

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (ПРОШИВКА)
ДЛЯ ИЗДЕЛИЯ КДСУ-КД2402-А1Б с ОС ROS Linux

Описание системы команд

643.18184162.00040-01 94-1

Листов 318

СОДЕРЖАНИЕ

1. Команды 802.1X	13
1.1. Команда aaa authentication dot1x	13
1.2. Команда authentication open	13
1.3. Команда clear dot1x statistics	14
1.4. Команда dot1x authentication	14
1.5. Команда dot1x guest-vlan	15
1.6. Команда dot1x guest-vlan enable	16
1.7. Команда dot1x guest-vlan timeout	17
1.8. Команда dot1x host-mode	17
1.9. Команда dot1x max-hosts	20
1.10. Команда dot1x max-req	20
1.11. Команда dot1x port-control	21
1.12. Команда dot1x radius-attributes vlan	22
1.13. Команда dot1x radius-attributes filter-id	24
1.14. Команда dot1x re-authenticate	24
1.15. Команда dot1x reauthentication	25
1.16. Команда dot1x system-auth-control	25
1.17. Команда dot1x timeout quiet-period	26
1.18. Команда dot1x timeout reauth-period	27
1.19. Команда dot1x timeout server-timeout	27
1.20. Команда dot1x timeout sup-timeout	28
1.21. Команда dot1x timeout tx-period	29
1.22. Команда dot1x traps authentication failure	29
1.23. Команда dot1x traps authentication quiet	30
1.24. Команда dot1x traps authentication success	31
1.25. Команда dot1x unlock client	31
1.26. Команда dot1x violation-mode	32
1.27. Команда show dot1x	33
1.28. Команда show dot1x locked clients	35
1.29. Команда show dot1x statistics	36
1.30. Команда show dot1x users	37
2. Команды authentication, authorization and accounting (AAA)	40
2.1. Команда aaa authentication login	40
2.2. Команда aaa authentication enable	41
2.3. Команда login authentication	42
2.4. Команда enable authentication	43

2.5. Команда ip http authentication.....	43
2.6. Команда show authentication methods.....	44
2.7. Команда password	45
2.8. Команда enable password.....	45
2.9. Команда service password-recovery.....	47
2.10. Команда username	47
2.11. Команда show users accounts.....	48
2.12. Команда aaa accounting login	49
2.13. Команда aaa accounting dot1x.....	51
2.14. Команда show accounting.....	52
2.15. Команда password complexity enable.....	53
2.16. Команда password complexity	54
2.17. Команда password aging.....	55
2.18. Команда show password configuration	55
2.19. Команда aaa accounting commands	56
2.20. Команда aaa authorization commands.....	56
3. Команды ACL	58
3.1. Команда ip access-list extended.....	58
3.2. Команда permit (IP).....	58
3.3. Команда deny (IP).....	61
3.4. Команда mac access-list	64
3.5. Команда permit (MAC)	64
3.6. Команда deny (MAC).....	66
3.7. Команда service-acl input.....	67
3.8. Команда service-acl output.....	68
3.9. Команда time-range	69
3.10. Команда absolute	70
3.11. Команда periodic	71
3.12. Команда show time-range.....	72
3.13. Команда show access-list.....	72
3.14. Команда show interfaces access-lists.....	73
3.15. Команда show interfaces access-lists trapped packets.....	73
3.16. Команда clear access-lists counters	74
3.17. Команда ip access-list (IP standard)	74
4. Команды адресных таблиц	76
4.1. Команда bridge multicast filtering.....	76
4.2. Команда bridge multicast mode.....	76

4.3. Команда bridge multicast address.....	78
4.4. Команда bridge multicast forbidden address	79
4.5. Команда bridge multicast ip-address	80
4.6. Команда bridge multicast forbidden ip-address.....	81
4.7. Команда bridge multicast source group.....	81
4.8. Команда bridge multicast forbidden source group	82
4.9. Команда bridge multicast unregistered.....	83
4.10. Команда bridge multicast forward-all.....	84
4.11. Команда bridge multicast forbidden forward-all	84
4.12. Команда bridge unicast unknown	85
4.13. Команда show bridge unicast unknown.....	86
4.14. Команда mac address-table static	86
4.15. Команда clear mac address-table	87
4.16. Команда mac address-table aging-time	88
4.17. Команда port security	88
4.18. Команда port security mode.....	89
4.19. Команда port security max.....	90
4.20. Команда port security routed secure-address.....	91
4.21. Команда show mac address-table	92
4.22. Команда show mac address-table count	93
4.23. Команда show bridge multicast mode	93
4.24. Команда show bridge multicast address-table	94
4.25. Команда show bridge multicast address-table static.....	96
4.26. Команда show bridge multicast filtering	98
4.27. Команда show bridge multicast unregistered	99
4.28. Команда show ports security	100
4.29. Команда show ports security addresses	101
4.30. Команда bridge multicast reserved-addresses	102
4.31. Команда show bridge multicast reserved-adresses	103
5. Команды управления загрузкой по сети	104
5.1. Команда boot host auto-config	104
5.2. Команда boot host auto-update	105
5.3. Команда show boot.....	106
5.4. Команда ip dhcp tftp-server address	106
5.5. Команда ip dhcp tftp-server file.....	107
5.6. Команда ip dhcp tftp-server image file.....	107
5.7. Команда show ip dhcp tftp-server.....	108

6. Команды установки даты и времени	109
6.1. Команда absolute	109
6.2. Команда clock dhcp timezone	109
6.3. Команда clock set	110
6.4. Команда clock source	111
6.5. Команда clock summer-time.....	112
6.6. Команда clock timezone	113
6.7. Команда periodic	114
6.8. Команда snmp anycast client enable.....	115
6.9. Команда snmp authenticate.....	115
6.10. Команда snmp authentication-key	116
6.11. Команда snmp broadcast client enable	116
6.12. Команда snmp client enable.....	117
6.13. Команда snmp client enable (interface).....	117
6.14. Команда snmp server	118
6.15. Команда snmp source interface	118
6.16. Команда snmp trusted-key	119
6.17. Команда snmp unicast client enable	120
6.18. Команда snmp unicast client poll	120
6.19. Команда show clock	121
6.20. Команда show snmp configuration.....	122
6.21. Команда show snmp status	122
6.22. Команда show time-range.....	124
6.23. Команда time-range	124
7. Команды отслеживания DHCP.....	126
7.1. Команда ip dhcp snooping	126
7.2. Команда ip dhcp snooping vlan	126
7.3. Команда ip dhcp snooping trust.....	127
7.4. Команда ip dhcp snooping information option allowed-untrusted.....	127
7.5. Команда ip dhcp snooping verify	128
7.6. Команда ip dhcp snooping database	128
7.7. Команда ip dhcp snooping binding.....	129
7.8. Команда clear ip dhcp snooping database	130
7.9. Команда show ip dhcp snooping.....	130
7.10. Команда show ip dhcp snooping binding	131
7.11. Команда ip source-guard.....	132
7.12. Команда ip source-guard binding	132

7.13. Команда ip source-guard tcam retries-freq	133
7.14. Команда ip source-guard tcam locate	134
7.15. Команда show ip source-guard configuration.....	134
7.16. Команда show ip source-guard status	135
7.17. Команда show ip source-guard inactive	135
7.18. Команда show ip source-guard statistics	136
7.19. Команда ip arp inspection	137
7.20. Команда ip arp inspection vlan	137
7.21. Команда ip arp inspection trust.....	138
7.22. Команда ip arp inspection validate	138
7.23. Команда ip arp inspection list create	139
7.24. Команда ip mac.....	140
7.25. Команда ip arp inspection list assign	140
7.26. Команда ip arp inspection logging interval	141
7.27. Команда show ip arp inspection	141
7.28. Команда show ip arp inspection list.....	142
7.29. Команда show ip arp inspection statistics.....	142
7.30. Команда clear ip arp inspection statistics	143
8. Команды сервера DHCP.....	144
8.1. Команда address (DHCP Host).....	144
8.2. Команда address (DHCP Network)	145
8.3. Команда bootfile	145
8.4. Команда clear ip dhcp binding.....	146
8.5. Команда client-name.....	146
8.6. Команда default-router.....	147
8.7. Команда dns-server	147
8.8. Команда domain-name.....	148
8.9. Команда ip dhcp excluded-address	149
8.10. Команда ip dhcp pool host	149
8.11. Команда ip dhcp pool network	150
8.12. Команда ip dhcp server	150
8.13. Команда lease.....	151
8.14. Команда netbios-name-server	151
8.15. Команда netbios-node-type.....	152
8.16. Команда next-server.....	153
8.17. Команда next-server-name.....	153
8.18. Команда option	154

8.19. Команда show ip dhcp	155
8.20. Команда show ip dhcp allocated.....	155
8.21. Команда show ip dhcp binding	156
8.22. Команда show ip dhcp declined.....	157
8.23. Команда show ip dhcp excluded-addresses	157
8.24. Команда show ip dhcp expired	158
8.25. Команда show ip dhcp pool host	158
8.26. Команда show ip dhcp pool network	159
8.27. Команда show ip dhcp pre-allocated	160
8.28. Команда show ip dhcp server statistics.....	160
8.29. Команда time-server	161
8.30. Команда ip dhcp ping enable	161
8.31. Команда ip dhcp ping count.....	162
8.32. Команда ip dhcp ping timeout	162
8.33. Команда ping enable	163
9. Команды посредника DHCP	164
9.1. Команда ip dhcp relay enable (Global).....	164
9.2. Команда ip dhcp relay enable (Interface)	164
9.3. Команда ip dhcp relay address (Global)	165
9.4. Команда ip dhcp relay address (Interface).....	165
9.5. Команда show ip dhcp relay	166
9.6. Команда ip dhcp information option.....	166
9.7. Команда show ip dhcp information option	167
10. Команды DNS клиента.....	168
10.1. Команда clear host	168
10.2. Команда ip domain lookup	168
10.3. Команда ip domain name.....	169
10.4. Команда ip domain pooling-interval.....	169
10.5. Команда ip domain retry	170
10.6. Команда ip domain timeout	171
10.7. Команда ip host.....	171
10.8. Команда ip name-server.....	172
10.9. Команда show hosts.....	173
11. Команды защиты от DOS (denial of service)	175
11.1. Команда security-suite enable.....	175
11.2. Команда security-suite deny fragmented	176
11.3. Команда security-suite deny icmp	177

11.4. Команда security-suite deny martian-addresses	178
11.5. Команда security-suite deny syn.....	179
11.6. Команда security-suite deny syn-fin	180
11.7. Команда security-suite dos protect	180
11.8. Команда security-suite dos syn-attack	181
11.9. Команда security-suite syn protection mode	182
11.10. Команда security-suite syn protection recovery	182
11.11. Команда security-suite protection threshold	183
11.12. Команда show security-suite configuration	183
11.13. Команда show security-suite syn protection.....	185
12. Команды конфигурирования ethernet	186
12.1. Команда interface.....	186
12.2. Команда interface range.....	186
12.3. Команда shutdown	187
12.4. Команда operation time	187
12.5. Команда description.....	188
12.6. Команда speed	189
12.7. Команда duplex.....	189
12.8. Команда negotiation.....	190
12.9. Команда flowcontrol	190
12.10. Команда mdix	191
12.11. Команда back-pressure	192
12.12. Команда port jumbo-frame	192
12.13. Команда clear counters	193
12.14. Команда set interface active.....	193
12.15. Команда errdisable recovery cause	194
12.16. Команда errdisable recovery interval.....	195
12.17. Команда errdisable recovery reset	195
12.18. Команда show interfaces configuration	196
12.19. Команда show interfaces status	197
12.20. Команда show interfaces advertise	199
12.21. Команда show interfaces description.....	200
12.22. Команда show interfaces counters	201
12.23. Команда show ports jumbo-frames.....	204
12.24. Команда show errdisable recovery	205
12.25. Команда show errdisable interfaces	205
12.26. Команда clear switchport monitor	206

