (`access-mode option`). Опция `access-mode` не сконфигурирована и по умолчанию все службы могут использовать текущий RADIUS-сервер.

Пример: Задать адрес RADIUS-сервера аутентификации 2004:1:2:3::2.

```
Switch(config)#radius-server authentication host 2004:1:2:3::2
```

21.1.13 radius-server dead-time

Синтаксис: `radius-server dead-time <minutes>`

`no radius-server dead-time`

Назначение: Позволяет задать время восстановления RADIUS-сервера после его выключения и повторного включения. Команда `no radius-server dead-time` восстанавливает настройки, используемые по умолчанию.

Параметры: `<minutes>`: время восстановления RADIUS-сервера в минутах после его выключения и повторного включения, диапазон значений от 1 до 255.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 5 минут.

Описание: Эта команда позволяет задать время ожидания восстановления RADIUS-сервера из недоступного в доступное состояние. Когда подтверждения, посылаемые сервером,

недоступны на коммутаторе, он помечает этот сервер как сервер, имеющий неправильное состояние. По истечении интервала времени, заданного в команде, система переустанавливает состояние сервера на правильное.

Пример: Задать время восстановления RADIUS-сервера после выключения и повторного включения 3 минуты.

```
Switch(config)#radius-server dead-time 3
```

21.1.14 radius-server key

Синтаксис: `radius-server key <string>`

`no radius-server key`

Назначение: Позволяет задать ключ для RADIUS-сервера (для аутентификации и учета сетевых сервисов). Команда `no radius-server key` удаляет ключ RADIUS-сервера.

Параметры: `<string>`: строка ключа RADIUS-сервера, допустимая длина – не более 16 символов.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Ключ используется для криптозащиты связи коммутатора с указанным RADIUS-сервером. Ключ должен совпадать с тем ключом, который задан для RADIUS-сервера, в противном случае RADIUS-аутентификация и учет сетевых сервисов будут работать неправильно.

Пример: Задать ключ аутентификации RADIUS "test".

```
Switch(config)# radius-server key test
```

21.1.15 radius-server retransmit

Синтаксис: `radius-server retransmit <retries>`

`no radius-server retransmit`

Назначение: Позволяет настроить для RADIUS число попыток повторной передачи пакетов аутентификации. Отмена команды `no radius-server retransmit` восстанавливает настройки, используемые по умолчанию.

Параметры: `<retries>`: число попыток повторной передачи пакетов аутентификации для RADIUS-сервера, в пределах от 0 до 100.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 3 попытки.

Описание: Команда позволяет задать число попыток повторной передачи пакета, если RADIUS-сервер не ответил после того, как коммутатор послал на него пакет аутентификации. Если аутентификационная информация, поступающая от сервера аутентификации, потеряна, на сервер необходимо повторно передать запрос аутентификации AAA. Если счетчик числа попыток повторной передачи запроса AAA достигает порогового значения, а сервер не отвечает, то сервер будет считаться неработоспособным (на коммутаторе его состояние изменится на invalid).

Пример: Задать 5 попыток повторной передачи пакета аутентификации RADIUS.

```
Switch(config)# radius-server retransmit 5
```

21.1.16 radius-server timeout

Синтаксис: `radius-server timeout <seconds>`

`no radius-server timeout`

Назначение: Позволяет настроить для RADIUS-сервера время таймера. Команда `no radius-server timeout` восстанавливает настройки, используемые по умолчанию.

Параметры: `<seconds>`: время таймера RADIUS-сервера в секундах, диапазон значений от 1 до 1000.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 3 секунды.

Описание: Эта команда позволяет задать интервал времени, в течение которого коммутатор будет ожидать ответа RADIUS-сервера. После отправки на RADIUS-сервер пакетов запросов, коммутатор будет ожидать ответных пакетов заданное в команде число секунд. Если ответ RADIUS-сервера не получен в течение заданного времени, коммутатор повторно пошлет пакет, либо установит для сервера состояние `invalid` (в зависимости от текущих условий).

Пример: Установить таймер аутентификации RADIUS на 30 секунд.
`Switch(config)# radius-server timeout 30`

21.1.17 radius-server accounting-interim-update timeout

Синтаксис: `radius-server accounting-interim-update timeout <seconds>`

`no radius-server accounting-interim-update timeout`

Назначение: Позволяет задать интервал отправки сообщений обновления информации учета сервисов. Отмена команды `no radius-server accounting-interim-update timeout` восстанавливает настройки, используемые по умолчанию.

Параметры: `<seconds>`: интервал отправки сообщений обновления учета сервисов, в секундах, в пределах от 60 до 3600.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Задан интервал отправки сообщений обновления учета сервисов 300 секунд.

Описание: Эта команда позволяет задать интервал, через который NAS посылает сообщения обновления учета сервисов. Для того, чтобы реализовать учет сервисов для пользователей в реальном времени, с момента подключения пользователя в режиме онлайн, NAS посылает на RADIUS-сервер сообщения обновления учета сервисов для этого пользователя.

Интервал отправки сообщений обновления учета сервисов зависит от максимального числа пользователей, поддерживаемых NAS. Чем меньше интервал, тем меньше максимальное число пользователей, поддерживаемых NAS. Чем больше интервал, тем больше максимальное число пользователей, поддерживаемых NAS. В таблице приведены рекомендуемые отношения интервала отправки сообщений обновления учета сервисов к максимальному числу пользователей, поддерживаемых NAS:

Рекомендуемые отношения интервала отправки сообщений обновления учета сервисов к максимальному числу пользователей, поддерживаемых NAS.

Максимальное число пользователей	Интервал отправки сообщений обновления учета сервисов (в секундах)
1~299	300 (значение по умолчанию)
300~599	600
600~1199	1200
1200~1799	1800
≥1800	3600

Пример: Задать максимальное число пользователей, поддерживаемых NAS, равным 700 и интервал отправки сообщений обновления учета сервисов равным 1200 с.
`Switch(config)#radius-server accounting-interim-update timeout 1200`

21.1.18 show aaa authenticated-user

Синтаксис: `show aaa authenticated-user`

Назначение: Выводит на дисплей информацию об аутентифицированных пользователях.

Режим конфигурирования: Привилегированный режим

Описание: Администратора обычно интересует информация только об аутентифицированных пользователях, остальная информация используется при устранении неполадок службой технической поддержки.

Пример:

```
Switch#show aaa authenticated-user
----- authenticated users -----
UserName Retry RadID Port EapID ChapID OnTime      UserIP MAC
----- total: 0 -----
```

21.1.19 show aaa authenticating-user

Синтаксис: show aaa authenticating-user

Назначение: Выводит на дисплей информацию об аутентифицируемых пользователях.

Режим конфигурирования: Привилегированный режим

Описание: Администратора обычно интересует информация только об аутентифицируемых пользователях, остальная информация используется при устранении неполадок службой технической поддержки.

Пример:

```
Switch#show aaa authenticating-user
----- authenticating users -----
User-name  Retry-time  Radius-ID  Port    Eap-ID  Chap-ID  Mem-Addr  State
-----
----- total: 0 -----
```

21.1.20 show aaa config

Синтаксис: show aaa config

Назначение: Позволяет вывести на дисплей информацию коммутатора, характеризующую его как RADIUS-клиента.

Режим конфигурирования: Привилегированный режим

Описание: Выводит на дисплей информацию аутентификации AAA, информацию о включении учета сетевых сервисов, ключе аутентификации, сервере учета сетевых сервисов.

Пример:

```
Switch#show aaa config
```

21.1.21 show radius count

Синтаксис: show radius {authenticated-user | authenticating-user} count

Назначение: Выводит на дисплей статистику для пользователей RADIUS-аутентификации.

Параметры: **authenticated-user:** вывод информации об аутентифицированных онлайн-пользователях;

authenticating-user: вывод информации обо всех пользователях, проходящих аутентификацию.

Режим конфигурирования: Привилегированный режим

Описание: С помощью команды "show radius count" на дисплей может быть выведена статистика аутентифицированных пользователей RADIUS.

Пример:

Вывести на дисплей статистику пользователей, прошедших RADIUS-аутентификацию.

```
Switch #show radius authenticated-user count
The authenticated online user num is: 0
```

Вывести на дисплей статистику пользователей, прошедших RADIUS-аутентификацию и остальных пользователей.

```
Switch #sho radius authenticating-user count
```

22 Команды для настройки функции RA Security протокола IPv6

22.1.1 ipv6 security-ra enable

Синтаксис: `ipv6 security-ra enable`

no ipv6 security-ra enable

Назначение: Позволяет включить функцию RA security протокола IPv6 в глобальном режиме конфигурирования. Все сообщения с уведомлениями RA не будут передаваться через аппаратные средства, они будут только посылаться в CPU для обработки. Отмена команды **no ipv6 security-ra enable** выключает функцию RA security протокола IPv6 в глобальном режиме конфигурирования.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Функция RA security протокола IPv6 выключена.

Описание: Функция RA security протокола IPv6 в порту может быть включена только после того, как она включена в глобальном режиме конфигурирования. Если функция RA security протокола IPv6 выключена в глобальном режиме конфигурирования, станут неработоспособными и все настройки ее в портах.

Пример: Включить функцию RA security при IPv6 в глобальном режиме конфигурирования
`Switch(config)#ipv6 security-ra enable`

22.1.2 show ipv6 security-ra

Синтаксис: `show ipv6 security-ra [interface <interface-list>]`

Назначение: Выводит на дисплей информацию о всех интерфейсах, на которых включена функция IPv6 RA.

Параметры: Если команда введена без параметров будет выведена информация о всех небезопасных портах. Если параметр задан, будет выведена информация об указанном небезопасном порту.

Режим конфигурирования: Привилегированный режим

Пример:

```
Switch# show ipv6 security-ra
IPv6 security ra config and state information in the switch
Global IPv6 Security RA State: Enable
Ethernet0/0/1 IPv6 Security RA State: Yes
Ethernet0/0/3 IPv6 Security RA State: Yes
```

22.1.3 debug ipv6 security-ra

Синтаксис: `debug ipv6 security-ra`

no debug ipv6 security-ra

Назначение: Позволяет включить вывод отладочной информации функции RA security при IPv6. Отмена команды **no debug ipv6 security-ra** выключает вывод отладочной информации.

Режим конфигурирования: Привилегированный режим.

Параметры: Нет.

Описание: Команда позволяет проверить процесс обработки сообщений RA security при IPv6, что позволяет установить причины возникновения проблем.

Пример: Включить вывод отладочной информации RA security при IPv6.
`Switch#debug ipv security-ra`

23 Команды для настройки MAB

23.1.1 clear mac-authentication-bypass binding

Синтаксис: `clear mac-authentication-bypass binding {mac WORD | interface (ethernet IFNAME | IFNAME) | all}`

Назначение: Очищает информацию о привязках MAB.

Параметры: **mac:** удаление привязок MAB для указанного MAC-адреса; **IFNAME:** удаление привязок MAB для указанного интерфейса; **all:** удаление всех привязок.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#clear mac-authentication-bypass binding all
```

23.1.2 debug mac-authentication-bypass

Синтаксис: `debug mac-authentication-bypass {packet | event | binding}`

Назначение: Включает вывод отладочных сообщений MAB.

Параметры: **packet:** отладочные сообщения о пакетах MAB аутентификации; **event:** отладочные сообщения о событиях MAB аутентификации; **binding:** отладочные сообщения о привязках MAB аутентификации.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#debug mac-authentication-bypass packet
```

23.1.3 mac-authentication-bypass binding-limit

Синтаксис: `mac-authentication-bypass binding-limit <1-100>`

no mac-authentication-bypass binding-limit

Назначение: Устанавливает максимальное количество привязок MAB.

Параметры: **<1-100>:** количество привязок.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Три привязки.

Описание: Устанавливает максимальное количество привязок MAB. Если количество привязок достигнет максимума, новые привязки создаваться не будут. Если устанавливаемое значение меньше, чем текущее количество привязок, оно не будет принято.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#mac-authentication-bypass binding-limit 10
```

23.1.4 mac-authentication-bypass

Синтаксис: `mac-authentication-bypass enable`

no mac-authentication-bypass enable

Назначение: Включает глобально и на порту функцию MAB.

Режим конфигурирования: Глобальный режим конфигурирования и режим настройки порта.

Значение по умолчанию: Отключено.

Пример:

```
Switch(config)#mac-authentication-bypass enable
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#mac-authentication-bypass enable
```

23.1.5 mac-authentication-bypass guest-vlan

Синтаксис: `mac-authentication-bypass guest-vlan <1-4094>`

no mac-authentication-bypass guest-vlan

Назначение: Устанавливает гостевой vlan для MAB аутентификации.

Параметры: `<1-4094>`: ID гостевого vlan, в диапазоне от 1 до 4094.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Нет.

Описание: Устанавливает гостевой vlan для MAB аутентификации. Только на порту типа hybrid можно использовать данную команду. Если гостевой vlan сконфигурирован, то после неудачной MAB аутентификации, MAB пользователь может присоединиться к гостевому vlan.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#mac-authentication-bypass guest-vlan 10
```

23.1.6 mac-authentication-bypass timeout linkup-period

Синтаксис: `mac-authentication-bypass timeout linkup-period <0-30>`

no mac-authentication-bypass timeout linkup-period

Назначение: Устанавливает период между переключениями состояний down и up, когда привязка vlan на порту меняется, для гарантии того, что пользователь может получить IP-адрес снова.

Параметры: `<0-30>`: Интервал в секундах, по истечении которого, порт может перейти в состояние up, после автоматического выключения порта. 0 – отсутствие перехода.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 0.

Описание: В случае успешной MAB аутентификации, принадлежность к vlan определяется на основании настроек auto-vlan, если MAB аутентификация закончилась неуспешно, принадлежность к vlan определяется на основании настроек guest-vlan. Если период linkup установлен, то когда привязка интерфейса к vlan изменяется, порт будет выключен автоматически, и будет включен снова спустя установленный период.

Пример:

```
Switch(config)#mac-authentication-bypass timeout linkup-period 12
```

23.1.7 mac-authentication-bypass timeout offline-detect

Синтаксис: `mac-authentication-bypass timeout offline-detect {0 | <60-7200>}`

no mac-authentication-bypass timeout offline-detect

Назначение: Устанавливает offline-время определения MAB привязок.

Параметры: `{0 | <60-7200>}`: время определения MAB привязок.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 180 сек.

Описание: Если время определения установлено в 0, то коммутатор не определяет MAB привязки. Если время установлено в интервале от 60 до 7200 сек., то коммутатор периодически определяет потоки, соответствующие MAB привязке. Если поток не обнаружен за указанное время, привязка удаляется и данные перестают передаваться.

Пример:

```
Switch(config)#mac-authentication-bypass timeout offline-detect 200
```

23.1.8 mac-authentication-bypass timeout quiet-period

Синтаксис: `mac-authentication-bypass timeout quiet-period <1-60>`

no mac-authentication-bypass timeout quiet-period

Назначение: Устанавливает период тишины (quiet-period) MAB привязок.

Параметры: <1-60>: период тишины, в диапазоне от 1 до 60 сек.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 30 сек.

Описание: Если MAB аутентификация закончилась неуспешно, коммутатор не будет отвечать на запросы аутентификации с этого MAC-адреса. Спустя период тишины, коммутатор снова начнет отвечать на запросы аутентификации с этого MAC-адреса.

Пример:

```
Switch(config)#mac-authentication-bypass timeout quiet-period 60
```

23.1.9 mac-authentication-bypass timeout reauth-period

Синтаксис: mac-authentication-bypass timeout reauth-period <1-3600>

no mac-authentication-bypass timeout reauth-period

Назначение: Устанавливает интервал повторной аутентификации для состояния неудачной аутентификации.

Параметры: <1-3600>: интервал повторной аутентификации, в диапазоне от 1 до 3600 сек.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 30 сек.

Описание: В состоянии неудачной аутентификации, пользователь запрашивает повторную аутентификацию периодически до тех пор пока попытка не завершится успешно.

Пример:

```
Switch(config)#mac-authentication-bypass timeout reauth-period 20
```

23.1.10 mac-authentication-bypass timeout stale-period

Синтаксис: mac-authentication-bypass timeout stale-period <0-60>

no mac-authentication-bypass timeout stale-period

Назначение: Устанавливает период по прошествии которого удаляется привязка, после того, как MAB-порт перешел в состояние down.

Параметры: <0-60>: период до удаления, в диапазоне от 0 до 60 сек.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 30 сек.

Описание: Если установлено значение 0, то будут удалены все пользовательские привязки на данном порту как только порт перейдет в состояние down.

Пример:

```
Switch(config)#mac-authentication-bypass timeout stale-period 40
```

23.1.11 mac-authentication-bypass username-format

Синтаксис: mac-authentication-bypass username-format {mac-address | {fixed username WORD password WORD}}

Назначение: Устанавливает метод MAB-аутентификации.

Параметры: mac-address: использовать MAC-адрес в качестве имени пользователя и пароля; fixed username WORD password WORD: использовать указанные имя пользователя и пароль для аутентификации, длина имени пользователя и пароля от 1 до 32 символов.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Использовать MAC-адрес в качестве имени пользователя и пароля.

Пример:

```
Switch(config)#mac-authentication-bypass username-format fixed username mab-
user password mab-pwd
```

23.1.12 show mac-authentication-bypass

Синтаксис: show mac-authentication-bypass interface {ethernet IFNAME | IFNAME}

Назначение: Отображает информацию о MAB-аутентификации.

Параметры: {ethernet IFNAME | IFNAME}: имя порта.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show mac-authentication-bypass
```

```
The Number of all binding is 5
```

MAC	Interface	Vlan ID	State
00-11-22-6a-7f-88	Ethernet0/0/1	1	MAB_QUIET
00-12-22-6a-7f-88	Ethernet0/0/1	1	MAB_QUIET
00-13-22-6a-7f-88	Ethernet0/0/1	1	MAB_QUIET
00-14-22-6a-7f-88	Ethernet0/0/1	1	MAB_AUTHENTICATED

Отображаемая информация	Комментарий
The Number of all binding	Общее количество привязок
MAC	MAC-адрес
Interface	Порт, содержащий привязки
Vlan	Vlan к которому принадлежит пользователь
State	Состояние аутентификации

```
Switch#show mac-authentication-bypass int e0/0/1
```

```
Interface Ethernet0/0/1 user config:
```

```
MAB enable: Enable
```

```
Binding info: 1
```

```
MAB Binding built at SUN JAN 01 01:14:48 2006
```

```
VID 1, Port: Ethernet0/0/1
```

```
Client MAC: 00-22-33-6a-7f-8e
```

```
Binding State: MAB_AUTHENTICATED
```

```
Binding State Lease: 164 seconds left
```

Отображаемая информация	Комментарий
MAB enable	Состоянии MAB функционала
Binding info	Количество привязок на данном порту
MAB binding built at	Время создания привязки
VID	Vlan к которому принадлежит пользователь
Port	Порт привязки
Client MAC	MAC-адрес клиента
Binding State	Состояние аутентификации
Binding State Lease	Оставшееся время до окончания привязки

24 Команды для настройки MRPP

24.1.1 control-vlan

Синтаксис: control-vlan <vid>

no control-vlan

Назначение: Позволяет задать идентификатор VLAN ID для VLAN, управляющего кольцом MRPP. Отмена команды **no control-vlan** удаляет идентификатор VLAN ID для VLAN, управляющего кольцом MRPP.

Параметры: <vid>: идентификатор VLAN ID, в пределах от 1 до 4094.

Режим конфигурирования: Режим настройки кольца MRPP.

Значение по умолчанию: Нет.

Описание: Команда позволяет задать виртуальный VLAN ID для кольца MRPP, в настоящее время его значение должно быть в пределах 1-4094. Во избежание конфликтов рекомендуется, чтобы этот ID принадлежал VLAN, который еще не сконфигурирован и совпадал с ID кольца. При конфигурировании кольца MRPP одной и той же петли коммутаторов MRPP, VLAN ID управляющей VLAN на коммутаторах должны быть одинаковыми, в противном случае, все кольцо MRPP может работать неправильно, либо возникнет broadcast-шторм. Для того, чтобы команда control-vlan была работоспособной, предварительно должна быть введена команда mrpp enable.

Если после ввода команды control-vlan сконфигурированы первичный и вторичный порты, режим портов и введена команда enable, то тем самым будет включена функция mrpp-ring.

Пример: Для кольца mrpp 4000 назначить VLAN 4000.

```
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
```

24.1.2 clear mrpp statistics

Синтаксис: clear mrpp statistics [<ring-id>]

Назначение: Очищает статистику принимаемых и передаваемых пакетов MRPP в кольце MRPP.

Параметры: <ring-id>: идентификатор (ID) кольца MRPP, в пределах от 1 до 4094. Если ID не указан, будет очищена статистическая информация всех колец MRPP.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Нет.

Описание: Нет.

Пример: Очистить статистическую информацию кольца MRPP 4000 на коммутаторе.

```
Switch#clear mrpp statistics 4000
```

24.1.3 debug mrpp

Синтаксис: debug mrpp

no debug mrpp

Назначение: Выводит на дисплей отладочную информацию MRPP. Отмена команды **no description** прекращает вывод на дисплей отладочной информации MRPP.

Режим конфигурирования: Привилегированный режим.

Параметры: Нет.

Описание: Команда позволяет вывести на дисплей отладочную информацию MRPP, проверить обработку сообщений протокола MRPP, процесс приема пакетных данных.

Пример: Вывести на дисплей отладочную информацию MRPP.

```
Switch#debug mrpp
```

24.1.4 enable

Синтаксис: `enable`

`no enable`

Назначение: Позволяет включить сконфигурированное кольцо MRPP. Отмена команды `no enable` выключает кольцо MRPP.

Режим конфигурирования: Режим настройки кольца MRPP.

Значение по умолчанию: Кольцо MRPP выключено.

Описание: Перед вводом этой команды необходимо включить протокол MRPP. Если кольцо MRPP уже сконфигурировано соответствующими командами, то команда `enable` включит его.

Пример: Сконфигурировать кольцо MRPP 4000 коммутатора в первичном узле и включить его.

```
Switch(config)#mrpp enable
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#node-mode master
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 6
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/25)#mrpp ring 4000 primary-port
Switch(config)#interface ethernet 0/0/3
Switch(config-If-Ethernet0/0/26)#mrpp ring 4000 secondary-port
```

24.1.5 fail-timer

Синтаксис: `fail-timer <timer>`

`no fail-timer`

Назначение: Позволяет задать таймер получения пакетов Hello в первичном узле кольца MRPP. Отмена команды `no fail-timer` восстанавливает значение таймера, заданное по умолчанию.

Параметры: `<timer>`: значение таймера, в пределах от 1 до 300 с.

Режим конфигурирования: Режим настройки кольца MRPP.

Значение по умолчанию: 3 с.

Описание: Если первичный узел кольца MRPP не примет пакет Hello от первичного порта первичного узла в течение интервала таймера, то кольцо считается неработоспособным. На промежуточных узлах кольца MRPP задавать этот таймер не требуется. Во избежание задержки передачи пакетов Hello промежуточным узлом, значение таймера должно быть, как минимум, втрое больше таймера Hello. Из-за задержки в кольце необходимо изменить значение таймера, заданное по умолчанию. Необходимо увеличить его и установить таким, чтобы не создавалось ситуаций, когда таймер уже истек, а первичный узел еще не принял пакета Hello из-за задержки в кольце.

Пример: Установить fail-timer кольца MRPP 4000 равным 10 с.

```
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#fail-timer 10
```

24.1.6 hello-timer

Синтаксис: `hello-timer <timer>`

`no hello-timer`

Назначение: Позволяет задать таймер передачи пакетов Hello из первичного узла кольца MRPP. Отмена команды `no hello-timer` восстанавливает значение таймера, заданное по умолчанию.

Параметры: `<timer>`: значение таймера, в пределах от 1 до 300 с.

Режим конфигурирования: Режим настройки кольца MRPP.

Значение по умолчанию: 1 с.

Описание: Первичный узел кольца MRPP регулярно передает пакеты Hello (через интервал таймера Hello). Если вторичному порту первичного узла удастся принять эти пакеты в течение заданного периода времени, кольцо считается работоспособным (в противном случае – неработоспособным). На промежуточных узлах кольца MRPP задавать этот таймер не требуется.

Пример: Установить таймер hello кольца MRPP 4000 равным 3 с.

```
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#hello-timer 3
```

24.1.7 mrpp enable

Синтаксис: mrpp enable

no mrpp enable

Назначение: Позволяет включить модуль протокола MRPP. Отмена команды **no mrpp enable** выключает протокол MRPP.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Модуль протокола MRPP не включен.

Описание: Если необходимо сконфигурировать кольцо MRPP, должен быть включен протокол MRPP. Команда позволяет включить этот протокол.

Пример: Включить MRPP в глобальном режиме конфигурирования.

```
Switch(config)#mrpp enable
```

24.1.8 mrpp poll-time

Синтаксис: mrpp poll-time <20-2000>

Назначение: Позволяет установить интервал опроса MRPP.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Позволяет задать интервал опроса для корректировки времени опроса MRPP.

Пример:

```
Switch(Config)# mrpp poll-time 200
```

24.1.9 mrpp ring

Синтаксис: mrpp ring <ring-id>

no mrpp ring <ring-id>

Назначение: Позволяет создать кольцо MRPP и включить режим кольца MRPP. Отмена команды **no mrpp ring<ring-id>** удаляет сконфигурированное кольцо MRPP.

Параметры: <ring-id>: идентификатор (ID) кольца MRPP, в пределах от 1 до 4096.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Если данное кольцо MRPP не существует, будет создано новое кольцо и включен режим кольца MRPP.

Пример:

```
Switch(config)#mrpp ring 100
```

24.1.10 mrpp ring primary-port

Синтаксис: mrpp ring <ring-id> primary-port

no mrpp ring <ring-id> primary-port

Назначение: Позволяет задать первичный порт кольца MRPP.

Параметры: <ring-id>: идентификатор (ID) кольца MRPP, в пределах <1-4096>.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Нет.

Описание: Команда позволяет задать первичный порт кольца MRPP. Первичный узел отправляет пакеты Hello через первичный порт. Вторичный порт принимает пакеты Hello, посылаемые первичным узлом. Первичный и вторичный порты вторичного узла работают одинаково.

Команда `mrpp enable` должна быть введена до ввода команды `control-vlan`, иначе эта последняя команда будет неработоспособна. Если после ввода команды `control-vlan` сконфигурированы первичный и вторичный порты, режим портов и введена команда `enable`, то тем самым будет включена функция `mrpp-ring`.

Пример: Установить порт Ethernet 0/0/25 как первичный порт кольца MRPP 4000.

```
Switch(Config)#interface ethernet 0/0/25
Switch(config-If-Ethernet0/0/25)#mrpp ring 4000 primary-port
```

24.1.11 mrpp ring secondary-port

Синтаксис: `mrpp ring <ring-id> secondary-port`

по `mrpp ring <ring-id> secondary-port`

Назначение: Позволяет задать вторичный порт кольца MRPP.

Параметры: `<ring-id>`: идентификатор (ID) кольца MRPP, в пределах `<1-4096>`.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Нет.

Описание: Команда позволяет задать вторичный порт кольца MRPP. Первичный узел использует вторичный порт для приема пакетов Hello от первичного узла. Первичный и вторичный порты вторичного узла работают одинаково.

Команда `mrpp enable` должна быть введена до ввода команды `control-vlan`, иначе эта последняя команда будет неработоспособна. Если после ввода команды `control-vlan` сконфигурированы первичный и вторичный порты, режим портов и введена команда `enable`, то тем самым будет включена функция `mrpp-ring`.

Пример: Установить порт 0/0/26 как вторичный порт кольца MRPP.