12.27. Команда show switchport monitor.....	206
13. Команды настройки протокола GVRP (garp vlan registration protocol)	209
13.1. Команда clear gvrp statistics.....	209
13.2. Команда gvrp enable (Global)	209
13.3. Команда gvrp enable (Interface).....	210
13.4. Команда garp timer	210
13.5. Команда gvrp registration-forbid	211
13.6. Команда gvrp vlan-creation-forbid	212
13.7. Команда show gvrp configuration	212
13.8. Команда show gvrp error-statistics	214
13.9. Команда show gvrp statistics	215
14. Команды igmp snooping	216
14.1. Команда ip igmp snooping (Global)	216
14.2. Команда ip igmp snooping vlan.....	216
14.3. Команда ip igmp snooping vlan mrouter	217
14.4. Команда ip igmp snooping vlan mrouter interface	217
14.5. Команда ip igmp snooping vlan forbidden mrouter	218
14.6. Команда ip igmp snooping vlan static	219
14.7. Команда ip igmp snooping vlan multicast-tv.....	219
14.8. Команда ip igmp snooping map cpe vlan	220
14.9. Команда ip igmp snooping querier	221
14.10. Команда ip igmp snooping vlan querier	221
14.11. Команда ip igmp snooping vlan querier address	222
14.12. Команда ip igmp snooping vlan querier election.....	223
14.13. Команда ip igmp snooping vlan querier version.....	223
14.14. Команда ip igmp snooping vlan immediate-leave	224
14.15. Команда show ip igmp snooping cpe vlans	225
14.16. Команда show ip igmp snooping groups	225
14.17. Команда show ip igmp snooping interface	226
14.18. Команда show ip igmp snooping mrouter	227
14.19. Команда show ip igmp snooping multicast-tv	227
15. Команды ip адресации (ip адресация и интерфейсы второго уровня).....	229
15.1. Команда ip address	229
15.2. Команда ip address dhcp.....	230
15.3. Команда renew dhcp	231
15.4. Команда ip default-gateway.....	231
15.5. Команда show ip interface	232

15.6. Команда arp	232
15.7. Команда arp timeout (Global).....	233
15.8. Команда ip arp proxy disable.....	234
15.9. Команда ip proxy-arp.....	234
15.10. Команда clear arp-cache	235
15.11. Команда show arp	235
15.12. Команда show arp configuration	236
15.13. Команда interface ip	236
15.14. Команда ip helper-address	237
15.15. Команда show ip helper-address.....	238
15.16. Команда show ip dhcp client interface	238
16. Команды ip маршрутизации не привязанные к протоколу	239
16.1. Команда accept-lifetime.....	239
16.2. Команда directed-broadcast	240
16.3. Команда ip redirects.....	240
16.4. Команда ip route	241
16.5. Команда ip routing.....	241
16.6. Команда key-string	242
16.7. Команда key (key-chain)	243
16.8. Команда key chain	244
16.9. Команда send-lifetime	245
16.10. Команда show ip protocols	246
16.11. Команда show ip route.....	247
16.12. Команда show key chain.....	249
17. Команды многоадресной маршрутизации ipv4	251
17.1. Команда ip multicast-routing.....	251
17.2. Команда ip multicast ttl-threshold	251
17.3. Команда show ip mroute.....	252
17.4. Команда show ip multicast	256
18. Системные команды управления ip.....	259
18.1. Команда ping	259
18.2. Команда ssh	260
18.3. Команда telnet.....	261
18.4. Команда traceroute.....	263
19. Команды lisp.....	266
19.1. Команда lisp port	266
19.2. Команда lisp system-priority	266

19.3. Команда lacp timeout.....	267
19.4. Команда show lacp	267
19.5. Команда show lacp port-channel	269
20. Команды LLDP	270
20.1. Команда clear lldp table.....	270
20.2. Команда lldp chassis-id.....	270
20.3. Команда lldp hold-multiplier	271
20.4. Команда lldp lldpdu	271
20.5. Команда lldp management-address.....	272
20.6. Команда lldp med	273
20.7. Команда lldp med notification topology-change	274
20.8. Команда lldp med fast-start repeat-count	274
20.9. Команда lldp med location.....	275
20.10. Команда lldp med network-policy (Global)	276
20.11. Команда lldp med network-policy (Interface)	277
20.12. Команда lldp med network-policy voice auto	277
20.13. Команда lldp notifications	278
20.14. Команда lldp notifications interval	279
20.15. Команда lldp optional-tlv.....	279
20.16. Команда lldp optional-tlv 802.1.....	280
20.17. Команда lldp run	281
20.18. Команда lldp receive.....	281
20.19. Команда lldp reinit	282
20.20. Команда lldp timer	282
20.21. Команда lldp transmit	283
20.22. Команда lldp tx-delay	283
20.23. Команда show lldp configuration	284
20.24. Команда show lldp local	286
20.25. Команда show lldp local tlvs-overloading.....	287
20.26. Команда show lldp med configuration	288
20.27. Команда show lldp neighbors	289
20.28. Команда show lldp statistics	293
21. Команды настройки линии	296
21.1. Команда autobaud.....	296
21.2. Команда exec-timeout.....	296
21.3. Команда line.....	297
21.4. Команда speed	297

21.5. Команда show line	298
22. Команды обнаружения обратной петли (loopback).....	300
22.1. Команда loopback-detection enable (Global).....	300
22.2. Команда loopback-detection enable (Interface).....	300
22.3. Команда loopback-detection interval.....	301
22.4. Команда show loopback-detection	301
23. Команды настройки асl управления устройством.....	303
23.1. команда allow	303
23.2. Команда deny (Management)	303
23.3. Команда permit (Management).....	304
23.4. Команда management access-list.....	305
23.5. Команда management access-class.....	305
23.6. Команда show management access-list	306
23.7. Команда show management access-class	307
24. Команды макросов	308
24.1. Команда macro name	308
24.2. Команда macro.....	310
24.3. Команда macro description.....	311
24.4. Команда macro global.....	312
24.5. Команда macro global description.....	313
24.6. Команда show parser macro	314
Перечень сокращений	317

Часть 2 - 643.18184162.00040-01 94-2

1. КОМАНДЫ 802.1X

1.1. Команда `aaa authentication dot1x`

Команда **aaa authentication dot1x** используется для указания последовательности перебора способов аутентификации. Для отключения команды используется префикс «**no**».

Синтаксис:

```
aaa authentication dot1x default { radius | none } [ { radius | none } ]
```

```
no aaa authentication dot1x default
```

Параметры:

- *radius* – используется список всех описанных в конфигурации RADIUS серверов;
- *none* – аутентификация не применяется.

Состояние по умолчанию:

Аутентификация с помощью RADIUS сервера.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Допускается выбор проверки подлинности сервером RADIUS или отключение проверки (*none*), либо использование обоих методов.
2. Если требуется, чтобы проверка подлинности прошла успешно даже в случае недоступности RADIUS сервера, то в качестве последнего метода проверки требуется указать *none*.

Пример:

В данном случае устанавливается режим аутентификации 802.1X для аутентификации с использованием сервера RADIUS. Даже если ответ не получен, проверка подлинности завершается успешно.

```
console(config)# aaa authentication dot1x default radius none
```

1.2. Команда `authentication open`

Команда **authentication open** используется для включения режима открытого доступа (режим мониторинга) на порту. Для отключения режима используется префикс «**no**».

Синтаксис:

```
authentication open
```

```
no authentication open
```

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

Режим открытого доступа или мониторинга позволяет пользователям или устройствам получать доступ к сети до аутентификации. В этом режиме коммутатор обрабатывает ответы об ошибках полученные с сервера RADIUS.

Пример:

```
console(config)# interface gi 1/0/1  
console(config-if)# authentication open
```

1.3. Команда clear dot1x statistics

Для удаления статистики 802.1x на интерфейсе используется команда **clear dot1x statistics**

Синтаксис:

clear dot1x statistics [*interface-id*]

Параметры:

- *interface-id* – номер порта Ethernet.

Состояние по умолчанию:

Без указания параметра статистика сбрасывается на всех портах.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Данная команда очищает значения всех счетчиков, отображаемых командами **show dot1x** и **show dot1x statistics**.

Пример:

```
console# clear dot1x statistics
```

1.4. Команда dot1x authentication

Команда **dot1x authentication** служит для включения на порту аутентификации протокола 802.1x. Для отключения функции используется префикс «**no**».

Синтаксис:

dot1x authentication [{ **802.1x** | **mac** } [{ **802.1x** | **mac** }]]

no dot1x authentication

Параметры:

- **802.1x** – включение проверки подлинности на основе протокола 802.1x;
- **mac** – включение проверки подлинности на основе MAC-адреса подключаемого устройства.

Состояние по умолчанию:

По умолчанию включена проверка подлинности на основе протокола 802.1x.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. Статические MAC-адреса не могут быть разрешены параметром **mac**.
2. Не рекомендуется изменять динамический MAC-адрес на статический или удалять его из таблицы адресов, если он был разрешен к аутентификации параметром **mac**:
 - если динамический MAC-адрес, прошедший проверку подлинности с использованием MAC-аутентификации, будет изменен на статический, он не будет повторно аутентифицирован вручную;
 - удаление динамического MAC-адреса, прошедшего проверку подлинности с помощью MAC-аутентификации, вызывает повторную аутентификацию.

Пример:

Этот пример включает аутентификацию на основе 802.1x и MAC-адреса устройства на порту gi 1/0/1:

```
console(config)# interface GigabitEthernet 1/0/1
console(config-if)# dot1x authentication 802.1x mac
```

1.5. Команда dot1x guest-vlan

Команда **dot1x guest-vlan** определяет VLAN как гостевой. Использование префикса «**no**» возвращает состояние VLAN по умолчанию.

Синтаксис:

dot1x guest-vlan

no dot1x guest-vlan

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Гостевой VLAN не определен.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Примечания:

1. Для доступа неавторизованных пользователей в гостевой VLAN используется команда **dot1x guest-vlan enable**.
2. Коммутатор может иметь только один гостевой VLAN.
3. Гостевой VLAN должен быть статическим и его нельзя удалить.
4. Неавторизованный VLAN не может быть настроен как гостевой VLAN.

Пример:

В этом примере VLAN 2 определяется как гостевой VLAN

```
console(config)# interface vlan 2  
console(config-if)# dot1x guest-vlan
```

1.6. Команда dot1x guest-vlan enable

Команда **dot1x guest-vlan enable** разрешает доступ неавторизованным пользователям в гостевой VLAN. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

dot1x guest-vlan enable

no dot1x guest-vlan enable

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

По умолчанию доступ в гостевой VLAN запрещен.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. Команда не может быть выполнена, если на интерфейсе включен мониторинг VLAN.
2. Если порт не принадлежит гостевому VLAN, он добавляется в гостевой VLAN в качестве выходного немаркированного порта.
3. Если проверка подлинности выполняется в режиме **singe-host** или **multi-host**, то значение PVID устанавливается в гостевой VLAN_ID.
4. Если режим проверки подлинности установлен в **multi-sessions**, то PVID не изменяется и весь немаркированный и маркированный трафик, не принадлежащий неавторизованным VLAN от неавторизованных узлов, отправляется в гостевую VLAN.
5. Если 802.1X будет отключен, статическая конфигурация порта сбрасывается.

6. Для получения большей информации см. команду **dot1x host-mode**.

Пример:

Следующий пример разрешает доступ неавторизованных пользователей в гостевой VLAN.

```
console(config)# interface GigabitEthernet 1/0/5  
console(config-if)# dot1x guest-vlan enable
```

1.7. Команда dot1x guest-vlan timeout

Команда **dot1x guest-vlan timeout** устанавливает временную задержку между включением 802.1X (или порта) и добавлением порта в гостевой VLAN. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

dot1x guest-vlan timeout *timeout*

no dot1x guest-vlan timeout

Параметры:

- *timeout* – значение временной задержки в секундах. Диапазон: 30 – 180 с.

Состояние по умолчанию:

Добавление в гостевой VLAN производится немедленно.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Команда имеет значение, если гостевой VLAN включена на порту. Настройка временной задержки добавляет задержку с включением 802.1X (или порта) до момента, когда коммутатор добавит порт в гостевой VLAN.