```
Switch(config)#interface ethernet0/0/26
Switch(Config-If-Ethernet0/0/26)#mrpp ring 4000 secondary-port
```

24.1.12 node-mode

Синтаксис: `node-mode {maser | transit}`

Назначение: Позволяет задать тип узла кольца MRPP (первичный узел или вторичный узел).

Параметры: `master`: первичный узел;

`transit`: вторичный узел.

Режим конфигурирования: Режим настройки кольца MRPP.

Значение по умолчанию: Вторичный узел.

Пример: Установить коммутатор, как первичный узел кольца MRPP 4000.

```
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#node-mode master
```

24.1.13 show mrpp

Синтаксис: `show mrpp [ring-id>]`

Назначение: Позволяет вывести на дисплей информацию о настройках кольца MRPP.

Параметры: `<ring-id>`: идентификатор (ID) кольца MRPP, в пределах от 1 до 4096. Если ID не указан, будет выведена информация о настройках всех колец MRPP.

Режим конфигурирования: Привилегированный режим.

Пример: Вывести на дисплей информацию о настройках кольца MRPP 4000.

```
Switch# show mrpp 4000
```

24.1.14 show mrpp statistics

Синтаксис: `show mrpp statistics [<ring-id>]`

Назначение: Позволяет вывести на дисплей информацию о переданных и принятых пакетах кольца MRPP.

Параметры: `<ring-id>`: идентификатор (ID) кольца MRPP, в пределах от 1 до 4096. Если ID не задан будут выведена статистическая информация для всех колец MRPP.

Режим конфигурирования: Привилегированный режим.

Пример: Вывести на дисплей статистическую информацию кольца MRPP 4000 на коммутаторе.

```
Switch#show mrpp statistic 4000
```

25 Команды для настройки ULPP

25.1.1 clear ulpp flush counter interface

Синтаксис: `clear ulpp flush counter interface <name>`

Назначение: Очищает статистику flush-пакетов.

Параметры: `<name>`: имя порта.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Нет.

Пример:

```
Switch#clear ulpp flush counter interface e0/0/1
ULPP flush counter has been reset.
```

25.1.2 control-vlan

Синтаксис: `control-vlan <vid>`

`no control-vlan`

Назначение: Позволяет задать идентификатор VLAN ID, управляющего группой ULPP.

Параметры: `<vid>`: идентификатор VLAN ID, в котором отправляются flush-пакеты, значение в пределах от 1 до 4094.

Режим конфигурирования: Режим настройки группы ULPP.

Значение по умолчанию: 1.

Описание: Команда позволяет задать VLAN ID для группы ULPP. Этот VLAN ID должен соответствовать VLAN, который был ранее создан, после чего этот VLAN не может быть удален. Также, данный VLAN должен быть VLAN ID, защищаемый ULPP группой во избежании возникновения петли flush-пакетов.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#control vlan 10
```

25.1.3 debug ulpp error

Синтаксис: `debug ulpp error`

`no debug ulpp error`

Назначение: Выводит на дисплей отладочную информацию об ошибках ULPP.

Режим конфигурирования: Привилегированный режим.

Параметры: Нет.

Пример:

```
Switch#debug ulpp error
Unrecognized Flush packet received
```

25.1.4 debug ulpp event

Синтаксис: `debug ulpp event`

`no debug ulpp event`

Назначение: Выводит на дисплей отладочную информацию о событиях ULPP.

Режим конфигурирования: Привилегированный режим.

Параметры: Нет.

Пример:

```
Switch#debug ulpp event
```

ULPP group 1 state changes:

Master port ethernet 0/0/1 in ULPP group 1 changed state to Forwarding.

Slave port ethernet 0/0/2 in ULPP group 1 changed state to Standby.

25.1.5 debug ulpp flush content interface

Синтаксис: `debug ulpp flush content interface <name>`

`no debug ulpp flush content interface <name>`

Назначение: Выводит на дисплей информацию, содержащуюся в полученных flush-пакетах ULPP.

Режим конфигурирования: Привилегированный режим.

Параметры: `<name>`: имя порта.

Пример:

```
Switch#debug ulpp flush content interface e0/0/1
Flush packet content:
Destination MAC: 00-33-ff-cc-cc-cc
Source MAC: 00-aa-cc-d7-5c-ea
Type: 8100
Vlan ID: 1
Length: 518
Control Type: 2
Control Vlan: 10
MAC number:0
Vlan Bitmap:
```

25.1.6 debug ulpp flush {send | receive} interface

Синтаксис: `debug ulpp flush {send | receive} interface <name>`

`no debug ulpp flush {send | receive} interface <name>`

Назначение: Выводит на дисплей информацию о переданных и полученных flush-пакетах ULPP. Детальная информация не выводится.

Режим конфигурирования: Привилегированный режим.

Параметры: `<name>`: имя порта; **send**: выводить информацию только о переданных flush-пакетах ULPP; **receive**: выводить информацию только о принятых flush-пакетах ULPP.

Пример:

```
Switch#debug ulpp flush send interface e0/0/1
Flush packet send on port Ethernet 0/0/1.
```

25.1.7 description

Синтаксис: `description <string>`

`no description`

Назначение: Задаёт описание для ULPP группы.

Режим конфигурирования: Режим настройки ULPP группы.

Параметры: `<string>`: имя ULPP группы, не более 128 символов.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#description testgroup
```

25.1.8 flush disable arp

Синтаксис: `flush disable arp`

Назначение: Отключает отправку flush-пакетов об удалении ARP.

Режим конфигурирования: Режим настройки ULPP группы.

Значение по умолчанию: Отправка включена.

Описание: Данная команда позволяет отключить отправку flush-пакетов, инициализирующих удаление записей ARP, вышестоящему коммутатору, которая производится, если произошло переключение линии.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#flush disable arp
```

25.1.9 flush disable mac

Синтаксис: flush disable mac

Назначение: Отключает отправку flush-пакетов об обновлении таблицы MAC-адресов.

Режим конфигурирования: Режим настройки ULPP группы.

Значение по умолчанию: Отправка включена.

Описание: Данная команда позволяет отключить отправку flush-пакетов, инициализирующих обновление таблицы MAC-адресов, вышестоящему коммутатору, которая производится, если произошло переключение линии.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#flush disable mac
```

25.1.10 flush enable arp

Синтаксис: flush enable arp

Назначение: Включает отправку flush-пакетов об удалении ARP.

Режим конфигурирования: Режим настройки ULPP группы.

Значение по умолчанию: Отправка включена.

Описание: Данная команда позволяет включить отправку flush-пакетов, инициализирующих удаление записей ARP, вышестоящему коммутатору, которая производится, если произошло переключение линии.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#flush enable arp
```

25.1.11 flush enable mac

Синтаксис: flush enable mac

Назначение: Включает отправку flush-пакетов об обновлении таблицы MAC-адресов.

Режим конфигурирования: Режим настройки ULPP группы.

Значение по умолчанию: Отправка включена.

Описание: Данная команда позволяет включить отправку flush-пакетов, инициализирующих обновление таблицы MAC-адресов, вышестоящему коммутатору, которая производится, если произошло переключение линии.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#flush enable mac
```

25.1.12 preemption delay

Синтаксис: preemption delay <integer>

no preemption delay

Назначение: Задает время задержки приоритетного переключения.

Параметры: <integer>: задержка, в диапазоне от 1 до 600 сек.

Режим конфигурирования: Режим настройки ULPP группы.

Значение по умолчанию: 60 сек.

Описание: Данная команда задает время задержки перед переключением с slave-порта на master-порт. Данная команда имеет силу, только когда введена команда `preemption mode`.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#preemption delay 50
```

25.1.13 preemption mode

Синтаксис: `preemption mode`

no preemption mode

Назначение: Включает/выключает режим приоритетного переключения.

Режим конфигурирования: Режим настройки ULPP группы.

Значение по умолчанию: Переключение не производится.

Описание: Когда slave-порт находится в состоянии передачи (`forwarding state`) и master-порт в резервном состоянии (`standby state`), то master-порта возвращается в состояние передачи, а slave-порт – в резервное состояние, только спустя время, заданное командой `preemption delay`.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#preemption mode
```

25.1.14 protect vlan-reference-instance

Синтаксис: `protect vlan-reference-instance <instance-list>`

no protect vlan-reference-instance <instance-list>

Назначение: Задает VLAN, защищаемые ULPP группой.

Параметры: `<instance-list>`: список MSTP экземпляров связующего дерева (`instance`).

Режим конфигурирования: Режим настройки ULPP группы.

Значение по умолчанию: Защита VLAN не производится.

Описание: Данная команда задает VLAN, защищаемые ULPP группой. Данные VLAN передаются через один из портов ULPP группы и заблокированы на другом порту. Каждая ULPP группа может ссылаться на все экземпляры связующего дерева. Различные ULPP группы не могут ссылаться на одни и те же экземпляры связующего дерева.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#protect vlan-reference-instance 1
```

25.1.15 show ulpp flush counter interface

Синтаксис: `show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}`

Назначение: Выводит на дисплей статистику о переданных и полученных flush-пакетах ULPP.

Режим конфигурирования: Привилегированный режим.

Параметры: `<IFNAME>`: имя порта.

Описание: Выводит на дисплей статистику о flush-пакетах - сколько пакетов было получено и время получения пакетов.

Пример:

```
Switch#show ulpp flush counter interface e0/0/1
Received flush packets: 10
```

25.1.16 show ulpp flush-receive-port

Синтаксис: show ulpp flush-receive-port

Назначение: Выводит на дисплей информацию о порте, получившем flush-пакет и тип пакета и управляющий VLAN.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show ulpp flush-receive-port
ULPP flush-receive portlist:
Portname          Type   Control  Vlan
-----
Ethernet0/0/1     ARP    1
Ethernet0/0/3     MAC    1;3;5-10
```

25.1.17 show ulpp group

Синтаксис: show ulpp group [group-id]

Назначение: Выводит на дисплей информацию о сконфигурированных ULPP группах.

Режим конфигурирования: Привилегированный режим.

Параметры: group-id: информация о указанной группе.

Описание: Выводит на дисплей информацию о сконфигурированных ULPP группах – состояние портов, режим переключения, задержку переключения.

Пример:

```
Switch#show ulpp group 1
ULPP group 1 information:
Description: abc
Preemption mode: on
Preemption delay: 30s
Control VLAN:1
Protected VLAN: Reference Instance 1
Member          Role          State
-----
Ethernet0/0/1   MASTER       FORWARDING
Ethernet0/0/2   SLAVE        STANDBY
```

25.1.18 ulpp control vlan

Синтаксис: ulpp control vlan <vlan-list>

no ulpp control vlan <vlan-list>

Назначение: Задаёт список управляющих VLAN, которые принимают flush-пакеты.

Параметры: <vlan-list>: список управляющих VLAN.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: VLAN 1.

Описание: Данная команда должна ссылаться на существующие VLAN. После ввода команды, эти VLAN не могут быть удалены.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#ulpp control vlan 10
```

25.1.19 ulpp flush disable arp

Синтаксис: ulpp flush disable arp

Назначение: Отключает прием flush-пакетов об удалении ARP.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Прием отключен.

Описание: Данная команда позволяет отключить прием flush-пакетов об удалении ARP на порту.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#ulpp flush disable arp
```

25.1.20 ulpp flush disable mac

Синтаксис: ulpp flush disable mac

Назначение: Отключает прием flush-пакетов об обновлении таблицы MAC-адресов.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Прием отключен.

Описание: Данная команда позволяет отключить прием flush-пакетов об обновлении таблицы MAC-адресов на порту.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#ulpp flush disable mac
```

25.1.21 ulpp flush enable arp

Синтаксис: ulpp flush enable arp

Назначение: Включает прием flush-пакетов об удалении ARP.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Прием отключен.

Описание: Данная команда позволяет включить прием flush-пакетов об удалении ARP на порту.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#ulpp flush enable arp
```

25.1.22 ulpp flush enable mac

Синтаксис: ulpp flush enable mac

Назначение: Включает прием flush-пакетов об обновлении таблицы MAC-адресов.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Прием отключен.

Описание: Данная команда позволяет включить прием flush-пакетов об обновлении таблицы MAC-адресов на порту.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#ulpp flush enable mac
```

25.1.23 ulpp group

Синтаксис: ulpp group <integer>

no ulpp group <integer>

Назначение: Создает ULPP группу.

Параметры: <integer>: идентификатор ULPP группы, от 1 до 48.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Группы не созданы.

Описание: Если группа существует, то данная команда позволяет перейти в режим конфигурирования группы.

Пример:

```
Switch(config)#ulpp group 20
Switch(ulpp-group-20)#
```

25.1.24 ulpp group master

Синтаксис: `ulpp group <integer> master`

`no ulpp group <integer> master`

Назначение: Задает master-порт ULPP группы.

Параметры: `<integer>`: идентификатор ULPP группы, от 1 до 48.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: master-порт не задан.

Описание: Последовательность определения master-порта и slave-порта в группе не важна, но защищаемые группой VLAN должны быть определены до конфигурации портов. В каждой группе может быть только один master-порт.

Пример:

```
Switch(config)#interface ethernet 0/0/1
Switch(config-If-Ethernet0/0/1)#ulpp group 20 master
```

25.1.25 ulpp group slave

Синтаксис: `ulpp group <integer> slave`

`no ulpp group <integer> slave`

Назначение: Задает slave-порт ULPP группы.

Параметры: `<integer>`: идентификатор ULPP группы, от 1 до 48.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: slave-порт не задан.

Описание: Последовательность определения master-порта и slave-порта в группе не важна, но защищаемые группой VLAN должны быть определены до конфигурации портов. В каждой группе может быть только один slave-порт.

Пример:

```
Switch(config)#interface ethernet 0/0/2
Switch(config-If-Ethernet0/0/2)#ulpp group 20 slave
```

26 Команды для настройки ULSM

26.1.1 debug ulsm event

Синтаксис: debug ulsm event

no debug ulsm event

Назначение: Выводит на дисплей отладочную информацию о событиях ULSM.

Режим конфигурирования: Привилегированный режим.

Параметры: Нет.

Пример:

```
Switch#debug ulsm event
Downlink synchoronized with ULSM group, change state to Down.
```

26.1.2 show ulsm group

Синтаксис: show ulsm group [group-id]

Назначение: Выводит на дисплей информацию о сконфигурированных ULSM группах.

Режим конфигурирования: Привилегированный режим.

Параметры: group-id: информация о указанной группе.

Описание: Выводит на дисплей информацию о сконфигурированных ULSM группах.

Пример:

```
Switch#show ulsm group 1
ULSM group 1 information:
ULSM group state: Down
Member          Role          State          Down by ULSM
-----
ethernet0/0/1   UpLINK        Down
ethernet0/0/2   DownLINK      Down           Yes
```

26.1.3 ulsm group

Синтаксис: ulsm group <group-id>

no ulsm group <group-id>

Назначение: Создает ULSM группу.

Параметры: <group-id>: идентификатор ULSM группы, от 1 до 32.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Группы не созданы.

Пример:

```
Switch(config)#ulsm group 10
```

26.1.4 ulsm group {uplink | downlink}

Синтаксис: ulsm group <group-id> {uplink | downlink}

no ulsm group <group-id>

Назначение: Задаёт uplink и downlink порты в ULSM группе.

Параметры: <group-id>: идентификатор ULSM группы, от 1 до 32; **uplink**: uplink порт в группе; **downlink**: downlink порт в группе.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Порты не принадлежат ULSM группе.

Описание: В каждой ULSM группе может быть до 8 uplink-портов и до 16 downlink-портов.

Пример:

```
Switch(config)#interface ethernet 0/0/3  
Switch(config-If-Ethernet0/0/3)#ulsm group 10 uplink
```

27 Команды для настройки PPPoE Intermediate Agent

27.1.1 debug pppoe-ia

Синтаксис: `debug pppoe-ia packet {receive | send} interface ethernet <interface-name>`

`no debug pppoe-ia packet {receive | send} interface ethernet <interface-name>`

Назначение: Включает вывод отладочных сообщений для пакетов PPPoE.

Параметры: **receive:** отладочные сообщения о принятых пакетах PPPoE; **send:** отладочные сообщения об отправленных пакетах PPPoE; **ethernet:** порт; **interface-name:** имя порта.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Вывод отладочных сообщений выключен.

Пример:

```
Switch#debug pppoe-ia packet send interface ethernet 0/0/2
```

27.1.2 pppoe intermediate-agent

Синтаксис: `pppoe intermediate-agent`

`no pppoe intermediate-agent`

Назначение: Включает функционал PPPoE intermediate agent глобально.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: PPPoE intermediate agent выключен.

Описание: После включения, коммутатор начинает обрабатывать пакеты инициализации PPPoE (discovery stage) в соответствии с введенной конфигурацией.

Пример:

```
Switch(config)#pppoe intermediate agent
```

27.1.3 pppoe intermediate-agent (для порта)

Синтаксис: `pppoe intermediate-agent`

`no pppoe intermediate-agent`

Назначение: Включает функционал PPPoE intermediate agent на порту.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: PPPoE intermediate agent выключен.

Описание: После включения, коммутатор начинает добавлять vendor-тег в пакеты PPPoE на данном порту. Обратите внимание:

1. PPPoE intermediate agent должен быть включен глобально;
2. Как минимум один порт коммутатора должен быть подключен к PPPoE-серверу и этот порт должен быть в режиме trust.

Пример:

```
Switch(config-if-ethernet0/0/2)#pppoe intermediate agent
```

27.1.4 pppoe intermediate-agent access-node-id

Синтаксис: `pppoe intermediate-agent access-node-id <string>`

`no pppoe intermediate-agent access-node-id`

Назначение: Задаёт значение поля access-node-id в circuit-id в добавляемом vendor-теге.

Параметры: **string:** access-node-id, максимальное количество символов 47 байт.

Режим конфигурирования: Глобальный режим конфигурирования.

27.1.7 pppoe intermediate-agent trust

Синтаксис: pppoe intermediate-agent trust

no pppoe intermediate-agent trust

Назначение: Переводит порт в режим trust.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Порт находится в режиме untrust.

Описание: Порт, к которому подключен PPPoE-сервер должен работать в режиме trust.

Пример:

```
Switch(config-if-ethernet0/0/1)#pppoe intermediate-agent trust
```

27.1.8 pppoe intermediate-agent vendor-tag strip

Синтаксис: pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

Назначение: Включает режим удаление vendor-тега из пакета PPPoE.

Режим конфигурирования: Режим настройки порта.

Значение по умолчанию: Удаление не производится.

Описание: Если пакет, полученный от PPPoE-сервера, содержит vendor-тег, то этот тег будет удален.

1. Функционал pppoe intermediate-agent должен быть включен глобально
2. Данный порт должен работать в режиме trust.

Пример:

```
Switch(config-if-ethernet0/0/1)#pppoe intermediate-agent trust
Switch(config-if-ethernet0/0/1)#pppoe intermediate-agent vendor-tag strip
```

27.1.9 show pppoe intermediate-agent access-node-id

Синтаксис: show pppoe intermediate-agent access-node-id

Назначение: Отображает значение access-node-id.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#pppoe intermediate-agent access-node-id switch1
Switch#show pppoe intermediate-agent access-node-id
pppoe intermediate-agent access-node-id is : switch1
```

27.1.10 show pppoe intermediate-agent identifier-string option delimiter

Синтаксис: show pppoe intermediate-agent identifier-string option delimiter

Назначение: Отображает значение access-node-id и формат комбинации для слота, порта, vlan.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#pppoe intermediate-agent identifier-string switch1 option spv
delimiter # delimiter /
Switch#show pppoe intermediate-agent identifier-string option delimiter
config identifier string is : switch1
config option is : slot , port and vlan
the first delimiter is : "# "
the second delimiter is : "/" "
```

27.1.11 show pppoe intermediate-agent info

Синтаксис: show pppoe intermediate-agent info [interface ethernet <interface-name>]

Назначение: Отображает настройки pppoe intermediate-agent для всех портов или для указанного порта.

Параметры: ethernet: порт; <interface-name>: имя порта.

Режим конфигурирования: Привилегированный режим.

Описание: Отображает текущие настройки pppoe intermediate-agent для порта. Режим работы trust/untrust, производится ли удаление vendor-тега, значения circuit ID and remote ID.

Пример:

```
Switch# show pppoe intermediate-agent info interface ethernet 0/0/2
Interface    IA      Trusted  vendor Strip  Rate limit  circuit id remote id
-----
Ethernet0/0/2  yes      no       no         no          test1/port1  host1
```

28 Команды для настройки зеркалирования портов

28.1.1 monitor session source interface

Синтаксис: `monitor session <session> source interface <interface-list>{rx| tx| both}`

`no monitor session <session> source interface <interface-list>`

Назначение: Позволяет задать интерфейс-источник для зеркального порта. Отмена команды `no monitor session <session> source interface <interface-list>` удаляет эту настройку.

Параметры: **<session>**: номер сеанса для порта-источника зеркального порта. В настоящее время поддерживается только 1 сеанс.

<interface-list>: список портов-источников зеркального порта, в качестве разделителей в списке можно использовать специальные символы, например "-", ",";

rx: поток, принятый от порта-источника;

tx: поток, посланный с порта-источника;

both: оба потока (принятый портом-источником и посланный с него).

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Эта команда используется для настройки интерфейсов-источников зеркала. На порт-источник в коммутаторах не накладывается никаких ограничений - это может быть один интерфейс, либо множество интерфейсов; могут зеркалироваться не только потоки, принимаемые и посылаемые портом-источником, но также принятые и посланные потоки, доступные на единственном порте-источнике. Если ключевое слово [rx | tx | both] не указано, по умолчанию системой выбирается опция both.

Пример: Настроить зеркалирование потока, посланного интерфейсами 0/0/1-4.

```
Switch(config)#monitor session 1 source interface ethernet 0/0/1-4 rx
```

28.1.2 monitor session source interface access-list

Синтаксис: `monitor session <session> source {interface <interface-list>} access-list <num> {rx}`

`no monitor session <session> source {interface <interface-list>} access-list <num>`

Назначение: Позволяет задать список доступа для управления источником зеркального порта. Отмена команды `no monitor session <session> source {interface <interface-list>} access-list <num>` удаляет эту настройку.

Параметры: **<session>**: номер сеанса для зеркального порта. В настоящее время поддерживается только 1 сеанс.

<interface-list>: список интерфейсов источника зеркального порта. В списке можно использовать символы-разделители "-" и ",".

<num>: номер списка доступа.

rx: фильтрация данных, принятых интерфейсом.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Эта команда используется для настройки интерфейсов-источников зеркала. На порт-источник в коммутаторах не накладывается никаких ограничений - это может быть один интерфейс, либо множество интерфейсов. При зеркалировании потоков могут зеркалироваться только принятые данные. Параметры могут быть опущены. Список доступа, используемый в команде, должен быть подготовлен до ее ввода. Настройка списков доступа описана в соответствующей главе. Зеркальный порт может быть создан только после того, как будут заданы интерфейс назначения и соответствующий сеанс.

Пример: Задать на зеркальном интерфейсе 0/0/6 фильтрацию пакетов в соответствии со списком доступа 120 в сеансе 1.

```
Switch(config)#monitor session 1 source interface 0/0/6 access-list 120 rx
```

28.1.3 monitor session destination interface

Синтаксис: `monitor session <session> destination interface <interface-number>`

`no monitor session <session> destination interface <interface-number>`

Назначение: Позволяет задать интерфейс назначения зеркала. Отмена команды `no monitor session <session> destination interface <interface-number>` удаляет эту настройку.

Параметры: `<session>`: номер сеанса зеркала, в настоящее время поддерживается только один сеанс.

`<interface-number>`: интерфейс назначения зеркала.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Коммутатором поддерживается только один интерфейс назначения зеркала. Интерфейс, который задан в качестве интерфейса назначения зеркала, не должен являться членом магистральной группы (trunk) интерфейсов. Рекомендуется, чтобы максимальная пропускная способность интерфейса назначения была больше суммы пропускных способностей интерфейсов-источников зеркала.

Пример: Задать интерфейс 0/0/7 в качестве интерфейса назначения зеркала.
`Switch(config)#monitor session 1 destination interface ethernet 0/0/7`

28.1.4 show monitor

Синтаксис: `show monitor`

Назначение: Выводит на дисплей информацию об источнике зеркала и о зеркальном порту.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей информацию об источнике зеркала и о зеркальном порту.

Пример:
`Switch#show monitor`
`monitor session 1:`

```
source ports:  
RX port: 8  
TX port: 8  
Flow monitor source:
```

```
Destination Ethernet0/0/16, output packet preserve tag  
-----
```

29 Команды для настройки SNTP

29.1.1 debug sntp

Синтаксис: `debug sntp {adjust | packet | select }`

`no debug sntp {adjust | packet | select}`

Назначение: Выводит на дисплей отладочную информацию SNTP, либо прекращает ее вывод на дисплей.

Параметры: `adjust`: информация подстройки часов SNTP;

`packet`: SNTP-пакеты,

`select`: выбор часов SNTP.

Режим конфигурирования: Привилегированный режим.

Пример: Вывести на дисплей отладочную информацию для SNTP-пакетов.

```
Switch#debug sntp packet
```

29.1.2 sntp server

Синтаксис: `sntp server {<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]`

`no sntp server {<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]`

Назначение: Позволяет указать сервер времени как источник синхронизации.

Параметры: `<ip-address>`: IPv4-адрес сервера времени; `<ipv6-address>`: IPv6-адрес сервера времени; `source`: интерфейс для выбора источника IP-адреса; `vlan <vlan no>`: идентификатор интерфейса vlan; `loopback <loopback no>`: идентификатор интерфейса loopback; `version <version_no>`: номер версии сервера, в пределах 1-4, по умолчанию 4.

Значение по умолчанию: Сервер времени не задан.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример:

```
Switch(config)#sntp server 1.1.1.1 source vlan 1
```

29.1.3 sntp polltime

Синтаксис: `sntp polltime <interval>`

`no sntp polltime`

Назначение: Позволяет задать интервал отправки запросов на NTP/SNTP-сервер. Отмена команды `no sntp polltime` отменяет настройки для интервала опроса и восстанавливает значение, заданное по умолчанию.

Параметры: `<interval>`: значение интервала, в пределах от 16 до 16284 секунд.

Значение по умолчанию: 64 секунды.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Задать отправку клиентом запросов на сервер каждые 128 секунд.

```
Switch#config Switch(config)#sntp polltime 128
```

29.1.4 sntp timezone

Синтаксис: `sntp timezone <name> [{add | subtract}] [<time_difference>]`

`no sntp timezone`

Назначение: Позволяет задать временной сдвиг часового пояса (относительно UTC), в котором находится клиент. Отмена команды `no sntp timezone` отменяет настройки часового пояса и восстанавливает настройки по умолчанию.