Пример:

Нижеследующий пример устанавливает значение временной задержки в 60 с.

```
console(config)# dot1x guest-vlan timeout 60
```

1.8. Команда dot1x host-mode

Команда **dot1x host-mode** устанавливает режим работы 802.1X порта для клиентских устройств. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x host-mode { **multi-host** | **single-host** | **multi-session** }

no dot1x host-mode

Параметры:

- **multi-host** – режим допускающий подключение нескольких узлов на один порт;
- **single-host** – режим допускающий подключение только одного узла на порт;
- **multi-session** – режим отдельной аутентификации каждого подключаемого хоста.

Состояние по умолчанию:

По умолчанию включен режим **multi-host**.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. Режим **Single-Host**

Данный режим управляет аутентификацией порта: порт разрешен, если есть авторизованное устройство. В этом режиме может быть только одно авторизованное устройство.

Когда порт не авторизован и гостевой VLAN включен, непомеченный трафик переназначается в гостевой VLAN. Помеченный трафик, если его тэг не относится к гостевому VLAN или не аутентифицированным VLAN, отбрасывается. Если гостевой VLAN не включен в порт, то пропускается только маркированный трафик не аутентифицированным VLAN.

Если порт авторизован, немаркированный и маркированный трафик с авторизованного устройства перенаправляется на основе статического членства VLAN, настроенного на порту. Трафик с других узлов отбрасывается.

Пользователь может указать, что немаркированный трафик с авторизованного узла будет перенаправлен в VLAN, который назначена сервером RADIUS во время процесса аутентификации. В этом случае маркированный трафик отбрасывается, если тэг VLAN не является назначенным RADIUS VLAN или не аутентифицированным VLAN. Более подробно см. команду **dot1x radius-attributes vlan**.

Коммутатор удаляет из FDB все MAC-адреса, полученные на порту, когда его статус аутентификации изменен с авторизованного на неавторизованный.

2. Режим **Multi-Host**

Данный режим управляет статусом аутентификации порта: порт разрешен после авторизации хотя бы одного устройства.

Когда порт не авторизован и гостевой VLAN включен, непомеченный трафик переназначается в гостевой VLAN. Тегированный трафик отбрасывается, если его тег не является тегом гостевого VLAN или не аутентифицированного VLAN. Если гостевой VLAN не разрешен на порту, то пропускается только тегированный трафик не аутентифицированного VLAN.

Когда порт разрешен, нетегированный и тегированный трафик со всех устройств, подключенных к порту разрешен для VLAN статически прописанных на порту.

Пользователь может указать, что нетегированный трафик из авторизованного порта будет назначен в VLAN, который присваивается порту сервером RADIUS во время процесса проверки подлинности. В этом случае любой тегированный трафик отбрасывается, если тег VLAN не принадлежит назначенному RADIUS VLAN или не аутентифицированному VLAN. Более подробно см. команду **dot1x radius-attributes vlan**.

Коммутатор удаляет из FDB все MAC-адреса, полученные на порту, когда его статус аутентификации изменен с авторизованного на неавторизованный.

3. Режим **Multi-Sessions**

В отличие от режимов **single-host** и **multi-host** (режимы на основе порта) данный режим управляет статусом аутентификации для каждого устройства, подключенного к порту (сеансовый режим). Если режим **multi-sessions** настроен на порту, аутентификация производится для каждого устройства отдельно. На порту может быть разрешено любое количество устройств. Команда **dot1x max-hosts** может ограничивать максимально разрешенное количество устройств, разрешенных на этом порту.

Каждому авторизованному устройству требуется правило в TCAM. Если в TCAM нет свободных ресурсов, то аутентификация отклоняется.

При использовании команды **dot1x host-mode** для изменения режима порта на **single-host** или **multi-host**, состояние порта меняется на не авторизованный.

Если команда **dot1x host-mode** изменят режим порта на **multi-sessions**, когда включена проверка подлинности, состояние всех подключенных к порту устройств меняется на неавторизованное.

Чтобы сменить режим порта на **single-host** или **multi-host**, установите порт в состояние принудительно неавторизованного (см. команду **dot1x port-control**), смените режим порта и настройте его на автоматическую авторизацию.

Режим **multi-sessions** не может быть установлен на том же интерфейсе, где применены политики VLAN (Policy Based VLAN), настроенные с помощью следующих команд:

- **switchport general map protocols-group**
- **switchport general map macs-group**

Тег, принадлежащий неаутентифицированному VLAN, всегда пропускается независимо от того, разрешено устройство или нет.

Если на порту разрешен гостевой VLAN, немаркированный и маркированный трафик от неавторизованных устройств, не принадлежащих к неаутентифицированному VLAN, перенаправляется в гостевой VLAN.

Трафик от авторизованных устройств перенаправляется в соответствии со статической конфигурацией порта. Пользователь может указать, что не маркированный и маркированный трафик с авторизованного устройства, не принадлежащего неаутентифицированному VLAN, будет перенаправлен в VLAN, назначенный сервером RADIUS во время процесса аутентификации. Для большей информации см. команду **dot1x radius-attributes vlan**.

Коммутатор не удаляет MAC-адрес устройства из FDB полученный на порту, когда статус порта изменяется с авторизованного на не авторизованный. MAC-адрес будет удален по истечении времени старения.

Пример:

```
console(config)# interface gi 1/0/10
console(config-if)# dot1x host-mode multi-host
```

1.9. Команда dot1x max-hosts

Команда **dot1x max-hosts** задает максимально разрешенное кол-во авторизованных устройств на интерфейсе. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x max-hosts *count*

no dot1x max-hosts

Параметры:

- *count* – Количество максимально разрешенных авторизованных устройств на интерфейсе. Возможно любое 32-битное положительное число.

Состояние по умолчанию:

Нет ограничений.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. По умолчанию, количество разрешенных устройств на интерфейсе не ограничено.
2. Данная команда относится только к режиму **multi-sessions**.
3. По умолчанию количество разрешенных хостов на интерфейсе не ограничено. Чтобы ограничить количество разрешенных хостов, разрешенных на интерфейсе, используйте команду **dot1x max-hosts**.

Пример:

```
console(config)# interface gi 1/0/10
console(config-if)# dot1x max-hosts 6
```

1.10. Команда dot1x max-req

Команда **dot1x max-req** устанавливает максимальное число попыток отправки запроса/идентификационного кадра (при условии отсутствии ответа) по протоколу EAP (Extensible Authentication Protocol) перед перезапуском процесса аутентификации. Использование префикса **no** устанавливает значения по умолчанию.

Синтаксис:

dot1x max-req *count*

no dot1x max-req

Параметры:

- *count* – количество попыток повторной отправки EAP кадров. Диапазон: 1 – 10.

Состояние по умолчанию:

Максимальное количество попыток установлено в 2.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

Значение по умолчанию должно быть изменено только для адаптации к необычным обстоятельствам, таким как ненадежные каналы передачи данных или конкретные поведенческие проблемы с определенными устройствами и серверами проверки подлинности.

Пример:

```
console(config)# interface gi 1/0/10
console(config-if)# dot1x max-req 6
```

1.11. Команда dot1x port-control

Команда **dot1x port-control** служит для управления состояние авторизации порта вручную. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** } [**time-range** *time-range-name*]

Параметры:

- **auto** – включает аутентификацию 802.1X на порту и приводит к переходу его в авторизованное или не авторизованное состояние, в зависимости от результата обмена аутентификацией между устройством и коммутатором;
- **force-authorized** – отключает аутентификацию 802.1X на интерфейсе и переводит порт в авторизованное состояние без какого-либо обмена идентификацией. Порт получает и отправляет трафик без аутентификации на основе 802.1X;
- **force-unauthorized** – запрещает любой доступ через этот порт, переводит его в неавторизованное состояние и игнорирует все попытки аутентификации. Коммутатор не может предоставить сервис аутентификации устройству через этот порт;
- **time-range** *time-range-name* – определяет временной диапазон. Если диапазон не действует, то состояние порта устанавливается в неавторизованный. Диапазон: 1 – 32 символа.

Состояние по умолчанию:

Порт находится в состоянии **force-authorized**.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. Коммутатор удаляет все MAC-адреса, полученные на порту, когда его состояние сменяется с **force-authorized** на любое другое.
2. Рекомендуется отключать режим spanning-tree или включать режим PortFast на портах 802.1X, имеющих режим **auto**, чтобы после успешной аутентификации сразу перейти в режим передачи трафика.

Пример:

```
console(config)# interface gi 1/0/10
console(config-if)# dot1x port-control auto
```

1.12. Команда dot1x radius-attributes vlan

Команда **dot1x radius-attributes vlan** используется для разрешения назначения VLAN на порт сервером RADIUS. Использование префикса «**no**» отключает функцию.

Синтаксис:

dot1x radius-attributes vlan [reject | static]

no dot1x radius-attributes vlan

Параметры:

- **reject** – если сервер RADIUS авторизовал устройство, но не предоставил запрашиваемую VLAN, то запрос устройство отклоняется. Данный параметр применяется по умолчанию.
- **static** – если сервер RADIUS авторизовал устройство, но не предоставил запрашиваемую VLAN, то устройство принимается.

Состояние по умолчанию:

По умолчанию применена команда **dot1x radius-attributes vlan reject**.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. Если RADIUS сервер предоставляет неверную информацию о VLAN, то аутентификация отклоняется.
2. Если RADIUS сервер назначает устройству несуществующий VLAN, то коммутатор создает этот VLAN. VLAN удаляется, когда он больше не используется.

3. Если RADIUS сервер предоставляет действительный VLAN, но порт не принадлежит к этому VLAN, он добавляется в VLAN в качестве выходного не тегированного порта. Когда последнее авторизованное устройство становится не авторизованным или 802.1X отключен на порту, порт исключается из VLAN.
4. Если режим аутентификации установлен в **single-host** или **multi-host**, значение PVID устанавливается в VLAN_ID.
5. Если авторизованный порт в режиме **single-host** или **multi-host** меняет статус на неавторизованный, статическая конфигурация порта сбрасывается.
6. Если режим аутентификации установлен в **multi-sessions**, PVID не изменяется и весь тегированный и не тегированный трафик, не принадлежащий не аутентифицированным VLAN перенаправляются в VLAN используя TCAM.
7. Если последний из авторизованных хостов назначен в VLAN полученную от RADIUS подключен к порту в режиме **multi-sessions**, изменяет статус на неавторизованный, порт удаляется из VLAN, если его конфигурация не статическая.
8. Если 802.1X отключается на порту, то его статическая конфигурация сбрасывается.
9. Если указан параметр **reject** и RADIUS сервер авторизует хост, но сообщение о принятии RADIUS не назначает запрашиваемый VLAN запрашивающему устройству, то аутентификация отклоняется.
10. Если указан параметр **static** и RADIUS сервер авторизует хост, но назначение запрашиваемого VLAN не происходит, аутентификация принимается и трафик с хоста перенаправляется в соответствии со статической конфигурацией порта.
11. Если данная команда используется, когда уже есть авторизованные порты/хосты, то результат ее выполнения вступит в силу при повторной аутентификации устройства. Для повторной проверки подлинности вручную используется команда **dot1x re-authenticate**.
12. Команда не может быть включена в статическую настройку порта одновременно с:
 - a. Multicast TV-VLAN;
 - b. Q-in-Q;
 - c. Voice VLAN.
13. Для большей информации см. описание команды **dot1x host-mode**.

Примеры:

Пример 1.

В данном примере RADIUS сервер назначает авторизуемому устройству пользовательский VLAN. Если сервер не может назначить VLAN, то устройство отклоняется.

```
console(config)# interface gi 1/0/12
console(config-if)# dot1x radius-attributes vlan
```

Пример 2.

В данном примере, если сервер RADIUS не предоставил запрашиваемый VLAN, то авторизуемое устройство все равно принимается, используя статическую конфигурацию порта.

```
console(config)# interface gi 1/0/12
```

```
console(config-if)# dot1x radius-attributes static
```

1.13. Команда dot1x radius-attributes filter-id

Команда **dot1x radius-attributes filter-id** используется для разрешения назначения ACL/QoS-Policy на порт сервером RADIUS. Использование префикса «**no**» отключает функцию.