Параметры: <name>: строка с именем часового пояса, допустимая длина — не более 16 символов;

<add>: время в часовом поясе = UTC + <time_difference>;

<subtract>: время в часовом поясе = UTC - <time_difference>;

<time-difference>: сдвиг по времени, в пределах от 0 до 12. (относительно времени UTC).

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Установить пользовательский часовой пояс для Москвы (UTC+3).

```
Switch(config)#sntp timezone Moscow add 3
```

29.1.5 show sntp

Синтаксис: show sntp

Назначение: Позволяет вывести на дисплей текущие настройки SNTP-клиента и состояние сервера.

Параметры: нет.

Режим конфигурирования: Привилегированный режим.

Пример: Вывести на дисплей текущие настройки SNTP.

```
Switch#show sntp
SNTP server    Version    Last Receive
2.1.1.0.2      1          6
```

30 Команды для настройки NTP

30.1.1 ntp enable

Синтаксис: ntp enable

ntp disable

Назначение: Позволяет включить или выключить функцию NTP в глобальном режиме конфигурирования.

Параметры: Нет.

Значение по умолчанию: Функция выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Включить функцию NTP.

```
Switch(config)#ntp enable
```

30.1.2 ntp server

Синтаксис: ntp server {<ip-address> | <ipv6-address>} [version <version_no>] [key <key-id>]

no ntp server {<ip-address>| <ipv6-address>}

Назначение: Позволяет указать в команде NTP-сервер. Отмена команды **no ntp server** {<ip-address> | <ipv6-address>} выключает указанный в команде NTP-сервер.

Параметры: ip-address: IPv4-адрес сервера времени.

ipv6-address: IPv6-адрес сервера времени.

version: информация о версии, заданной на сервере.

version_no: номер версии сервера, в пределах от 1 до 4, по умолчанию 4.

key: включение настройки ключа на сервере.

key-id: идентификатор ключа.

Значение по умолчанию: Функция выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Задать на коммутаторе адрес сервера времени 1.1.1.1

```
Switch(config)#ntp server 1.1.1.1
```

30.1.3 ntp broadcast server count

Синтаксис: ntp broadcast server count <number>

no ntp broadcast server count

Назначение: Позволяет задать максимальное число broadcast- или multicast-серверов, поддерживаемых клиентом NTP. Отмена команды **no ntp broadcast server count** удаляет введенные настройки и восстанавливает настройки, заданные по умолчанию.

Параметры: number1-100, максимальное число broadcast-серверов.

Значение по умолчанию: задано 50 broadcast-серверов.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Задать на коммутаторе максимальное число broadcast-серверов равным 70.

```
Switch(config)#ntp broadcast server count 70
```

30.1.4 ntp timezone

Синтаксис: `ntp timezone <name> [{add | subtract}] [<time_difference>]`

`no ntp timezone`

Назначение: Позволяет задать для NTP-клиента часовой пояс и сдвиг по времени относительно UTC. Отмена команды `no ntp timezone` отменяет настройку часового пояса и восстанавливает настройки, заданные по умолчанию.

Параметры: **name:** имя часового пояса, длина не более 16 символов.

add: к времени UTC будет добавлено значение, указанное в `time_difference`.

subtract: из времени UTC будет вычитаться значение, указанное в `time_difference`. По умолчанию задана опция `add`.

time_difference: значение сдвига по времени, в пределах от 0 до 12.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Установить часовой пояс для Москвы.

```
Switch#config Switch(config)#ntp timezone Moscow add 3
```

30.1.5 ntp access-group

Синтаксис: `ntp access-group server <acl>`

`no ntp access-group server <acl>`

Назначение: Позволяет установить фильтрацию по списку доступа ACL, когда коммутатор работает в режиме NTP-сервера. Отмена команды `no ntp access-group server <acl>` отменяет фильтрацию по списку доступа ACL на NTP-сервере.

Параметры: **<acl>:** Номер ACL, в пределах от 1 до 99.

Значение по умолчанию: Список доступа ACL не задан на NTP-сервере.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Задать для коммутатора список доступа ACL с номером 2.

```
Switch(config)#ntp access-group server 2
```

30.1.6 ntp authenticate

Синтаксис: `ntp authenticate`

`no ntp authenticate`

Назначение: Позволяет включить функцию аутентификации NTP. Отмена команды `no ntp authenticate` выключает функцию аутентификации NTP.

Параметры: Нет.

Значение по умолчанию: Функция выключена.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Включить функцию аутентификации NTP.

```
Switch(config)#ntp authenticate
```

30.1.7 ntp authentication-key

Синтаксис: `ntp authentication-key <key-id> md5 <value>`

`no ntp authentication-key <key-id>`

Назначение: Позволяет включить функцию аутентификации NTP и задать ключ аутентификации. Отмена команды `no ntp authentication-key <key-id>` выключает функцию аутентификации NTP.

Параметры: **key-id:** Идентификатор ключа, в пределах от 1 до 4294967295.

value: Значение ключа, в пределах от 1 до 16 символов ascii.

Значение по умолчанию: Ключ NTP-аутентификации не задан.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Задать ключ NTP-аутентификации - идентификатор ключа 20, значение abc (используется алгоритм md5).

```
Switch(config)#ntp authentication-key 20 md5 abc
```

30.1.8 ntp trusted-key

Синтаксис: ntp trusted-key <key-id>

no ntp trusted-key <key-id>

Назначение: Позволяет задать безопасный ключ. Отмена команды **no ntp trusted-key <key-id>** отменяет безопасный ключ.

Параметры: **key-id:** Идентификатор ключа, в пределах от 1 до 4294967295.

Значение по умолчанию: Безопасный ключ не задан.

Режим конфигурирования: Глобальный режим конфигурирования.

Пример: Задать ключ 20 как безопасный.

```
Switch(config)#ntp trusted-key 20
```

30.1.9 ntp disable

Синтаксис: ntp disable

no ntp disable

Назначение: Позволяет включить функцию NTP в порту. Отмена команды **no ntp disable** выключает функцию NTP в порту.

Параметры: Нет.

Значение по умолчанию: Функция NTP включена во всех портах.

Режим конфигурирования: Режим настройки интерфейсов.

Пример: Выключить функцию NTP в интерфейсе vlan1.

```
Switch(config)#interface vlan 1  
Switch(Config-if-Vlan1)#ntp disable
```

30.1.10 debug ntp authentication

Синтаксис: debug ntp authentication

no debug ntp authentication

Назначение: Позволяет вывести на дисплей информацию NTP-аутентификации. Отмена команды **no debug ntp authentication** прекращает вывод на дисплей информации NTP-аутентификации.

Параметры: Нет.

Значение по умолчанию: функция выключена.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет вывести на дисплей информацию NTP-аутентификации. Если коммутатор включен и принимаемые/передаваемые пакеты содержат аутентификационную информацию, то идентификатор ключа будет выведен на печать.

Пример: Включить вывод отладочных сообщений аутентификации NTP.

```
Switch(config)#debug ntp authentication
```

30.1.11 debug ntp packet

Синтаксис: debug ntp packet [send | receive]

no debug ntp packet [send | receive]

Назначение: Позволяет включить вывод отладочных сообщений о пакетах NTP. Отмена команды **no debug ntp packet [send | receive]** прекращает вывод отладочных сообщений о пакетах NTP.

Параметры: **send:** включает вывод информации о посланных NTP-пакетах.

receive: включает вывод информации о принятых NTP-пакетах.

Если команда введена без параметров, будет выведена информация о принятых и посланных пакетах.

Значение по умолчанию: Функция выключена.

Режим конфигурирования: Привилегированный режим.

Пример: Включить вывод отладочных сообщений о пакетах NTP.
Switch(config)#debug ntp packet

30.1.12 debug ntp adjust

Синтаксис: debug ntp adjust

no debug ntp adjust

Назначение: Позволяет включить вывод отладочных сообщений о локальных настройках времени. Отмена команды **no debug ntp adjust** прекращает вывод отладочных сообщений о локальных настройках времени.

Параметры: Нет.

Значение по умолчанию: Функция выключена.

Режим конфигурирования: Привилегированный режим.

Пример: Включить вывод отладочных сообщений о локальных настройках времени.
Switch(config)#debug ntp adjust

30.1.13 debug ntp sync

Синтаксис: debug ntp sync

no debug ntp sync

Назначение: Позволяет включить вывод отладочных сообщений о локальных настройках синхронизации времени. Отмена команды **no debug ntp sync** прекращает вывод отладочных сообщений о локальных настройках синхронизации времени.

Параметры: Нет.

Значение по умолчанию: Функция выключена.

Режим конфигурирования: Привилегированный режим.

Пример: Включить вывод отладочных сообщений о локальных настройках синхронизации времени.
Switch(config)#debug ntp sync

30.1.14 debug ntp events

Синтаксис: debug ntp events

no debug ntp events

Назначение: Позволяет включить вывод отладочных сообщений о событиях NTP. Отмена команды **no debug ntp events** прекращает вывод отладочных сообщений о событиях NTP.

Параметры: Нет.

Значение по умолчанию: Вывод отладочных сообщений о событиях NTP выключен.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет включить вывод на дисплей отладочных сообщений о событиях NTP. После этого, если какой-либо сервер изменил свое состояние с доступного на недоступное (или наоборот), принятые ошибочные пакеты о событиях будут выведены на печать.

Пример: Включить вывод отладочных сообщений о событиях NTP.
Switch(config)#debug ntp events

30.1.15 show ntp status

Синтаксис: show ntp status

Назначение: Позволяет вывести на дисплей состояние временной синхронизации, в том числе информацию о том, синхронизирован коммутатор или нет, уровни, адрес источника времени и т. д.

Параметры: Нет.

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch# show ntp status
Clock status: synchronized
Clock stratum: 3
Reference clock server: 1.1.1.2
Clock offset: 0.010 s
Root delay: 0.012 ms
Root dispersion: 0.000 ms
Reference time: TUE JAN 03 01:27:24 2006
```

30.1.16 show ntp session

Синтаксис: show ntp session [<ip-address> | <ipv6-address>]

Назначение: Позволяет вывести на дисплей информацию о всех сеансах NTP или об одном конкретном сеансе, в том числе, идентификатор (ID) сервера, уровень сервера, локальный сдвиг, соответствующий серверу. (Символ * означает, что этот сервер выбран в качестве локального источника времени).

Параметры: ip-address: IPv4-адрес некоторого настроенного сервера времени.

ipv6-address: IPv6-адрес некоторого настроенного сервера времени.

Если команда введена без параметров, на дисплей будет выведена информация о сеансах всех серверов (в том числе для broadcast- и multicast- серверов).

Значение по умолчанию: Нет.

Режим конфигурирования: Привилегированный режим.

Пример:

```
switch#show ntp session
```

server	stream	type	rootdelay	rootdispersion	trustlevel
* 1.1.1.2	2	unicast	0.010s	0.002s	10
2.2.2.2	3	unicast	0.005s	0.000s	10

31 Команды для настройки перехода на летнее/зимнее время

31.1.1 clock summer-time absolute

Синтаксис: clock summer-time <word> absolute <HH:MM> <YYYY.MM.DD> <HH:MM> <YYYY.MM.DD> [<offset>]

no clock summer-time

Назначение: Позволяет указать временной интервал в котором используется летнее время.

Параметры: <word>: наименование временной зоны; <HH:MM>: время начала интервала, в формате - часы (от 0 до 23) и минуты (от 0 до 59); <YYYY.MM.DD>: дата начала интервала, в формате – год (от 1970 до 2038), месяц (от 1 до 12) и число (от 1 до 31); <HH:MM>: время окончания интервала, в формате - часы (от 0 до 23) и минуты (от 0 до 59); <YYYY.MM.DD>: дата окончания интервала, в формате – год (от 1970 до 2038), месяц (от 1 до 12) и число (от 1 до 31); <offset>: сдвиг времени, в формате от 1 до 1440 минут, по-умолчанию 60 мин.

Значение по умолчанию: Временной интервал не задан.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Данная команда устанавливает абсолютное время начала и окончания временного интервала в котором используется летнее время.

Пример:

```
Switch(config)#clock summer-time Moscow absolute 12:00 2011.4.6 12:00  
2011.8.6 120
```

31.1.2 clock summer-time recurring

Синтаксис: clock summer-time <word> recurring <HH:MM> <MM.DD> <HH:MM> <MM.DD> [<offset>]

no clock summer-time

Назначение: Позволяет указать временной интервал в котором используется летнее время.

Параметры: <word>: наименование временной зоны; <HH:MM>: время начала интервала, в формате - часы (от 0 до 23) и минуты (от 0 до 59); <MM.DD>: дата начала интервала, в формате – месяц (от 1 до 12) и число (от 1 до 31); <HH:MM>: время окончания интервала, в формате - часы (от 0 до 23) и минуты (от 0 до 59); <MM.DD>: дата окончания интервала, в формате – месяц (от 1 до 12) и число (от 1 до 31); <offset>: сдвиг времени, в формате от 1 до 1440 минут, по-умолчанию 60 мин.

Значение по умолчанию: Временной интервал не задан.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Данная команда устанавливает время начала и окончания периодического временного интервала в котором используется летнее время.

Пример:

```
Switch(config)#clock summer-time Moscow absolute 12:00 4.6 12:00 8.6 120
```

31.1.3 clock summer-time recurring

Синтаксис: clock summer-time <word> recurring <HH:MM> <week> <day> <month> <HH:MM> <week> <day> <month> [<offset>]

no clock summer-time

Назначение: Позволяет указать временной интервал в котором используется летнее время.

Параметры: **<word>**: наименование временной зоны; **<HH:MM>**: время начала или окончания интервала, в формате - часы (от 0 до 23) и минуты (от 0 до 59); **<week>**: неделя начала или окончания интервала, от 1 до 4, а также первая (first) и последняя (last); **<day>**: день недели начала или окончания интервала, возможны значения "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"; **<month>**: месяц начала или окончания интервала, возможны значения "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"; **<offset>**: сдвиг времени, в формате от 1 до 1440 минут, по-умолчанию 60 мин.

Значение по умолчанию: Временной интервал не задан.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Данная команда позволяет гибко установить время начала и окончания периодического временного интервала в котором используется летнее время.

Пример:

```
Switch(config)#clock summer-time Moscow recurring 02:00 last Sun Mar 03:00  
last Sun Oct 60
```

32 Команды для диагностики и контроля состояния устройства

32.1.1 clear logging

Синтаксис: `clear logging {sdram}`

Назначение: С помощью этой команды можно удалить системные сообщения, имеющиеся в буферах системных сообщений.

Режим конфигурирования: Привилегированный режим.

Описание: Когда информация в буфере устаревает и становится больше не актуальной можно использовать эту команду для очистки всей информации в буфере.

Пример: Удалить всю информацию из зоны sdram буфера.
`Switch#clear logging sdram`

См. также: `show logging buffered`

32.1.2 logging

Синтаксис: `logging {<ipv4-addr> | <ipv6-addr>} [facility <local-number>] [level <severity>]
no logging {<ipv4-addr> | <ipv6-addr>}[facility <local-number>]`

Назначение: Команда используется для настройки канала вывода на хост системных сообщений. Отмена команды `no logging {<ipv4-addr> | <ipv6-addr>} [facility <local-number>]` включает эту функцию.

Параметры: `<ipv4-addr>`: IPv4-адрес хоста;

`<ipv6-addr>`: IPv6-адрес хоста;

`<local-number>`: записывающее оборудование хоста с идентификаторами local0 ~ local7, соответствующее оборудованию, определенному в RFC3164;

`<severity>`: уровень значимости системных сообщений.

Правила вывода системных сообщений следующие: выводятся только те системные сообщения, уровень значимости которых равен или больше заданного порогового значения. Подробное описание уровней значимости см. в руководстве по настройке коммутатора.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Информация системных сообщений на хост не выводится. По умолчанию оборудованию записи хоста системных сообщений присвоена метка local0, уровень значимости – предупреждения.

Описание: Эта команда доступна только в том случае, когда хост системных сообщений сконфигурирован командой `logging`. Можно сконфигурировать несколько хостов системных сообщений с IPv4- и IPv6-адресами.

Пример: Послать информацию системных сообщений с уровнем значимости равным или большим уровня предупреждений (warning) на сервер системных сообщений с IPv4-адресом 100.100.100.5 и сохранить их в записывающем оборудовании с идентификатором local1.
`Switch(config)#logging 100.100.100.5 facility local1 level warnings`

Послать информацию системных сообщений с уровнем значимости равным или большим уровня предупреждений (informational) на сервер системных сообщений с IPv6-адресом 3ffe:506:1:2::3 и сохранить их в записывающем оборудовании с идентификатором local5.
`Switch(config)#logging 3ffe:506:1:2::3 facility local5 level informational`

32.1.3 logging loghost sequence-number

Синтаксис: `logging loghost sequence-number`

`no logging loghost sequence-number`

Назначение: Команда добавляет к сообщению порядковый номер.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Порядковый номер не добавляется.

Пример:

```
Switch(config)#logging loghost sequence-number
```

32.1.4 logging executed-commands

Синтаксис: logging executed-commands {enable | disable}

Назначение: Включает протоколирование вводимых в CLI команд.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Команды не протоколируются.

Пример:

```
Switch(config)#logging executed-commands enable
```

32.1.5 ping

Синтаксис: ping [[src <source-address>] {<destination-address> | host <hostname>}]

Назначение: Коммутатор посылает пакет запроса ICMP удаленному клиентскому устройству и проверяет связь на обеих сторонах — присутствует она или нет.

Параметры: <source-address>: IP-адрес источника.

<destination-address>: IP-адрес назначения.

<hostname>: имя хоста назначения — символьная строка, содержащая буквы и цифры. Пробелы не допускаются, длина строки от 1 до 30 символов.

Значение по умолчанию: отправка 5 пакетов с запросами ICMP; размер пакета 56 байт, интервал отправки — 2 с.

Режим конфигурирования: Привилегированный режим.

Описание: Если команда ping введена без параметров, включается интерактивный режим. В нем можно задать параметры команды ping.

Пример: Использовать опции ping, заданные по умолчанию.

```
Switch#ping 10.1.128.160
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds. ....!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms
```

В этом примере команда ping будет выдана из коммутатора в некоторое устройство с IP-адресом 10.1.128.160. После отправки трех первых эхо-пакетов ICMP (echo request), коммутатор определяет, что другая сторона недоступна, так как соответствующие ответные пакеты ICMP (echo reply) не были получены в течение 2 секунд с начала посылки эхо-пакетов. Для следующих двух эхо-пакетов ответные пакеты были получены, поэтому процент успешно полученных ответных пакетов будет 40%. Здесь сбой обозначен точкой ".", а успешная операция — знаком "!!".

Использовать ping с IP-адресом источника, остальные параметры выбраны по умолчанию.

```
Switch#ping src 10.1.128.161 10.1.128.160
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.1.128.160, using source address
10.1.128.161, timeout is 2 seconds.
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

В примере, приведенном выше, IP-адрес источника равен 10.1.128.161, IP-адрес назначения 10.1.128.160. Для пяти эхо-пакетов ответ получен правильно, поэтому процент успеха равен 100%. Как и ранее, сбой обозначается точками ".", а успех — восклицательными знаками "!!".

Запуск команды ping с пользовательскими параметрами.

```
Switch#ping
VRF name:
Target IP address: 10.1.128.160
Use source address option[n]: y
```

Source IP address: 10.1.128.161
Repeat count [5]:100
Datagram size in byte [56]:1000
Timeout in milli-seconds [2000]:500
Extended commands [n]:n

Отображаемая информация	Описание
VRF name	Имя VRM. Если протокол MPLS не включен, это поле должно оставаться незаполненным.
Target IP address :	IP-адрес устройства назначения.
Use source address option[n]	Следует ли использовать опцию адреса источника?
Source IP address	Присваивает IP-адрес источника, который используется в команде ping.
Repeat count [5]	Число посылаемых командой ping эхо-пакетов. По умолчанию равно 5.
Datagram size in byte [56]	Размер эхо-пакета команды ping в байтах. По умолчанию равен 56.
Timeout in milli-seconds [2000] :	Временной интервал для ответных пакетов в миллисекундах. По умолчанию равен 2 с.
Extended commands [n] :	Нужны ли расширенные команды?

32.1.6 ping6

Синтаксис: ping6 [<dst-ipv6-address> | host <hostname> | src <src-ipv6-address> {<dst-ipv6-address> | host <hostname>}]

Назначение: Позволяет проверить связь с сетью назначения.

Параметры: <dst-ipv6-address>: IPv6-адрес назначения.

<src-ipv6-address>: IPv6-адрес источника.

<hostname>: имя хоста назначения — символьная строка, содержащая буквы и цифры. Пробелы не допускаются, длина строки от 1 до 30 символов.

Значение по умолчанию: отправка 5 пакетов с запросами ICMP6; размер пакета 56 байт, с интервалом - 2 с.

Режим конфигурирования: Пользовательский режим.

Описание: Если команда ping6 введена только с IPv6-адресом, остальные параметры будут выбраны по умолчанию. Когда ipv6-адрес является link local адресом, необходимо указать имя VLAN-интерфейса. Когда задан IPv6-адрес источника, командой будут сформированы запросы icmp6 с этим адресом для приема эхо-пакетов.

Пример: Использовать опции ping6, заданные по умолчанию.

```
Switch>ping6 2001:1:2::4
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 2001:1:2::4, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms
```

Ввести команду ping6 с указанием IPv6-адреса источника.

```
switch>ping6 src 2001:1:2::3 2001:1:2::4
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 2001:1:2::4, using src address 2001:1:2::3,
timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Запуск команды ping6 с пользовательскими параметрами (в интерактивном режиме).

```

Switch>ping6
Target IPv6 address:fe80::2d0:59ff:feb8:3b27
Output Interface: vlan1
Use source address option[n]:y
Source IPv6 address: fe80::203:fff:fe0b:16e3
Repeat count [5]:
Datagram size in byte [56]:
Timeout in milli-seconds [2000]:
Extended commands [n]:
Type ^c to abort.
Sending 5 56-byte ICMP Echos to fe80::2d0:59ff:feb8:3b27, using src address
fe80::203:fff:fe0b:16e3, timeout is 2 seconds.
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

```

Информация, отображаемая на дисплее	Описание
ping6	Команда ping6
Target IPv6 address	IPv6-адрес назначения.
Output Interface	Имя интерфейса VLAN, должно быть указано, когда адрес назначения является link local адресом.
Use source IPv6 address [n]:	Следует ли использовать опцию IPv6-адреса источника? По умолчанию задано не использовать опцию IPv6-адреса источника.
Source IPv6 address	IPv6-адрес источника.
Repeat count[5]	Число посылаемых командой ping6 эхо-пакетов. По умолчанию равно 5.
Datagram size in byte[56]	Размер эхо-пакета команды ping6 в байтах. По умолчанию равен 56.
Timeout in milli-seconds[2000]	Временной интервал для ответных пакетов в миллисекундах. По умолчанию равен 2 с.
Extended commands[n]	Расширенный формат команды. По умолчанию выключен.
!	Связь с узлом установлена (успех).
.	Связь с узлом не установлена (неудача).
Success rate is 100 percent(8/8), round-trip min/avg/max = 1/1/1ms	Статистическая информация, 100 % успех.

32.1.7 show debugging

Синтаксис: show debugging {l4 | lldp | nsm | other | spanning-tree}

Назначение: Позволяет вывести на дисплей информацию о включенных опциях отладки.

Описание: Эта команда используется для вывода на дисплей включенных опций отладки.

Режим конфигурирования: Привилегированный режим.

Пример:

```

Switch#show debugging other
TCP IP:
arp rx debugging is on
arp tx debugging is on
arp sm debugging is on

```

См. также: debug

32.1.8 show flash

Синтаксис: show flash

Назначение: Выводит на дисплей информацию о файлах, хранящихся во флэш-памяти.

Режим конфигурирования: Привилегированный режим.

Пример: Проверить размер файлов, хранящихся во флэш-памяти.

```
Switch#show flash
file name                file length(bytes)
nos.img                  4343433
startup-config           0
```

32.1.9 show history

Синтаксис: show history

Назначение: Отображает введенные пользователем команды в хронологическом порядке.

Режим конфигурирования: Привилегированный режим.

Описание: Система сохраняет в хронологическом порядке до 20 команд, введенных пользователями. Команды из последовательности ввода можно выбирать клавишами UP и DOWN, либо комбинациями клавиш Ctrl+P и Ctrl+N.

Пример:

```
Switch#show history
enable
config interface ethernet 1/3
enable dir
show ftp
```

32.1.10 show logging buffered

Синтаксис: show logging buffered [level {critical | warnings} | range <begin-index> <end-index>]

Назначение: Выводит на дисплей детальную информацию о канале буфера системных сообщений.

Параметры: level {critical | warnings}: уровень значимости информации.

<begin-index>: начальный номер системного сообщения, в пределах 1-65535,

<end-index>: конечный номер системного сообщения, в пределах 1-65535.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: При вводе команды без параметров будут выведены все системные сообщения критического уровня значимости.

Описание: В буфере хранятся сообщения критического уровня значимости и предупреждения. При выводе на терминал они имеют следующий формат: идентификационный номер (ID), время, <уровень> ID модуля [имя задания], информация сообщения.

Пример: Вывести системные сообщения критического уровня значимости, хранящиеся в буфере системных сообщений, номера с 940 по 946.

```
Switch#show logging buffered level critical range 940 946
```

Вывести на дисплей информацию предупреждений, хранящихся в буфере системных сообщений с уровнем значимости warning.

```
Switch#show logging buffered level warning
```

32.1.11 show logging source mstp

Синтаксис: show logging source mstp

Назначение: Выводит на дисплей детальную информацию о сообщениях модуля MSTP.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Нет.

Пример:

```
Switch#show logging source mstp
system module log switch status:
Channel          Onoff          Severity
```

```

logbuff          on          warning
logghost        on          warning
terminal        on          warning

```

32.1.12 show memory

Синтаксис: `show memory [usage]`

Назначение: Выводит на дисплей содержимое памяти.

Параметры: `usage`: информация об использовании памяти.

Режим конфигурирования: Привилегированный режим.

Описание: Эта команда используется для отладки. В интерактивном режиме можно ввести базовый адрес и длину. Информация, формируемая системой, содержит три области: адреса, слова дампа памяти в виде шестнадцатеричных слов и соответствующие им символы ASCII.

Пример:

```

Switch#show memory
start address : 0x2100
number of words[64]:
002100:  0000 0000 0000 0000  0000 0000 0000 0000  * .....*
002110:  0000 0000 0000 0000  0000 0000 0000 0000  * .....*
002120:  0000 0000 0000 0000  0000 0000 0000 0000  * .....*
002130:  0000 0000 0000 0000  0000 0000 0000 0000  * .....*
002140:  0000 0000 0000 0000  0000 0000 0000 0000  * .....*
002150:  0000 0000 0000 0000  0000 0000 0000 0000  * .....*
002160:  0000 0000 0000 0000  0000 0000 0000 0000  * .....*
002170:  0000 0000 0000 0000  0000 0000 0000 0000  * .....*

```

32.1.13 show running-config

Синтаксис: `show running-config`

Назначение: Выводит на дисплей параметры текущей конфигурации коммутатора.

Значение по умолчанию: Если параметры текущей конфигурации те же, что и параметры, заданные по умолчанию, то на дисплей ничего не выводится.

Режим конфигурирования: Привилегированный режим.

Описание: Команда `show running-config` используется для проверки правильности введенных пользователями конфигураций и отображения текущих параметров.

Пример:

```
Switch#show running-config
```

32.1.14 show startup-config

Синтаксис: `show startup-config`

Назначение: Выводит на дисплей конфигурацию параметров коммутатора, сохраненную во флэш-памяти в процессе текущей работы. Выводится также информация о файлах конфигурации, которые будут использоваться после следующего включения питания.

Значение по умолчанию: Если параметры текущей конфигурации те же, что и параметры, считанные из флэш-памяти, то на дисплей ничего выведено не будет.

Режим конфигурирования: Привилегированный режим.

Описание: Между командами `show running-config` и `show startup-config` имеются некоторые различия. Новые опции, заданные при конфигурировании, могут быть выведены на дисплей командой `show running-config`. Если была введена команда `write`, результат будет в обоих случаях одинаковым.

32.1.15 show switchport interface

Синтаксис: `show switchport interface [ethernet <IFNAME>]`

Назначение: Выводит на дисплей информацию о режиме работе порта, идентификаторе VLAN и т. п.

Параметры: <IFNAME>: номер порта.

Режим конфигурирования: Привилегированный режим

Пример: Show VLAN messages of port ethernet 0/0/1.

```
Switch#show switchport interface ethernet 0/0/1
Ethernet0/0/1 Type :Universal
Mac addr num : No limit
Mode :Access
Port VID :1
Trunk allowed Vlan :ALL
```

Параметры	Описание
Ethernet0/0/1	Имя порта Ethernet-интерфейса.
Type	Состояние текущего интерфейса.
Mac addr num	Максимальный размер таблицы MAC-адресов, которую может обслуживать текущий интерфейс.
Mode :Access	Режим работы текущего интерфейса
Port VID :1	Идентификатор vlan, которому принадлежит текущий интерфейс.
Trunk allowed Vlan :ALL	Разрешенные VLA для интерфейса, работающего в режиме trunk.

32.1.16 show tcp

Синтаксис: show tcp

Назначение: Выводит на дисплей состояние текущего TCP-соединения, установленного с коммутатором.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show tcp
LocalAddress      LocalPort  ForeignAddress  ForeignPort  State        IF
VRF
127.0.0.1         2650      127.0.0.1      3095         ESTABLISHED0 0
127.0.0.1         3095      127.0.0.1      2650         ESTABLISHED0 0
192.168.2.24      23        192.168.2.105  1456         ESTABLISHED0 0
0.0.0.0           23        0.0.0.0        0            LISTEN        0 0
127.0.0.1         2650      0.0.0.0        0            LISTEN        0 0
```

Параметры	Описание
LocalAddress	Локальный адрес TCP-соединения
LocalPort	Локальные порты TCP-соединения
ForeignAddress	Адреса удаленного устройства TCP-соединения
ForeignPort	Порт удаленного устройства TCP-соединения
State	Текущее состояние TCP-соединения

32.1.17 show tcp ipv6

Синтаксис: show tcp ipv6

Назначение: Выводит на дисплей состояние текущего TCP-соединения, установленного с коммутатором.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show tcp ipv6
LocalAddress      LocalPort  RemoteAddress  RemotePort  State
IF VRF
::                80         ::            0           LISTEN
0 0
```

Параметры	Описание
LocalAddress	Локальный IPv6-адрес TCP-соединения
LocalPort	Локальные порты TCP-соединения
ForeignAddress	IPv6-адреса удаленного устройства TCP-соединения
ForeignPort	Порт удаленного устройства TCP-соединения
State	Текущее состояние TCP-соединения
IF	Индекс локального порта TCP-соединения
VRF	Экземпляр VRF

32.1.18 show telnet login

Синтаксис: show telnet login

Назначение: Информация о текущих telnet-сессиях к коммутатору.

Режим конфигурирования: Привилегированный режим.

Описание: Данная команда используется для отображения информации о пользователях, подключенных к коммутатору по telnet.

Пример:

```
Switch#show telnet login
Authenticate login by local.
Login user:
admin
```

32.1.19 show tech-support

Синтаксис: show tech-support

Назначение: Собирает и отображает информацию технического характера. Предназначена для использования специалистами службы технической поддержки.

Режим конфигурирования: Привилегированный режим.

Описание: Информация, собранная по этой команде, позволяет определить причины сбоев системы.

Пример:

```
Switch#show tech-support
```

32.1.20 show udp

Синтаксис: show udp

Назначение: Выводит на дисплей состояние текущего UDP-соединения, установленного с коммутатором.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show udp
LocalAddress    LocalPort  ForeignAddress  ForeignPort  State
0.0.0.0        161       0.0.0.0        0            CLOSE
```

Параметры	Описание
LocalAddress	Локальный адрес UDP-соединения
LocalPort	Локальные порты UDP-соединения
ForeignAddress	Адреса удаленного устройства UDP-соединения
ForeignPort	Порт удаленного устройства UDP-соединения
State	Текущее состояние UDP-соединения

32.1.21 show udp ipv6

Синтаксис: show udp ipv6

Назначение: Выводит на дисплей состояние текущего UDP-соединения, установленного с коммутатором.

Режим конфигурирования: Привилегированный режим.

Пример:

```
Switch#show udp ipv6
LocalAddress                               LocalPort  RemoteAddress
RemotePort  State
::                               0          ::
0                               UNKNOWN
```

Параметры	Описание
LocalAddress	Локальный IPv6-адрес UDP-соединения
LocalPort	Локальные порты UDP-соединения
ForeignAddress	IPv6-адреса удаленного устройства UDP-соединения
ForeignPort	Порт удаленного устройства UDP-соединения
State	Текущее состояние UDP-соединения

32.1.22 show version

Синтаксис: show version

Назначение: Отображает версию коммутатора.

Режим конфигурирования: Привилегированный режим.

Описание: Выводит на дисплей информацию об аппаратных и программных функциях коммутатора.

Пример:

```
Switch#show version
Zelax ZES-2026C Switch Device, Compiled on Feb 03 19:05:40 2010
SoftWare Version Zelax ZES-2026C Switch_6.0.85.100
BootRom Version Zelax ZES-2026C Switch_2.0.3
HardWare Version R01
Copyright 2009 by Zelax
All rights reserved.
Uptime is 0 weeks, 2 days, 22 hours, 12 minutes.
```

32.1.23 traceroute

Синтаксис: traceroute [source <ipv4-addr>] {<ip-addr> | host <hostname>} [hops <hops>] [timeout <timeout>]

Назначение: Команда используется для проверки маршрута прохождения пакета от отправившего их оборудования до оборудования назначения. Это необходимо для проверки доступности и локализации отказов сети.

Параметры: <ipv4-addr>: IPv4-адрес хоста назначения.

<ip-addr>: IP-адрес хоста;

<hostname>: имя удаленного хоста.

<hops>: максимальное число шлюзов, допускаемое при трассировке.

<timeout>: время таймера для пакетов в миллисекундах, диапазон значений - от 100 до 10000.

Значение по умолчанию: По умолчанию максимальное число шлюзов равно 30, время таймера: 2000 миллисекунд.

Режим конфигурирования: Привилегированный режим.

Описание: Команда трассировки используется для локализации отказавшей сети, когда пакеты не достигают оборудования назначения.

Пример:

```
Switch#traceroute 192.168.2.105
Type ^c to abort.
```

```
Traceroute to host 192.168.2.105, maxhops is 30, timeout is 2000ms.  
1 0ms 192.168.2.105  
Traceroute completed.
```

32.1.24 traceroute6

Синтаксис: `traceroute6 [source <addr>] {<ipv6-addr> | host <hostname>} [hops <hops>] [timeout <timeout>]`

Назначение: Команда используется для проверки маршрута прохождения пакета от отправившего их оборудования до оборудования назначения. Это необходимо для проверки доступности сети и локализации отказов в ней.

Параметры: `<addr>`: IPv6-адрес хоста источника в шестнадцатеричной записи (с двоеточиями).

`<ipv6-addr>`: IPv6-адрес хоста назначения в шестнадцатеричной записи (с двоеточиями);

`<hostname>`: имя удаленного хоста.

`<hops>`: максимальное число шлюзов, допускаемое при трассировке с использованием команды `traceroute6`, в пределах от 1 до 255;

`<timeout>`: время таймера для пакетов в миллисекундах, диапазон значений - от 100 до 10000.

Значение по умолчанию: По умолчанию максимальное число шлюзов равно 30, время таймера: 2000 миллисекунд.

Режим конфигурирования: Привилегированный режим.

Описание: Команда `Traceroute6` используется для локализации отказавшей сети, когда пакеты не достигают оборудования назначения.

Пример:

```
Switch#traceroute6 2004:1:2:3::4
```

33 Перегрузка коммутатора по истечении заданного времени

33.1.1 reload after

Синтаксис: reload after <HH:MM:SS>

Назначение: Перегрузка коммутатора по истечении заданного периода времени.

Параметры: <HH:MM:SS>: заданный период времени, HH (часы) в пределах от 0 до 23, MM (минуты) и SS (секунды) в пределах от 0 до 59.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет перезагрузить коммутатор без отключения питания по истечении указанного периода времени. Обычно используется после обновления ПО коммутатора. Коммутатор может быть перезагружен по истечении заданного времени (но не немедленно) после того, как успешно обновлено его ПО. Эта команда используется однократно.

Пример: Перегрузить коммутатор по прошествии 10 часов и 1 секунды.

```
Switch#reload after 10:00:01
Process with reboot after? [Y/N] y
```

См. также:

Команда	Описание
reload	Перезагрузка коммутатора
reload cancel	Отменяет перезагрузку коммутатора по истечении заданного периода времени
show reload	Выводит на дисплей настройки, введенные пользователем в команде reload after

33.1.2 reload cancel

Синтаксис: reload cancel

Назначение: Отменяет перезагрузку коммутатора по истечении заданного периода времени.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим

Описание: Команда позволяет отменить перезагрузку коммутатора по истечении заданного периода времени (то есть отменить действие команды reload after). Эта команда не может быть продублирована.

Пример: Запретить автоматическую перезагрузку коммутатора по истечении указанного времени.

```
Switch#reload cancel
Reload cancel successful.
```

33.1.3 show reload

Синтаксис: show reload

Назначение: Выводит на дисплей настройки, введенные пользователем в команде reload after.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Описание: Команда позволяет просмотреть настройки, заданные в команде reload after и проверить, сколько времени осталось до перезагрузки коммутатора.

Пример: Вывести на дисплей настройки команды reload after. Ниже приведен ответ системы. Пользователь задал перезагрузку коммутатора через 10 часов и 1 секунду, до перезагрузки осталось 9 часов 59 минут и 48 секунд.

```
Switch#show reload
```

The original reload after configuration is 10:00:01.
System will be rebooted after 09:59:48 from now.

34 Команды для отладки и диагностики пакетов, принятых и посланных CPU

34.1.1 `cpu-rx-ratelimit enhanced`

Синтаксис: `cpu-rx-ratelimit enhanced`

`no cpu-rx-ratelimit enhanced`

Назначение: Включает на CPU режим ограничения скорости приема пакетов в соответствии с более детальной информацией протокола. Отмена команды `no cpu-rx-ratelimit enhanced` выключает этот режим.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Режим включен.

Описание: Команда включает на CPU режим ограничения скорости приема пакетов. Ее рекомендуется использовать под руководством инженера, работающего в компании-изготовителе коммутатора.

Пример: Выключить режим ограничения скорости приема пакетов в CPU.
`Switch(config)#no cpu-rx-ratelimit enhanced`

34.1.2 `cpu-rx-ratelimit total`

Синтаксис: `cpu-rx-ratelimit total <packets>`

`no cpu-rx-ratelimit total`

Назначение: Позволяет задать для CPU максимальную скорость приема пакетов. Отмена команды `no cpu-rx-ratelimit total` устанавливает максимальную скорость приема пакетов, заданную по умолчанию.

Параметры: `<packets>`: максимальное число пакетов, принимаемых CPU за 1 секунду.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: 350 пакетов/с.

Описание: Команда позволяет установить максимальную скорость приема пакетов в CPU. Рекомендуется, чтобы эту команду использовали только специалисты службы технической поддержки.

Пример: Задать максимальную скорость приема пакетов CPU равной 300 пакетов/с.
`Switch(config)#cpu-rx-ratelimit total 300`

34.1.3 `cpu-rx-ratelimit protocol`

Синтаксис: `cpu-rx-ratelimit protocol <protocol-type> <packets>`

`no cpu-rx-ratelimit protocol <protocol-type>`

Назначение: Позволяет задать максимальную скорость приема пакетов для указанного типа протокола. Отмена команды `no cpu-rx-ratelimit protocol <protocol-type>` устанавливает для указанного типа протокола максимальную скорость приема пакетов, заданную по умолчанию.

Параметры: `<protocol-type>`: тип протокола - arp, dhcp, dot1x, http, igmp, snmp, ssh, stp, telnet, ssl, ftp, tftp, nd, dhcpv6, ipv6-ntp-m, mld, gvrp, lacp, cluster-dp-dr, cluster-cpu-mac, uldp, lldp, eaps, loopback, ntp.

`<packets>`: максимальная скорость приема пакетов определенного типа протокола в CPU, в пределах от 1 до 500 пакетов/с.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Для разных типов протоколов заданы разные скорости.

Описание: Команда позволяет установить максимальную скорость приема пакетов определенного типа протокола в CPU. Рекомендуется, чтобы эту команду использовали только специалисты службы технической поддержки.

Пример: Установить скорость приема пакетов arp в CPU равной 500 пакетов/с.
Switch(config)#cpu-rx-ratelimit protocol arp 500

34.1.4 clear cpu-rx-stat protocol

Синтаксис: clear cpu-rx-stat protocol [<protocol-type>]

Назначение: Очищает статистику принятых CPU пакетов протокола указанного типа.