Синтаксис:

dot1x radius-attributes filter-id

no dot1x radius-attributes filter-id

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

По умолчанию механизм назначения ACL/QoS-Policy на порт выключен.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. Назначение ACL/QoS-Policy на порт работает только в режиме **multi-sessions**.
2. Включение и выключение механизма возможно только если порт находится в состоянии Force-Authorized или Force-Unauthorized.
3. Для большей информации см. описание команды **dot1x host-mode**.

Пример:

```
console(config)# interface gi 1/0/12  
console(config-if)# dot1x radius-attributes filter-id
```

1.14. Команда dot1x re-authenticate

Команда **dot1x re-authenticate** служит для ручного вызова аутентификации 802.1X.

Синтаксис:

dot1x re-authenticate [interface-id]

Параметры:

1. *interface-id* – идентификатор порта

Состояние по умолчанию:

Если идентификатор порта не указан, то команда применяется ко всем интерфейсам.

Режим ИКС:

Привилегированный режим управления.

Пример:

В данном примере выполняется ручная повторная аутентификация устройств подключенных к порту gi 1/0/12

```
console# dot1x re-authenticate gi1/0/12
```

1.15. Команда dot1x reauthentication

Команда **dot1x reauthentication** используется для включения периодической повторной аутентификации устройства. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x reauthentication

no dot1x reauthentication

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Периодическая повторная аутентификация отключена.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

Временной интервал повторной аутентификации задается командой **dot1x timeout reauth-period**.

Пример:

```
console(config)# interface gi 1/0/12  
console(config-if)# dot1x reauthentication
```

1.16. Команда dot1x system-auth-control

Команда **dot1x system-auth-control** включает возможность использования 802.1X на коммутаторе. Использование префикса «**no**» отключает функцию.

Синтаксис:

dot1x system-auth-control

no dot1x system-auth-control

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Функция отключена.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# dot1x system-auth-control
```

1.17. Команда dot1x timeout quiet-period

Команда **dot1x timeout quiet-period** используется для установки временного интервала, в течение которого устройство не пытается выполнить повторный запрос после неудачной попытки аутентификации. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Параметры:

- *seconds* – временной интервал в секундах. Диапазон: 10 - 65535 с.

Состояние по умолчанию:

По умолчанию временной интервал составляет 60 с.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. В течение данного периода устройство не принимает и не инициирует запросы на аутентификацию.
2. Рекомендуется изменять значения по умолчанию для данной команды только для адаптации к необычным обстоятельствам, таким как ненадежные каналы передачи данных или конкретные поведенческие особенности определенных устройств или серверов аутентификации.
3. Чтобы обеспечить устройству более быстрое время отклика, необходимо указать меньшее число, чем значение по умолчанию.
4. Для протокола 802.1X количество неудачных попыток аутентификации на основе MAC адреса равно 1.

Пример:

В данном примере временной интервал устанавливается в 120 с.

```
console(config)# interface gi 1/0/12  
console(config-if)# dot1x timeout quiet-period 120
```

1.18. Команда `dot1x timeout reauth-period`

Команда **`dot1x timeout reauth-period`** используется для установки количества секунд между попытками повторной аутентификации. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

`dot1x timeout reauth-period` *seconds*

`no dot1x timeout reauth-period`

Параметры:

- *seconds* – количество секунд между попытками повторной аутентификации, диапазон: 300 – 4294967295.

Состояние по умолчанию:

По умолчанию временной интервал составляет 3600 с.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

Команда применима только к методу аутентификации 802.1x.

Пример:

```
console(config)# interface gi1/0/12
console(config-if)# dot1x timeout reauth-period 5000
```

1.19. Команда `dot1x timeout server-timeout`

Команда **`dot1x timeout server-timeout`** устанавливает временной интервал, в течении которого ожидается ответ от сервера аутентификации. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

`dot1x timeout server-timeout` *seconds*

`no dot1x timeout server-timeout`

Параметры:

- *seconds* – время в секундах, в течении которого устройство ожидает ответа от сервера аутентификации (диапазон: 1 – 65535).

Состояние по умолчанию:

По умолчанию интервал составляет 30 с.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

Фактический период ожидания может быть определен путем сравнения значения, указанного данной командой с результатом умножения количества повторных попыток, заданных командой **radius-server retransmit** на период ожидания указанный в этой же команде и выбора меньшего из этих двух значений.

Пример:

В следующем примере устанавливается временной интервал между повторными попытками аутентификации в 3600 с.

```
console(config)# interface gil/0/12
console(config-if)# dot1x timeout server-timeout 3600
```

1.20. Команда dot1x timeout sup-timeout

Команда **dot1x timeout sup-timeout** устанавливает время, в течении которого ожидается ответный кадр на запрос EAP (Extensible Authentication Protocol) от клиента до того, как будет инициирована повторная отправка. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Параметры:

- *seconds* – время ожидания в секундах (диапазон: 1 – 65535).

Состояние по умолчанию:

Временной период по умолчанию: 30 с.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

Значение по умолчанию для этой команды должно быть изменено только для адаптации к необычным обстоятельствам, таким как ненадежные каналы передачи данных или конкретные поведенческие особенности с определенными устройствами и серверами проверки подлинности.

Данная команда применяется только к методу аутентификации 802.1x.

Пример:

В данном примере устанавливается время ожидания в 3600 с.

```
console(config)# interface gil/0/12
console(config-if)# dot1x timeout supp-timeout 3600
```

1.21. Команда `dot1x timeout tx-period`

Команда **dot1x timeout tx-period** устанавливает временной интервал, в течении которого устройство ожидает ответа на запрос/идентификационный код EAP (Extensible Authentication Protocol) от клиента до повторной отправки запроса. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Параметры:

- *seconds* – временной интервал в секундах (диапазон: 30 – 65535).

Состояние по умолчанию:

Временной интервал по умолчанию составляет 30 с.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

Значение по умолчанию для этой команды должно быть изменено только для адаптации к необычным обстоятельствам, таким как ненадежные каналы передачи данных или конкретные поведенческие особенности с определенными устройствами и серверами проверки подлинности.

Данная команда применяется только к методу аутентификации 802.1x.

Пример:

В данном примере время ожидания устанавливается в 60 с.

```
console(config)# interface gi1/0/12
console(config-if)# dot1x timeout tx-period 60
```

1.22. Команда `dot1x traps authentication failure`

Команда **dot1x traps authentication failure** используется для включения отправки событий SNMP при неудачной попытке аутентификации 802.1X. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x traps authentication failure [{ **802.1x** | **mac** } [{ **802.1x** | **mac** }]]

no dot1x traps authentication failure

Параметры:

- **802.1X** – разрешает события SNMP для аутентификации на основе 802.1X;

- **mac** – разрешает события SNMP для аутентификации на основе mac;

Состояние по умолчанию:

Отправка SNMP событий запрещена.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Допускается любая комбинация параметров. Для успешного выполнения команды необходимо указать хотя бы один параметр.
2. На отправку событий SNMP установлено временное ограничение: не более одного события SNMP каждые 10 с.

Пример:

В данном примере разрешается отправка события SNMP, в случае если MAC-адрес не может быть авторизован с помощью mac 802.1X

```
console(config)# interface gil/0/10  
console(config-if)# dot1x traps authentication failure mac
```

1.23. Команда dot1x traps authentication quiet

Команда **dot1x traps authentication quiet** используется для включения возможности отправки событий SNMP, когда состояние хоста переводится в состояние «молчания», при превышении максимального количества попыток входа в систему. Использование префикса «**no**» отключает отправку событий SNMP.

Синтаксис:

dot1x traps authentication quiet

no dot1x traps authentication quiet

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Отправка событий SNMP запрещена.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. События SNMP будут отправлять только после того, как клиент настроен на состояние «молчания» после максимального количества последовательных попыток авторизации.
2. Данная команда применяется к web-аутентификации.

3. На отправку событий SNMP установлено ограничение - не более одного события SNMP в течении 10 с.

Пример:

```
console(config)# dot1x traps authentication quiet
```

1.24. Команда dot1x traps authentication success

Команда **dot1x traps authentication success** используется для включения возможности отправки событий SNMP при успешной аутентификации 802.1X. Использование префикса «**no**» отключает отправку событий SNMP.

Синтаксис:

dot1x traps authentication success [{ 802.1x | mac } [{ 802.1x | mac }]]

no dot1x traps authentication success

Параметры:

- **802.1X** – разрешает события SNMP для аутентификации на основе 802.1X;
- **mac** – разрешает события SNMP для аутентификации на основе mac;

Состояние по умолчанию:

Отправка событий SNMP запрещена.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Допускается любая комбинация параметров. Для успешного выполнения команды необходимо указать хотя бы один параметр.
2. На отправку событий SNMP установлено временное ограничение: не более одного события SNMP каждые 10 с.

Пример:

В данном примере включается отправка событий SNMP после успешной аутентификации по mac-адресу в 802.1X

```
console(config)# dot1x traps authentication success mac
```

1.25. Команда dot1x unlock client

Команда **dot1x unlock client** служит для ручной разблокировки заблокированного ранее клиента (в режиме «молчания»).

Синтаксис:

dot1x unlock client interface-id mac-address

Параметры:

- *interface-id* – идентификатор интерфейса к которому подключен клиент
- *mac-address* – MAC-адрес клиента

Состояние по умолчанию:

Клиент остается заблокированным до истечения времени «молчания».

Режим ИКС:

Привилегированный режим управления.

Примечание:

Команда используется для ручной разблокировки клиента, который был заблокирован при превышении количества максимально допустимых попыток проверки подлинности и был переведен в режим «молчания». Если клиент не находится в режиме «молчания», команда не применяется.

Пример:

```
console# dot1x unlock client gil/0/12 04:62:73:6d:43:4c
```

1.26. Команда dot1x violation-mode

Команда **dot1x violation-mode** определяет действие, которое необходимо предпринять, в случае попытки доступа неавторизованного хоста на авторизованный порт в режиме **single-host**. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

dot1x violation-mode { restrict | protect | shutdown } [trap seconds]

no dot1x violation-mode

Параметры:

- **restrict** – генерирует SNMP trap, когда клиент MAC-адрес которого не совпадает с MAC-адресом запрашивающего устройства пытается получить доступ к интерфейсу. Минимальное время между отправкой SNMP trap составляет 1 с. Кадры запросов передаются, но их исходные адреса не запоминаются;
- **protect** – кадры, в которых исходные адреса не совпадают с адресом запрашивающего устройства отбрасываются;
- **shutdown** – кадры в которых исходные адреса не совпадают с адресом запрашивающего устройства отбрасываются, а порт отключается;
- **trap seconds** – задает время между последовательными отправками SNMP trap. Если количество секунд равно 0, отправка SNMP trap отключена. Если параметр не указан, то используются установки по умолчанию. Допустимое значение 0 – 1000000.

Состояние по умолчанию:

По умолчанию используется режим **protect**.

Если параметр **trap seconds** не указан, то для режима **restrict** заданное время равно 1 с, а для остальных режимов – 0 с.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. Команда применяется только для порта в режиме **single-host**.
2. BPDU пакеты, MAC-адреса которых не совпадают с MAC-адресом запрашивающего устройства не отбрасываются в режиме **protect**.
3. BPDU пакеты, MAC-адреса которых не совпадают с MAC-адресом запрашивающего устройства вызывают выключение порта в режиме **shutdown**.

Пример:

```
console(config)# interface gil/0/15
console(config-if)# dot1x violation-mode shutdown
```

1.27. Команда show dot1x

Команда **show dot1x** отображает на экране информацию о 802.1X для всех интерфейсов или только определенного.

Синтаксис:

show dot1x [{ **interface interface-id** | **detailed** }]

Параметры:

- **interface-id** – идентификатор Ethernet интерфейса или ООВ порта;
- **detailed** – отображает информацию о неучтенных портах в дополнение к текущим портам.

Состояние по умолчанию:

Выводит информацию обо всех портах. Если параметр **detailed** не используется, отображаются только текущие порты.

Режим ИКС:

Привилегированный режим управления.

Пример:

В следующем примере отображаются данные аутентификации для всех интерфейсов, на которых включен 802.1x (фрагмент вывода).

```
console# show dot1x

Authentication is disabled
Authenticating Servers: Radius
Unauthenticated VLANs:
Authentication failure traps are disabled
Authentication success traps are disabled
```

```
Authentication quiet traps are disabled

gil/0/1
Host mode: multi-host
Authentication methods: 802.1X
Port Administrated Status: force-authorized
Guest VLAN: disabled
VLAN Radius Attribute: disabled
Open access: disabled
Server timeout: 30 sec
Port Operational Status: authorized
Reauthentication is disabled
Reauthentication period: 3600 sec
Silence period: 0 sec
Quiet period: 60 sec
Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  Max req: 2
Authentication success: 0
Authentication fails: 0

gil/0/2
Host mode: multi-host
Authentication methods: 802.1X
Port Administrated Status: force-authorized
Guest VLAN: disabled
VLAN Radius Attribute: disabled
Open access: disabled
Server timeout: 30 sec
Port Operational Status: authorized*
* Port is down or not present
Reauthentication is disabled
Reauthentication period: 3600 sec
Silence period: 0 sec
Quiet period: 60 sec
Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  Max req: 2
Authentication success: 0
Authentication fails: 0
```

Ниже описаны наиболее важные поля в выводе:

- **Port** – идентификатор порта
- **Host mode** – сконфигурированный режим аутентификации порта. Допустимые значения: **single-host**, **multi-host**, **multi-sessions**
- **Authentication methods** – режим аутентификации сконфигурированный на порту. Допустимые значения: **802.1x**, **mac**, **web**
- **Port Administrated status** – административный (сконфигурированный) режим порта. Допустимые значения: **force-authorized**, **force-unauthorized**, **auto**.

- **Port Operational status** – режим работы порта (фактический). Допустимые значения: **authorized** или **unauthorized**.
- **Username** – имя пользователя, представляющее идентификатор просителя. Если порт авторизован, то отображается имя текущего пользователя. Если порт не авторизован, то отображается имя последнего успешно авторизованного пользователя.
- **Quiet period** – количество секунд, в течении которых устройство находится в режиме «молчания» после неудачного обмена аутентификацией (например, клиент предоставил неверный пароль).
- **Silence period** – количество секунд, в течении которых клиент в режиме «молчания» не отправляет трафик, по истечении которых состояние клиента будет изменено на неавторизованное.
- **Tx period** – количество секунд, в течении которых устройство ожидает от клиента ответа на запрос/идентификатор протокола EAP (Extensible Authentication Protocol), перед повтор-ной отправкой запроса.
- **Max req** – максимальное количество повторов отправки кадра запроса EAP (при условии отсутствия ответа) клиенту перед перезапуском процесса аутентификации.
- **Supplicant timeout** – количество секунд, в течении которых устройство ожидает ответа на кадр EAP-запроса от клиента, до повторной отправки.
- **Server timeout** – количество секунд, в течении которых устройство ожидает ответа от сервера аутентификации перед повторной отправкой запроса.
- **Session time** – прошедшее время с момента авторизации (в формате **HH:MM:SS**).
- **MAC address** – MAC-адрес запрашивающего устройства.
- **Authentication success** – количество успешных попыток аутентификации.
- **Authentication fails** – количество неудачных попыток аутентификации.

1.28. Команда show dot1x locked clients

Команда **show dot1x locked clients** отображает на экране информацию о заблокированных клиентах, находящихся в режиме «молчание».

Синтаксис:

show dot1x locked clients

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show dot1x locked clients

Port
-----
gil/0/1
gil/0/1
```

```
gil/0/2

MAC Address
-----
0008.3b79.8787
0008.3b89.3128
0008.3b89.3129

Remaining Time
-----
20
40
10
```

1.29. Команда show dot1x statistics

Команда **show dot1x statistics** выводит на экран статистику 802.1X для определенного порта.

Синтаксис:

show dot1x statistics interface *interface-id*

Параметры:

- *interface-id* – идентификатор Ethernet или ООВ порта.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show dot1x statistics interface gil/0/10
EapolFramesRx:          11
EapolFramesTx:          12
EapolStartFramesRx:    1
EapolLogoffFramesRx:   1
EapolRespIdFramesRx:   3
EapolRespFramesRx:     6
EapolReqIdFramesTx:    3
EapolReqFramesTx:      6
InvalidEapolFramesRx:  0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource:  00:08:78:32:78:98
```

Наиболее важные поля в выводе статистики

- **EapolFramesRx** - Количество действительных кадров EAPOL любого типа, которые были получены аутентификатором.
- **EapolFramesTx** - Количество кадров EAPOL любого типа, которые были переданы аутентификатором.

- **EapolStartFramesRx** - Количество кадров EAPOL Start, которые были получены аутентификатором.
- **EapolLogoffFramesRx** - Количество кадров EAPOL Stop, которые были получены аутентификатором.
- **EapolRespIdFramesRx** - Количество кадров EAP Resp/Id, которые были получены аутентификатором.
- **EapolRespFramesRx** - Количество действительных кадров ответа EAP (кроме кадров **Resp/Id**), которые были получены аутентификатором.
- **EapolReqIdFramesTx** - Количество кадров EAP Req/Id, которые были переданы аутенти-фикатором.
- **EapolReqFramesTx** - Количество кадров запроса EAP (кроме кадров Req/Id), которые были переданы аутентификатором.
- **InvalidEapolFramesRx** - Количество кадров EAPOL, которые были получены аутентификатором, в которых тип кадра не распознается.
- **EapLengthErrorFramesRx** - Количество кадров EAPOL, которые были получены аутентифика-тором, в котором поле Packet Body Length недействительно.
- **LastEapolFrameVersion** - Номер версии протокола, указанный в последнем полученном кадре EAPOL.
- **LastEapolFrameSource** - MAC-адрес источника, указанный в последнем полученном кадре EAPOL.

1.30. Команда show dot1x users

Команда **show dot1x users** выводит на экран авторизованных 802.1X на данный момент пользователей.

Синтаксис:

show dot1x users [username *username*]

Параметры:

- **username *username*** – задает конкретное имя пользователя. Длина: 1 – 160 символов.

Состояние по умолчанию:

Выводит список всех авторизованных пользователей.

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1:

В данном примере отображаются все авторизованные пользователи.

```
console# show dot1x users

Port
-----
te1/0/1
te1/0/2
te1/0/2

Username
-----
Bob
Allan
John

MAC Address
-----
0008.3b71.1111
0008.3b79.8787
0008.3baa.0022

Auth Method
-----
802.1x
802.1x
802.1x

Auth Server
-----
Remote
Remote
Remote

Session Time
-----
09:01:00
00:11:12
00:27:16

VLAN
---
1020
```

Пример 2:

В данном примере отображается информация об авторизованном пользователе Bob

```
console# show dot1x users username Bob
```

```
Port
```

```
-----  
te1/0/1
```

```
Username
```

```
-----  
Bob
```

```
MAC Address
```

```
-----  
0008.3b71.1111
```

```
Auth Method
```

```
-----  
802.1x
```

```
Auth Server
```

```
-----  
Remote
```

```
Session Time
```

```
-----  
09:01:00
```

```
VLAN
```

```
-----  
1020
```

2. КОМАНДЫ AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA)

2.1. Команда aaa authentication login

Команда **aaa authentication login** используется для настройки одного или нескольких методов аутентификации во время входа в систему. Использование префикса «**no**» устанавливает метод аутентификации по умолчанию.

Синтаксис:

```
aaa authentication login { default | list-name } method1 [ method2 ... ]
```

```
no aaa authentication login { default | list-name }
```

Параметры:

- **default** – использует методы аутентификации, которые следуют за этим аргументом как список методов по умолчанию, когда пользователь входит в систему (список не именован);
- *list-name* – задает имя списка методов аутентификации, активируемого при входе пользователя в систему (длина: 1 – 12 символов);
- *method1* [*method2* ...] – задает список методов, которые пытается выполнить алгоритм аутентификации (в указанной последовательности). Каждый дополнительный метод аутентификации используется только в случае, если предыдущий метод возвращает ошибку, а не в случае отказа аутентификации. Если вы хотите, чтобы аутентификация была успешной, даже если все методы возвращают ошибку, в качестве последнего метода в команде используйте параметр **none**.

Список доступных методов

- **enable** - Для аутентификации используется пароль привилегированного режима.
- **line** - Для аутентификации используется пароль линии.
- **local** - Для аутентификации используются локальные учетные записи.
- **none** - Аутентификация не используется.
- **radius** - Для аутентификации используется список RADIUS серверов.
- **tacacs** - Для аутентификации используется список TACACS+ серверов.

Состояние по умолчанию:

Если ни один метод не задан, то по умолчанию используются локальные учетные записи пользователей. Это аналогично вводу команды **aaa authentication login default local**.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Для создания списка методов проверки подлинности, команда вводится с параметром *list-name*, где *list-name* – любая символьная строка. В аргументе метода

указан список методов, которые алгоритм аутентификации пытается использовать в указанной последовательности.

2. Список по умолчанию и именованный список, созданный с помощью данной команды используется в команде **login authentication**.

Команда **no aaa authentication login list-name** удаляет список, только если на него не ссылается другая команда.

Пример:

В данном примере заданный список методов используется для проверки подлинности при входе в линию console.

```
console(config)# aaa authentication login auth-list radius local
none
console(config)# line console
console(config-line)# login authentication auth-list
```

2.2. Команда aaa authentication enable

Команда **aaa authentication enable** устанавливает один или несколько методов аутентификации входа в привилегированный режим. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

aaa authentication enable { default | list-name } method1 [method2 ...]

no aaa authentication enable { default | list-name }

Параметры:

- **default** – использует методы аутентификации, которые следуют за этим аргументом как список методов по умолчанию, когда пользователь входит в систему (список не именован);
- *list-name* – задает имя списка методов аутентификации, активируемого при входе пользователя в систему (длина: 1 – 12 символов);
- *method1 [method2 ...]* – задает список методов, которые пытается выполнить алгоритм аутентификации (в указанной последовательности). Каждый дополнительный метод аутентификации используется только в случае, если предыдущий метод возвращает ошибку, а не в случае отказа аутентификации. Если вы хотите, чтобы аутентификация была успешной, даже если все методы возвращают ошибку, в качестве последнего метода в команде используйте параметр **none**.

Список доступных методов

- **enable** - Для аутентификации используется пароль привилегированного режима.
- **line** - Для аутентификации используется пароль линии.
- **local** - Для аутентификации используются локальные учетные записи.
- **none** - Аутентификация не используется.
- **radius** - Для аутентификации используется список RADIUS серверов.

- **tacacs** - Для аутентификации используется список TACACS+ серверов.

Состояние по умолчанию:

Команда **enable password** определяет метод аутентификации по умолчанию. Это эквивалентно выполнению команды **aaa authentication enable default enable**.

При подключении через консольный порт привилегированный пароль используется если существует. Если пароль не установлен, то аутентификация по-прежнему выполняется успешно. Это эквивалентно выполнению команды **aaa authentication enable default enable none**.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

- Для создания списка методов проверки подлинности, команда вводится с параметром *list-name*, где *list-name* – любая символьная строка. В аргументе метода указан список методов, которые алгоритм аутентификации пытается использовать в указанной последовательности.
- Список по умолчанию и именованный список, созданный с помощью данной команды используется в команде **login authentication**.
- Команда **no aaa authentication enable list-name** удаляет список, только если на него не ссылается другая команда.

Пример:

```
console(config)# aaa authentication enable enable-list radius none
console(config)# line console
console(config-line)# enable authentication enable-list
```

2.3. Команда login authentication

Команда **login authentication** задает список методов аутентификации входа для удаленных сеансов Telnet, SSH или через консольный порт. Использование префикса «**no**» устанавливает метод аутентификации по умолчанию.

Синтаксис:

login authentication { default | list-name }

no login authentication

Параметры:

- **default** – используется неименованный список по умолчанию, заданный командой **aaa authentication login**;
- *list-name* – имя списка созданного ранее командой **aaa authentication login**.

Состояние по умолчанию:

Применяется параметр **default**

Режим ИКС:

Режим конфигурации линии

Пример:

```
console(config)# line console
console(config-line)# login authentication default
```

2.4. Команда enable authentication

Команда **enable authentication** используется для указания одного или нескольких методов доступа к привилегированному уровню доступа, для удаленных сеансов Telnet, SSH или через консольный порт. Использование префикса **no** устанавливает метод доступа по умолчанию.

Синтаксис:

enable authentication { default | *list-name* }

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

Параметры:

- **default** – используется неименованный список по умолчанию, заданный командой **aaa authentication login**;
- *list-name* – имя списка созданного ранее командой **aaa authentication login**.

Состояние по умолчанию:

Применяется параметр **default**

Режим ИКС:

Режим конфигурации линии

Пример:

```
console(config)# line console
console(config-line)# enable authentication default
```

2.5. Команда ip http authentication

Команда **ip http authentication** используется для задания методов аутентификации для доступа к HTTP серверу. Использование префикса **no** устанавливает метод аутентификации по умолчанию.

Синтаксис:

ip http authentication aaa login-authentication *method1* [*method2* ...]

no ip http authentication aaa login-authentication

Параметры:

- *method1* [*method2 ...*] – задает список методов, которые пытается выполнить алгоритм аутентификации (в указанной последовательности). Каждый дополнительный метод аутентификации используется только в случае, если предыдущий метод возвращает ошибку, а не в случае отказа аутентификации. Если вы хотите, чтобы аутентификация была успешной, даже если все методы возвращают ошибку, в качестве последнего метода в команде используйте параметр **none**.

Список доступных методов

- **enable** - Для аутентификации используется пароль привилегированного режима.
- **line** - Для аутентификации используется пароль линии.
- **local** - Для аутентификации используются локальные учетные записи.
- **none** - Аутентификация не используется.
- **radius** - Для аутентификации используется список RADIUS серверов.
- **tacacs** - Для аутентификации используется список TACACS+ серверов.

Состояние по умолчанию:

По умолчанию используется локальная база пользователей. Это эквивалентно команде **ip http authentication local**.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip http authentication aaa login-authentication  
radius none
```

2.6. Команда show authentication methods

Команда **show authentication methods** выводит на экран информацию о методах аутентификации.

Синтаксис:

show authentication methods

Параметры:

Дополнительные параметры отсутствуют

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show authentication methods  
  
Login Authentication Method Lists  
-----  
Default                               : Local
```

auth-list		: Radius	Local	None
Enable Authentication Method Lists				

Default		: Enable	None	
enable-list		: Radius	None	
Line	Login Method List		Enable Method List	
-----	-----		-----	
Console	Default		Default	
Telnet	Default		Default	
SSH	Default		enable-list	
http		: Radius	Local	None
https		: Radius	Local	None
dot1x		: Radius		

2.7. Команда password

Команда **password** используется для задания пароля в линии (Telnet, SSH или console). Использование префикса «**no**» сбрасывает установленный пароль.

Синтаксис:

password *password* [**encrypted**]

no password

Параметры:

- *password* – задаваемый пароль (длина: 1 – 159 символов);
- **encrypted** – указывает что пароль зашифрован и скопирован с конфигурации другого устройства.

Состояние по умолчанию:

Пароль не задан.

Режим ИКС:

Режим конфигурации линии

Пример:

```
console(config)# line telnet
console(config-line)# password secret
```

2.8. Команда enable password

Команда **enable password** используется для задания локального пароля обычного и привилегированного режима. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

enable password [*level privilege-level*] { *unencrypted-password* | **encrypted** *encrypted-password* }

no enable password [*level privilege-level*]

Параметры:

- **level privilege-level** – уровень для которого применяется пароль. Если уровень не указан, то по умолчанию уровень 15. Диапазон: 1-15;
- *unencrypted-password* – строка пароля. Длина: 1 – 159 символов;
- **encrypted** *encrypted-password* – указывает что пароль зашифрован. Данный параметр используется для указания что пароль уже зашифрован (например скопирован из другого файла конфигурации). Длина: 1 – 40 символов.

Состояние по умолчанию:

Без указания в команде уровня доступа, по умолчанию пароль будет задан для 15 уровня.

Пароль шифруется.

Пароль по умолчанию: **admin**.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

- Когда администратор создает новый пароль для привилегированного режима, этот пароль шифруется автоматически и сохраняется в файле конфигурации. Независимо от того, как был введен пароль, в конфигурации он отображается с ключевым словом **encrypted** и зашифрованным.
- Для копирования шифрованного пароля с одного устройства на другое, при вводе команды необходимо добавить ключевое слово **encrypted** перед зашифрованным паролем. Таким образом можно создать одинаковый enable пароль на нескольких устройствах.
- По умолчанию пароли шифруются. Ключевое слово *encrypted* необходимо использовать только в случае ввода ранее зашифрованного пароля.

Примеры:

Пример 1. В данном примере вводится ранее зашифрованный пароль. Для его использования пользователь должен знать его незашифрованную форму.

```
console(config)# enable password encrypted  
4b529f21c93d4706090285b0c10172eb0
```

Пример 2. В данном примере устанавливается незашифрованный пароль для 7 уровня доступа. В конфигурационном файле пароль будет зашифрован.

```
console(config)# enable password level 7 let-me-in
```

2.9. Команда `service password-recovery`

Команда **`service password-recovery`** используется для включения механизма восстановления утерянного пароля. Этот механизм позволяет администратору с физическим доступом к консольному порту войти в меню загрузки и запустить процесс восстановления пароля. Использование префикса «**no**» отключает механизм. Когда механизм отключен, доступ в загрузочное меню по-прежнему возможен и администратор может вновь инициировать механизм восстановления. Разница в том, что в этом случае все файлы конфигурации и пользовательские файлы удаляются. На терминал будет выведено сообщение: “All the configuration and user files were removed” («Все файлы конфигурации и пользователя удалены»).

Синтаксис:

`service password-recovery`

`no service password-recovery`

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Механизм восстановления пароля включен.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Если механизм восстановления пароля включен, администратор может получить доступ к загрузочному меню и запустить восстановление пароля. Все файлы конфигурации и пользовательские файлы сохраняются.
2. Если механизм восстановления пароля выключен, администратор может получить доступ через загрузочное меню и запустить процесс восстановления. Файлы конфигурации и пользовательские файлы удаляются.

Пример:

```
console(config)# no service password-recovery
Note that choosing to use Password recovery option in the Boot Menu
during
the boot process will remove the configuration files and the user
files.
Would you like to continue ? (Y/N) [N]
```

2.10. Команда `username`

Команда **`username`** создает локального пользователя устройства. Использование префикса **`no`** удаляет пользователя.

Синтаксис:

username *name* **nopassword**

username *name* [**privilege** *privilege-level*] { *unencrypted-password* | **encrypted** *encrypted-password* }

no username *name*

Параметры:

- *name* – имя пользователя. Длина: 1 – 20 символов;
- **nopassword** – для входа этого пользователя пароль не требуется;
- **password** *unencrypted-password* – задает пароль для пользователя. Пароль вводится как строка символов. Длина: 1 – 64 символа.
- **encrypted** *encrypted-password* – указывает, что пароль вводится в MD5 зашифрованном. Используется для переноса зашифрованных паролей с другого устройства. Длина: 1 – 40 символов;
- **privilege** *privilege-level* – задает уровень привилегий пользователя. Если параметр не задан, то присваивается 15 уровень. Диапазон: 1 – 15.

Состояние по умолчанию:

По умолчанию в системе заведен пользователь **admin** с паролем **admin**.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Последний пользователь с уровнем привилегий 15 (не зависимо от того, является ли он пользователем по умолчанию или заведенным вручную) не может быть удален.

Примеры:

Пример 1. В данном примере создается пользователь tom с паролем 1234 и уровнем привилегий по умолчанию (15).

```
console(config)# username tom password 1234
```

Пример 2. В данном примере создается пользователь jerry, с уровнем привилегий 15. Пароль взят с другого коммутатора и вводится в зашифрованном виде.

```
console(config)# username jerry privilege 15 encrypted  
4b529f21c93d4706090285b
```

2.11. Команда show users accounts

Команда **show users accounts** выводит на экран информацию о локальных пользователях устройства.

Синтаксис:

show users accounts

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Отсутствует.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show users accounts
```

UserName	Privilege	Password Expiry date	Lockout
tom	1	-	-
ttt	1	-	-
admin	15	-	-

2.12. Команда aaa accounting login

Команда **aaa accounting login** используется для включения функции учета сеансов управления устройством. Использование префикса **no** отключает учет сеансов.

Синтаксис:

aaa accounting login start-stop group { radius | tacacs+ }

no aaa accounting login start-stop

Параметры:

- **group radius** – для учета используется RADIUS сервер;
- **group tacacs+** - для учета используется TACACS+ сервер.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Команда включает запись сеанса управления устройством (Telnet, SSH, serial и WEB, кроме SNMP).
2. Запись осуществляется только для пользователей, которые были идентифицированы сервером (например пользователь, который был зарегистрирован с паролем линии не учитывается).
3. Если учетная запись активирована, устройство отправляет сообщения start/stop в логи на сервер RADIUS, когда пользователь регистрируется в системе.
4. Для выбора сервера RADIUS/TACACS+ коммутатор использует настроенные приоритеты доступных серверов RADIUS/TACACS+.

Поддерживаемые атрибуты учета RADIUS и в каких сообщениях они отправляются коммутатором:

Наименование атрибута	Сообщение о начале события	Сообщение о конце события	Описание
User-Name (1)	Да	Да	Идентификатор пользователя.
NAS-IP-Address (4)	Да	Да	IP-адрес коммутатора, который используется для сеанса связи с сервером RADIUS.
Class (25)	Да	Да	Произвольное значение, включается во все пакеты учета сеанса связи.
Called-Station-ID (30)	Да	Да	IP-адрес коммутатора, который используется для сеанса управления.
Calling-Station-ID (31)	Да	Да	IP-адрес пользователя.
Acct-Session-ID (44)	Да	Да	Уникальный идентификатор учета.
Acct-Authentic (45)	Да	Да	Указывает, как запрашивающий был идентифицирован.
Acct-Session-Time (46)	Нет	Да	Указывает длительность сеанса пользователя.
Acct-Terminate-Cause(49)	Нет	Да	Указывает причину прекращения сеанса.

Аргументы учета TACACS+ и в каких сообщениях они отправляются коммутатором

Наименование аргумента	Сообщение о начале события	Сообщение о конце события	Описание
task_id	Да	Да	Уникальный идентификатор учетной записи.
user	Да	Да	Имя пользователя используемое для аутентификации.
rem-addr	Да	Да	IP-адрес пользователя.
elapsed-time	Нет	Да	Продолжительность сеанса пользователя.
reason	Нет	Да	Причина прекращения сеанса.

Пример:

```
console(config)#aaa accounting login start-stop group radius
```

2.13. Команда aaa accounting dot1x

Команда **aaa accounting dot1x** используется для включения учета сеансов 802.1X. Использование префикса «no» отключает учет.

Синтаксис:

aaa accounting dot1x start-stop group radius

no aaa accounting dot1x start-stop

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Команда включает запись сессий 802.1X.
2. Если учет активирован, устройство отправляет сообщения start/stop на сервер RADIUS, когда пользователь входит/выходит в сеть.
3. Для выбора RADIUS сервера, коммутатор использует настроенные приоритеты доступных RADIUS серверов.
4. Если новое запрашивающее устройство заменяет старое (даже если состояние порта остается авторизованным), ПО отправляет сообщение stop для старого устройства и start для нового.
5. В режиме нескольких сеансов (**dot1x host-mode multi-sessions**), ПО отправляет сообщения start/stop для каждого авторизованного устройства.
6. В режиме нескольких хостов (**dot1x host-mode multi-host**), ПО отправляет сообщения start/stop только для устройства, прошедшего авторизацию.
7. ПО не отправляет сообщения start/stop если порт находится в состоянии **force-authorized**.
8. ПО не отправляет сообщения start/stop для устройств в гостевой VLAN или не авторизованных VLAN.