Параметры: <protocol-type>: тип протокола - arp, dhcp, dot1x, http, igmp, snmp, ssh, stp, telnet, ssl, ftp, tftp, nd, dhcpv6, ipv6-ntp-m, mld, gvrp, lacp, cluster-dp-dr, cluster-cpu-mac, uldp, lldp, eaps, loopback, ntp.

Режим конфигурирования: Глобальный режим конфигурирования.

Описание: Команда очищает статистику пакетов протокола определенного типа, принятых CPU. Рекомендуется, чтобы эту команду использовали только специалисты службы технической поддержки.

Пример: Очистить статистику принятых CPU пакетов протокола arp.
Switch(config)#clear cpu-rx-stat protocol arp

34.1.5 debug driver

Синтаксис: debug driver {receive | send} [interface {<interface-name> | all}] [protocol {<protocol-type> | discard | all}] [detail]

no debug driver {receive | send}

Назначение: Включает вывод на дисплей информации о пакетах, принятых и/или переданных CPU. Отмена команды no debug driver {receive | send} выключает вывод на дисплей этой информации.

Параметры: receive | send: вывод информации о принятых и/или переданных CPU пакетах;

interface {<interface-list>| all}: interface-list: номер Ethernet-порта.

all: вывод информации для всех Ethernet-портов.

protocol {<protocol-type> | discard | all}: тип протокола – snmp, telnet, http, dhcp, igmp, hsrp, arp, bgp, rip, ospf, pim, ssh, vrrp, ripng, ospfv3, pimv6, icmpv6, bgp4plus, unknown-mcast, unknown-mcast6, ttl0-2cpu, isis, dot1x, gvrp, stp, lacp, cluster, mld, vrrpv3, ra, uldp, lldp, eapou.

all: все типы протоколов,

discard: вывод информации для всех отброшенных пакетов.

detail: вывод детальной информации.

Режим конфигурирования: Привилегированный режим.

Описание: Команда используется для отладки. Рекомендуется, чтобы эту команду использовали только специалисты службы технической поддержки.

Пример: Включить вывод информации о принятых пакетах.
Switch#debug driver receive

34.1.6 show cpu-rx protocol

Синтаксис: show cpu-rx protocol [<protocol-type>]

Назначение: Выводит на дисплей статистики принятых CPU пакетов протокола указанного типа.

Параметры: <protocol-type>: тип протокола пакетов.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Нет.

Описание: Команда используется для отладки. Рекомендуется, чтобы эту команду использовали только специалисты службы технической поддержки.

Пример: Показать статистику принятых CPU пакетов протокола arp.
Switch#show cpu-rx protocol
arp Type Rate-limit TotPkts CurStatearp 500 3 allowed

35 Команды для работы с PoE

35.1 Команды для настройка PoE

35.1.1 power inline enable (глобальный режим конфигурирования)

Синтаксис: power inline enable

no power inline enable

Назначение: Позволяет включить или выключить PoE в глобальном режиме конфигурирования.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: PoE включено в глобальном режиме конфигурирования.

Описание: Если PoE выключено в глобальном режиме конфигурирования, то не имеет значения, включено или выключено электропитание на порту – электропитание будет отсутствовать.

Пример: Выключить PoE в глобальном режиме конфигурирования.

```
Switch(config)#no power inline enable
```

35.1.2 power inline max (глобальный режим конфигурирования)

Синтаксис: power inline max <max-wattage>

no power inline max

Назначение: Позволяет установить максимальную выходную мощность PoE в глобальном режиме конфигурирования.

Параметры: <max-wattage>: значение максимальной выходной мощности в Вт (целое число до 180).

Синтаксис: Глобальный режим конфигурирования.

Значение по умолчанию: Задана максимальная выходная мощность 180 Вт.

Описание: Установка в глобальном режиме конфигурирования максимальной выходной мощности может гарантировать надежное электропитание и эффективное управление мощностью, потребляемой подключенными устройствами.

Пример: Установить выходную мощность PoE в глобальном режиме конфигурирования равной 50 Вт.

```
Switch(Config)#power inline max 50
```

35.1.3 power inline police

Синтаксис: power inline police enable

no power inline police enable

Назначение: Позволяет включить или выключить режим управления электропитанием в соответствии с приоритетами (в глобальном режиме конфигурирования).

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Режим управления электропитанием в соответствии с приоритетами выключен.

Описание: Позволяет включить или выключить режим управления электропитанием в соответствии с приоритетами. Если режим включен, при управлении электропитанием будут учитываться заданные приоритеты. Отмена команды **no power inline police enable** восстанавливает электропитание по принципу «первому подключившемуся устройству электропитание предоставляется в первую очередь». В режиме электропитания по приоритетам,

в ситуации, когда мощности источника питания недостаточно, порты с малым приоритетом будут выключены, чтобы обеспечить питание портов, имеющих высокий приоритет - при этом не важно, сколько времени было доступно выключаемое устройство. Если два порта имеют одинаковые приоритеты, более высокий приоритет будет иметь порт с меньшим порядковым номером. В режиме «первому подключившемуся устройству электропитание предоставляется в первую очередь»: если мощности источника питания недостаточно, то на новые устройства электропитание подаваться не будет.

Пример: Включить режим управления электропитанием в соответствии с приоритетами.
`Switch(Config)#power inline police enable`

35.1.4 power inline legacy

Синтаксис: `power inline legacy enable`

no power inline legacy enable

Назначение: Позволяет задать настройку – следует или нет подавать электропитание на устройства, не соответствующие стандартам IEEE.

Параметры: Нет.

Режим конфигурирования: Глобальный режим конфигурирования.

Значение по умолчанию: Электропитание на устройства, не соответствующие стандартам IEEE подаваться не будет.

Описание: Когда эта функция включена, коммутатор будет подавать электропитание на устройства, не соответствующие стандартам IEEE.

Пример: Включить режим подачи электропитания на устройства, не соответствующие стандартам IEEE.
`Switch(Config)#power inline legacy enable`

35.1.5 power inline enable (режим настройки интерфейсов)

Синтаксис: `power inline enable`

no power inline enable

Назначение: Позволяет включить или выключить PoE.

Параметры: Нет.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Электропитание в портах включено.

Описание: Когда электропитание на порту включено, обнаружение устройств происходит автоматически. В этом состоянии PSE будет автоматически обнаруживать и классифицировать устройства и предоставлять им электропитание в соответствии с результатами классификации. Если обнаружено соединение с устройством, заявленная им выходная мощность будет обеспечиваться до тех пор пока мощности источника питания достаточно, при этом будет светиться соответствующий индикатор питания. Когда питание устройства будет выключено, этот индикатор перестанет светиться. Иными словами, решение об электропитании устройства будет приниматься на основе правил распределения электропитания. В нормальном режиме электропитания, если устройство запрашивает дополнительную мощность, превышающую пороговое предельно допустимое значение, источник питания выключит электропитание устройства и соответствующий индикатор перестанет светиться. Если устройство выключено пользователем, источник питания прекратит подачу электропитания на него, при этом соответствующий индикатор также перестанет светиться.

Когда электропитание на порту выключено, электропитание на устройства подаваться не будет, несмотря на установленное соединение. Это означает, что порт будет функционировать, как обычный Ethernet-порт и будет осуществлять обмен данными как обычно. Когда PoE выключено в глобальном режиме конфигурирования, электропитание подаваться не будет безотносительно к тому, включено или выключено оно в портах.

Примеры: Выключить PoE на портах 1, 3, 4, 5, 6.
`Switch(Config)#interface ethernet 0/0/1;3-6`
`Switch(Config-Port-Range)#no power inline enable`

35.1.6 power inline max (режим настройки интерфейсов)

Синтаксис: power inline max <max-wattage>

по power inline max

Назначение: Позволяет установить максимальную выходную мощность в указанном порту.

Параметры: <max-wattage>: Значение максимальной выходной мощности в мВт, в пределах от 1 до 15400 мВт с шагом 100 мВт. Любые значения менее 100 мВт будут трактоваться, как 100 мВт, поэтому при задании 1 — 100 мВт будет выставлена мощность 100 мВт, при задании 15301 — 15400 мВт будет выставлена мощность 15400 мВт. Однако если значение выставлено пользователем, округление с избытком выполняться не будет.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Задана максимальная выходная мощность порта 15400 мВт.

Описание: Эта команда позволяет эффективно управлять выходной мощностью каждого порта, при этом будет учитываться и мощность, заданная в глобальном режиме конфигурирования.

Пример: Задать выходную мощность порта 1 0,8 Вт.

```
Switch(Config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#power inline max 800
```

35.1.7 power inline priority

Синтаксис: power inline priority {critical | high | low}

Назначение: Позволяет задать приоритет электропитания для порту.

Параметры: **critical:** наивысший приоритет.

high: высокий приоритет.

low: низкий приоритет.

Режим конфигурирования: Режим настройки интерфейсов.

Значение по умолчанию: Задан низкий приоритет (**low**).

Описание: Эта команда возымеет действие только после ввода команды "power inline police enable". Если мощности источника питания для подключенных новых устройств недостаточно, в первую очередь будет осуществляться электропитание устройств, подключенных к портам с более высоким приоритетом.

Примеры: Задать для порта 1 приоритет high, а для порта 2 critical.

```
Switch(Config)#interface ethernet 0/0/1
Switch(Config-Ethernet0/0/1)#power inline priority high
Switch(Config)#interface ethernet 0/0/2
Switch(Config-Ethernet0/0/2)#power inline priority critical
```

35.2 Команды для мониторинга и отладки PoE

35.2.1 show power inline

Синтаксис: show power inline

Назначение: Позволяет вывести на дисплей настройки и состояние PoE в глобальном режиме конфигурирования.

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Нет.

Описание: Описание каждого параметра, отображаемого на дисплее приведено в таблице ниже.

Информация, отображаемая на дисплее	Описание
-------------------------------------	----------

Power Inline Status	Состояние PoE в глобальном режиме конфигурирования: включено или выключено.
Power Available	Максимальная общая мощность, доступная на коммутаторе.
Power Used	Общая используемая мощность.
Power Remaining	Общая оставшаяся мощность.
Min Voltage	Общее пороговое значение для падения напряжения.
Max Voltage	Общее пороговое значение для превышения напряжения.
Police	Управление электропитанием по приоритетам: включено или выключено.
Legacy	Электропитание нестандартных устройств: включено или выключено.
Disconnect	Режим отключения устройств.
HW Version	Версия аппаратуры модуля PoE.
SW Version	Версия ПО модуля PoE.
Mode	Режим работы источника питания: signal: электропитание осуществляется по сигнальным кабелям (вариант А); spare: электропитание осуществляется по резервным кабелям (вариант В).

Примеры: Вывести на дисплей общее состояние PoE.

```
Switch#show power inline
Power Inline Status: On
Power Available: 180 W
Power Used: 0 W
Power Remaining: 180 W
Min Voltage: 44 V
Max Voltage: 57 V
Police: Off
Legacy: Off
Disconnect: Ac
Mode: Signal
HW Version: 30
SW Version: 05.0.5
```

35.2.2 show power inline interface ethernet

Синтаксис: `show power inline interface [ethernet <interface-number> | <interface-name>]`

Назначение: Позволяет вывести на дисплей настройки PoE в указанных портах.

Параметры: `interface-list`: Список указанных портов (по умолчанию – список всех портов).

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Нет.

Описание: Описание каждого параметра, отображаемого на дисплее, приведено в таблице ниже.

Информация, отображаемая на дисплее	Описание
Interface	Номер Ethernet-порта.
Status	Состояние электропитания: enable: Электропитание включено disable: Электропитание выключено
Oper	Текущий статус: on: Устройство подключено, электропитание подано; off: Устройство не подключено; faulty: Сбой обнаружения устройств. deny: Мощность источника питания недостаточна или требуемая

	мощность превышает установленное предельно допустимое значение.
Power	Мощность, используемая портом
Max	Максимальная мощность, которая может быть отдана порту
Current	Ток, протекающий через порт
Volt	Напряжение на порту
Priority	Приоритет электропитания: critical: высший приоритет; high: высокий приоритет; low: низкий приоритет.
Class	Класс использования устройством PD входной мощности (Вт): 0 По умолчанию 0,44 — 12,95; 1 Опция 0.44 — 3.84; 2 Опция 3.84 — 6.49; 3 Опция 6.49 — 12.95; 4 Резервирован — интерпретируется как класс 0 и зарезервирован для использования в будущем. Совместимые устройства сигнал класса 4 не выдают.

Примеры: Вывести на дисплей текущее состояние PoE портов 1 – 6.

```
Switch#show power inline interface ethernet 0/0/1-6
Interface      Status      Oper      Power(mW)  Max(mW)  Current(mA)  Volt(V)  Priority  Class
-----
Ethernet0/0/1  enable     off       0          15400    0            0        high     0
Ethernet0/0/2  enable     off       0          15400    0            0        low      0
Ethernet0/0/3  enable     off       0          15400    0            0        low      0
Ethernet0/0/4  enable     off       0          15400    0            0        low      0
Ethernet0/0/5  enable     off       0          15400    0            0        low      0
Ethernet0/0/6  enable     off       0          15400    0            0        low      0
```

35.2.3 debug power inline

Синтаксис: debug power inline

no debug power inline

Назначение: Позволяет включить или выключить вывод отладочных сообщений PoE

Параметры: Нет.

Режим конфигурирования: Привилегированный режим.

Значение по умолчанию: Нет.

Описание: Когда включен вывод отладочных сообщений, будут выводиться сообщения об основных процессах, обусловленных введенными командами. Это необходимо для поиска ошибок. Отмена команды - no debug power inline выключает вывод отладочных сообщений.

Примеры: Включить вывод отладочных сообщений PoE.

```
Switch#debug power inline
```