Поддерживаемые атрибуты учета RADIUS и в каких сообщениях они отправляются коммутатором:

Наименование атрибута	Сообщение о начале события	Сообщение о конце события	Описание
User-Name (1)	Да	Да	Идентификатор запрашивающего устройства.
NAS-IP-Address (4)	Да	Да	IP адрес коммутатора, который используется для связи с RADIUS сервером.

NAS-Port (5)	Да	Да	Порт коммутатора с которого зарегистрировалось устройство.
Class (25)	Да	Да	Произвольное значение, которое включено во все пакеты сеанса.
Called-Station-ID (30)	Да	Да	MAC адрес коммутатора.
Calling-Station-ID (31)	Да	Да	MAC адрес запрашивающего устройства.
Acct-Session-ID (44)	Да	Да	Уникальный идентификатор учета.
Acct-Authentic (45)	Да	Да	Указывает как устройство было аутентифицировано.
Acct-Session-Time (46)	Нет	Да	Отображает время сеанса устройства.
Acct-Terminate-Cause (49)	Нет	Да	Указывает причину прекращения сессии.
Nas-Port-Type (61)	Да	Да	Указывает тип физического порта устройства.

Пример:

```
console(config)# aaa accounting dot1x start-stop group radius
```

2.14. Команда show accounting

Команда **show accounting** служит для вывода на экран информации о типе учета, включенном на коммутаторе.

Синтаксис:

show accounting

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show accounting  
  
Login: Radius  
802.1x: Disable
```

2.15. Команда password complexity enable

Команда **password complexity enable** служит для включения режима проверки минимальной сложности пароля. Использование префикса «**no**» отключает режим.

Синтаксис:

password complexity enable

no password complexity enable

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Режим **password complexity enable** включен.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Если режим включен, то пароль должен соответствовать следующим требованиям:
 - минимальная длина – 8 символов;
 - должен содержать не менее 3 классов символов (заглавные и строчные буквы, цифры и специальные символы доступные на стандартной клавиатуре);
 - отличаться от текущего пароля;
 - не содержит повторяющегося более 3-х раз подряд одного символа;
 - не повторяет имя пользователя, его имя набранное в обратном порядке или любой другой комбинации символов из имени;
 - не повторяет имя производителя, его имя набранное в обратном порядке или любой другой комбинации символов.
2. Все вышеприведенные атрибуты сложности пароля могут быть изменены с помощью команд описанных в данном разделе.
3. Если ранее были заданы другие настройки сложности пароля, то при применении данной команды предыдущие настройки не уничтожаются. Команда работает как переключатель.

Пример:

```
console(config)# passwords complexity enable
console(config)# exit
console# show passwords configuration

Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 8 characters
Minimal classes: 3
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
```

```
New password must be different than the user name: Enabled  
New password must be different than the manufacturer name: Enabled
```

2.16. Команда password complexity

Команда **password complexity** используется для настройки минимальных требований к паролю, после включения функции командой **password complexity enable**. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

```
password complexity { min-length number | min-classes number | not-current | no-repeat number | not-username | not-manufacturer-name }
```

```
no password complexity { min-length | min-classes | not-current | no-repeat | not-username | not-manufacturer-name }
```

Параметры:

- **min-length** *number* – задает минимальную длину пароля. Диапазон: 1 – 64;
- **min-classes** *number* – минимальное количество классов символов (буквы верхнего и нижнего регистра, числа, специальные символы). Диапазон: 0 – 4;
- **not-current** – указывает, что новый пароль не может совпадать с текущим;
- **no-repeat** *number* – задает максимальное количество символов, которое может повторяться в пароле. Значение 0 указывает, что для повторяющихся символов нет ограничений. Диапазон: 0 – 16;
- **not-username** – указывает, что пароль не может повторять имя пользователя, обратное его написание или любой другое сочетание символов;
- **not-manufacturer-name** – указывает, что пароль не может повторять название производителя, обратное его написание или любое другое сочетание символов.

Состояние по умолчанию:

Минимальная длина, символов: 8.

Количество классов символов: 3.

Количество повторений символов: 3

Все остальные элементы по умолчанию включены.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# passwords complexity min-classes 4
```

2.17. Команда password aging

Команда **password aging** служит для установки срока действия пароля. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

password aging *days*

no password aging

Параметры:

- *days* – количество дней до принудительного изменения пароля. Задание 0 указывает на неограниченный срок действия пароля. Диапазон: 0 – 365.

Состояние по умолчанию:

180 дней.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Срок действия пароля относится только к пользователям локальной базы с уровнем привилегии 15, а также для пароля `enable`.

Пример:

```
console(config)# passwords aging 90
```

2.18. Команда show password configuration

Команда **show password configuration** служит для отображения информации о текущей конфигурации пароля.

Синтаксис:

show password configuration

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show passwords configuration

Passwords aging is enabled with aging time 90 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 8 characters
```

```
Minimal classes: 0
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled
New password must be different than the manufacturer name: Enabled
```

2.19. Команда `aaa accounting commands`

Команда **`aaa accounting commands`** предназначена для включения регистрации вводимых в ИКС команд на настроенном сервере учета RADIUS или TACACS+. Использование префикса «**no**» выключает регистрацию вводимых в ИКС команд на настроенном сервере учета RADIUS или TACACS+.

Синтаксис:

```
aaa accounting commands priv-level group { radius | tacacs+ }
```

```
no aaa accounting commands priv-level group { radius | tacacs+ }
```

Параметры:

- *priv-level* – указывает уровень привилегий, начиная с которого и ниже, будет производиться регистрация вводимых в ИКС команд.
- **radius** – указывает, что регистрация вводимых в ИКС команд будет производиться на настроенный сервер RADIUS.
- **tacacs+** – указывает, что регистрация вводимых в ИКС команд будет производиться на настроенный сервер TACACS+.

Состояние по умолчанию:

Регистрация вводимых в ИКС команд на сервера RADIUS и TACACS+ выключена

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# aaa accounting commands 15 group tacacs+
```

2.20. Команда `aaa authorization commands`

Команда **`aaa authorization commands`** предназначена для включения проверки вводимых в ИКС команд через настроенный сервер аутентификации и авторизации RADIUS или TACACS+. Использование префикса «**no**» выключает проверку вводимых в ИКС команд через настроенный сервер аутентификации и авторизации RADIUS или TACACS+.

Синтаксис:

```
aaa authorization commands priv-level group { radius | tacacs+ }
```

```
no aaa authorization commands priv-level group { radius | tacacs+ }
```

Параметры:

- *priv-level* – указывает уровень привилегий, начиная с которого и ниже, будет производиться проверка вводимых в ИКС команд.
- **radius** – указывает, что проверка вводимых в ИКС команд будет производиться через настроенный сервер RADIUS.
- **tacacs+** – указывает, что проверка вводимых в ИКС команд будет производиться через настроенный сервер TACACS+.

Состояние по умолчанию:

Проверка вводимых в ИКС команд через сервера RADIUS и TACACS+ выключена

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# aaa authorization commands 15 group tacacs+
```

3. КОМАНДЫ ACL

3.1. Команда ip access-list extended

Команда **ip access-list extended** служит для создания именованного списка доступа IPv4 (ACL) и перехода в режим конфигурирования ACL. После выполнения команды, все последующие команды относятся к данному списку доступа. Правила для этого списка определены в командах **permit** (IP) и **deny** (IP). Команда **service-acl input** используется для назначения созданного списка на интерфейс. Использование префикса «**no**» удаляет созданный список.

Синтаксис:

ip access-list extended *acl-name*

no ip access-list extended *acl-name*

Параметры:

- *acl-name* – имя IPv4 списка доступа. Диапазон: 1 – 32 символа.

Состояние по умолчанию:

IPv4 списки не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Список доступа IPv4 определяется уникальным именем. Списки доступа IPv4, IPv6, MAC или карты политик (**policy maps**) не могут иметь одинаковые имена.

Пример:

```
console(config)# ip access-list extended service
console(config-ip-a1)#
```

3.2. Команда permit (IP)

Команда **permit** (IP) используется для создания разрешающего правила для списка доступа IPv4 (ACL). Правила разрешения также известны как записи контроля доступа (Access Control Entries (ACE)). Использование префикса «**no**» удаляет правило.

Синтаксис:

permit *protocol* { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [**ace-priority** *priority*] [{ **dscp** *number* | **precedence** *number* }] [**time-range** *time-range-name*] [**log-input**]

permit icmp { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [**any** | *icmp-type*] [**any** | *icmp-code*] [**ace-priority** *priority*] [{ **dscp** *number* | **precedence** *number* }] [**time-range** *time-range-name*] [**log-input**]

permit igmp { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [*igmp-type*] [**ace-priority** *priority*] [{ **dscp** *number* | **precedence** *number* }] [**time-range** *time-range-name*] [**log-input**]

permit tcp { **any** | *source source-wildcard* } { **any** | *source-port/port-range* } { **any** | *destination destination-wildcard* } { **any** | *destination-port/port-range* } [**ace-priority** *priority*] [{ **dscp** *number* | **precedence** *number* }] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input**]

permit udp { **any** | *source source-wildcard* } { **any** | *source-port/port-range* } { **any** | *destination destination-wildcard* } { **any** | *destination-port/port-range* } [**ace-priority** *priority*] [{ **dscp** *number* | **precedence** *number* }] [**time-range** *time-range-name*] [**log-input**]

no permit protocol { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [{ **dscp** *number* | **precedence** *number* }] [**time-range** *time-range-name*] [**log-input**]

no permit icmp { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [{ **any** | *icmp-type* }] [{ **any** | *icmp-code* }] [{ **dscp** *number* | **precedence** *number* }] [**time-range** *time-range-name*] [**log-input**]

no permit igmp { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [*igmp-type*] [{ **dscp** *number* | **precedence** *number* }] [**time-range** *time-range-name*] [**log-input**]

no permit tcp { **any** | *source source-wildcard* } { **any** | *source-port/port-range* } { **any** | *destination destination-wildcard* } { **any** | *destination-port/port-range* } [{ **dscp** *number* | **precedence** *number* }] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input**]

no permit udp { **any** | *source source-wildcard* } { **any** | *source-port/port-range* } { **any** | *destination destination-wildcard* } { **any** | *destination-port/port-range* } [{ **dscp** *number* | **precedence** *number* }] [**time-range** *time-range-name*] [**log-input**]

Параметры:

- *protocol* – наименование или номер IP протокола. Доступные наименования: **icmp**, **igmp**, **ip**, **tcp**, **egp**, **igp**, **udp**, **hmp**, **rdp**, **idpr**, **ip6**, **ip6:rout**, **ip6:frag**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **ip6:icmp**, **eigrp**, **ospf**, **ipinip**, **pim**, **l2tp**, **isis**. Для указания любого другого протокола используется его номер. Диапазон: 0 – 255.
- *source* – исходный IP-адрес пакета.
- *source-wildcard* – обратная маска IP-адреса источника.
- *destination* – IP-адрес получателя пакета.
- *destination-wildcard* – обратная маска IP-адреса получателя.
- **ace-priority** *priority* – задает приоритет правила в списке. «1» указывает на наивысший приоритет, а «2147483647» - наименьший. Диапазон: 1 – 2147483647.
- **dscp** *number* – значение значение DSCP.
- **precedence** *number* – задает значение приоритета IP.

- *icmp-type* – задает тип сообщения ICMP для фильтрации пакетов ICMP. Указывается номер типа (диапазон: 0 – 255) или одно из следующих значений: **echo-reply**, **destination-unreachable**, **source-quench**, **redirect**, **alternate-host-address**, **echo-request**, **router-advertisement**, **router-solicitation**, **time-exceeded**, **parameter-problem**, **timestamp**, **timestamp-reply**, **information-request**, **information-reply**, **address-mask-request**, **address-mask-reply**, **traceroute**, **datagram-conversion-error**, **mobile-host-redirect**, **mobile-registration-request**, **mobile-registration-reply**, **domain-name-request**, **domain-name-reply**, **skip**, **photuris**.
- *icmp-code* – задает код сообщения ICMP для фильтрации ICMP пакетов. Диапазон: 0 – 255.
- *igmp-type* – IGMP пакеты могут быть отфильтрованы по типу сообщения IGMP. Используется номер (диапазон: 0 – 255) или одно из следующих значений: **host-query**, **host-report**, **dvmrp**, **pim**, **cisco-trace**, **host-report-v2**, **host-leave-v2**, **host-report-v3**.
- *destination-port* – указывает определенный UDP/TCP порт назначения. Допускается назначение диапазона портов, используя дефис. Например: 20 – 21. Для TCP вводится число или одно из следующих значений: **bgp** (179), **chargen** (19), **daytime** (13), **discard** (9), **domain** (53), **drip** (3949), **echo** (7), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (42), **irc** (194), **klogin** (543), **kshell** (544), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (1110), **syslog** (514), **tacacs-ds** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (117), **whois** (43), **www** (80). Для UDP вводится число или одно из следующих значений: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dnsix** (90), **domain** (53), **echo** (7), **mobile-ip** (434), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **on500-isakmp** (4500), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (49), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177). Диапазон: 0 – 65535.
- *source-port* – указывает определенный UDP/TCP порт источника. Предопределенные имена портов указаны в параметре *destination-port*. Диапазон: 0 – 65535.
- *match-all list-of-flags* – список флагов TCP которые могут быть получены. Если флаг должен быть установлен, он имеет префикс «+», если отменен – префикс «-». Доступны следующие флаги: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** и **-fin**. Флаги могут быть объединены в одну строку. Например: **+fin-ack**.
- *time-range-name* – имя списка временного диапазона применяемого к данному правилу. Диапазон: 1 – 32 символа.
- **log-input** – задает отправку информационного сообщения в SYSLOG о пакете, который соответствует записи. Так как пересылка/отбрасывание пакетов осуществляется на аппаратном уровне, а регистрация сообщений выполняется программным обеспечением, при большом количестве пакетов соответствующих правилу, содержащему данный параметр не все сообщения могут быть записаны в журнал.

Состояние по умолчанию:

IPv4 списки доступа не заданы.

Режим ИКС:

Режим конфигурации списка доступа IP

Примечания:

1. Количество диапазонов TCP / UDP, которые могут быть определены в списках ACL, ограничено.
2. Если диапазон портов для порта источника задан в одном правиле и также используется в другом правиле, то повторно он не учитывается. Если диапазон портов для порта назначения задан в одном правиле и используется в другом, то он также повторно не учитывается.
3. Если диапазон портов используется для порта источника и также используется для порта назначения, то он учитывается повторно.
4. Если для правила ace-priority не указан, то система устанавливает приоритет для него приоритет ACE с самым высоким приоритетом + 20. Приоритет для правила должен быть уникальным в текущем списке доступа. Если указанный приоритет уже существует, то команда отвергается.

Пример:

```
console(config)# ip access-list extended service
console(config-ip-al)# permit ip 172.16.20.124 0.0.255.255 any
```

3.3. Команда deny (IP)

Команда **deny** используется для создания запрещающего правила для списка доступа IPv4 (ACL). Правила разрешения также известны как записи контроля доступа (Access Control Entries (ACE)). Использование префикса «**no**» удаляет правило.

Синтаксис:

deny protocol { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [**ace-priority priority**] [{ **dscp number** | **precedence number** }] [**time-range time-range-name**] [**log-input**]

deny icmp { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [**any** | *icmp-type*] [**any** | *icmp-code*] [**ace-priority priority**] [{ **dscp number** | **precedence number** }] [**time-range time-range-name**] [**log-input**]

deny igmp { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [*igmp-type*] [**ace-priority priority**] [{ **dscp number** | **precedence number** }] [**time-range time-range-name**] [**log-input**]

deny tcp { **any** | *source source-wildcard* } { **any** | *source-port/port-range* } { **any** | *destination destination-wildcard* } { **any** | *destination-port/port-range* } [**ace-priority priority**] [{ **dscp number** | **precedence number** }] [**match-all list-of-flags**] [**time-range time-range-name**] [**log-input**]

deny udp { **any** | *source source-wildcard* } { **any** | *source-port/port-range* } { **any** | *destination destination-wildcard* } { **any** | *destination-port/port-range* } [**ace-priority priority**] [{ **dscp number** | **precedence number** }] [**time-range time-range-name**] [**log-input**]

no deny protocol { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [{ **dscp number** | **precedence number** }] [**time-range** *time-range-name*] [**log-input**]

no deny icmp { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [{ **any** | *icmp-type* }] [{ **any** | *icmp-code* }] [{ **dscp number** | **precedence number** }] [**time-range** *time-range-name*] [**log-input**]

no deny igmp { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [*igmp-type*] [{ **dscp number** | **precedence number** }] [**time-range** *time-range-name*] [**log-input**]

no deny tcp { **any** | *source source-wildcard* } { **any** | *source-port/port-range* } { **any** | *destination destination-wildcard* } { **any** | *destination-port/port-range* } [{ **dscp number** | **precedence number** }] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input**]

no deny udp { **any** | *source source-wildcard* } { **any** | *source-port/port-range* } { **any** | *destination destination-wildcard* } { **any** | *destination-port/port-range* } [{ **dscp number** | **precedence number** }] [**time-range** *time-range-name*] [**log-input**]

Параметры:

- *protocol* – наименование или номер IP протокола. Доступные наименования: **icmp**, **igmp**, **ip**, **tcp**, **egp**, **igr**, **udp**, **hmp**, **rdp**, **idpr**, **ipv6**, **ipv6:rout**, **ipv6:frag**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **ipv6:icmp**, **eigrp**, **ospf**, **ipinip**, **pim**, **l2tp**, **isis**. Для указания любого другого протокола используется его номер. Диапазон: 0 – 255.
- *source* – исходный IP-адрес пакета.
- *source-wildcard* – обратная маска IP-адреса источника.
- *destination* – IP-адрес получателя пакета.
- *destination-wildcard* – обратная маска IP-адреса получателя.
- **ace-priority** *priority* – задает приоритет правила в списке. «1» указывает на наивысший приоритет, а «2147483647» - наименьший. Диапазон: 1 – 2147483647.
- **dscp number** – значение значение DSCP.
- **precedence number** – задает значение приоритета IP.
- *icmp-type* – задает тип сообщения ICMP для фильтрации пакетов ICMP. Указывается номер типа (диапазон: 0 – 255) или одно из следующих значений: **echo-reply**, **destination-unreachable**, **source-quench**, **redirect**, **alternate-host-address**, **echo-request**, **router-advertisement**, **router-solicitation**, **time-exceeded**, **parameter-problem**, **timestamp**, **timestamp-reply**, **information-request**, **information-reply**, **address-mask-request**, **address-mask-reply**, **traceroute**, **datagram-conversion-error**, **mobile-host-redirect**, **mobile-registration-request**, **mobile-registration-reply**, **domain-name-request**, **domain-name-reply**, **skip**, **photuris**.
- *icmp-code* – задает код сообщения ICMP для фильтрации ICMP пакетов. Диапазон: 0 – 255.
- *igmp-type* – IGMP пакеты могут быть отфильтрованы по типу сообщения IGMP. Используется номер (диапазон: 0 – 255) или одно из следующих значений: **host-query**, **host-report**, **dvmrp**, **pim**, **cisco-trace**, **host-report-v2**, **host-leave-v2**, **host-report-v3**.

- *destination-port* – указывает определенный UDP/TCP порт назначения. Допускается назначение диапазона портов, используя дефис. Например: 20 – 21. Для TCP вводится число или одно из следующих значений: **bgp** (179), **chargen** (19), **daytime** (13), **discard** (9), **domain** (53), **drip** (3949), **echo** (7), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (42), **irc** (194), **klogin** (543), **kshell** (544), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (1110), **syslog** (514), **tacacs-ds** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (117), **whois** (43), **www** (80). Для UDP вводится число или одно из следующих значений: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dnsix** (90), **domain** (53), **echo** (7), **mobile-ip** (434), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **on500-isakmp** (4500), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (49), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177). Диапазон: 0 – 65535.
- *source-port* – указывает определенный UDP/TCP порт источника. Предопределенные имена портов указаны в параметре *destination-port*. Диапазон: 0 – 65535.
- **match-all** *list-of-flags* – список флагов TCP которые могут быть получены. Если флаг должен быть установлен, он имеет префикс «+», если отменен – префикс «-». Доступны следующие флаги: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** и **-fin**. Флаги могут быть объединены в одну строку. Например: **+fin-ack**.
- *time-range-name* – имя списка временного диапазона применяемого к данному правилу. Диапазон: 1 – 32 символа.
- **log-input** – задает отправку информационного сообщения в SYSLOG о пакете, который соответствует записи. Так как пересылка/отбрасывание пакетов осуществляется на аппаратном уровне, а регистрация сообщений выполняется программным обеспечением, при большом количестве пакетов соответствующих правилу, содержащему данный параметр не все сообщения могут быть записаны в журнал.

Состояние по умолчанию:

IPv4 списки доступа не заданы.

Режим ИКС:

Режим конфигурации списка доступа IP

Примечания:

1. Количество диапазонов TCP / UDP, которые могут быть определены в списках ACL, ограничено.
2. Если диапазон портов для порта источника задан в одном правиле и также используется в другом правиле, то повторно он не учитывается. Если диапазон портов для порта назначения задан в одном правиле и используется в другом, то он также повторно не учитывается.
3. Если диапазон портов используется для порта источника и также используется для порта назначения, то он учитывается повторно.
4. Если для правила **ace-priority** не указан, то система устанавливает приоритет для него приоритет ACE на 20 больше, чем текущее максимальное значение. Приоритет для правила должен быть уникальным в текущем списке доступа. Если указанный приоритет уже существует, то команда отвергается.

Пример:

```
console(config)# ip access-list extended service
console(config-ip-al)# deny ip 172.16.20.124 0.0.255.255 any
```

3.4. Команда mac access-list

Команда **mac access-list** предназначена для создания списков доступа (ACL) 2 уровня (Layer 2), основанных на MAC-адресах и перехода в режим конфигурирования этого списка. Правила для этого списка задаются командами **permit** (MAC) и **deny** (MAC). Командой **service-acl input** созданный список назначается на интерфейс. Использование префикса «**no**» удаляет созданный список.

Синтаксис:

mac access-list extended *acl-name*

no mac access-list extended *acl-name*

Параметры:

- *acl-name* – имя списка доступа на основе MAC-адресов. Длина: 1 – 32 символа.

Состояние по умолчанию:

Списки доступа не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Список доступа MAC определяется уникальным именем. Списки доступа IPv4, IPv6, MAC или карты политик (**policy maps**) не могут иметь одинаковые имена.

Пример:

```
console(config)# mac access-list extended farm
console(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff
any
```

3.5. Команда permit (MAC)

Команда **permit** (MAC) применяется для создания разрешающих правил списка доступа MAC. Использование префикса «**no**» удаляет правило.

Синтаксис:

permit { **any** | *source source-wildcard* } { **any** | *destination destination-wildcard* } [**ace-priority priority**] [{ **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** }] [**vlan vlan-id**] [**cos cos cos-wildcard**] [**time-range time-range-name**] [**log-input**]

no permit { any | source source-wildcard } { any | destination destination-wildcard } [ace-priority priority] [{ aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 }] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [log-input]

Параметры:

- *source* – MAC-адрес источника пакетов
- *source-wildcard* – обратная маска MAC-адреса источника
- *destination* – MAC-адрес назначения пакета
- *destination-wildcard* – обратная маска MAC-адреса назначения
- **ace-priority priority** – задает приоритет правила в списке. «1» указывает на наивысший приоритет, а «2147483647» - наименьший. Диапазон: 1 – 2147483647
- **aarp** - EtherType: AppleTalk ARP
- **amber** - EtherType: DEC-Amber
- **dec-spanning** - EtherType: DEC-Spanning-Tree
- **diagnostic** - EtherType: DEC-Diagnostic
- **decnet-iv** - EtherType: DECnet Phase IV
- **dsm** - EtherType: DEC-DSM
- **etype-6000** - EtherType: 0x6000
- *vlan-id* – тэг VLAN пакета. Диапазон: 1 – 4094
- *cos* – класс обслуживания пакета (CoS). Диапазон: 0 – 7
- *cos-wildcard* – обратная маска применяемая к пакету CoS
- *time-range-name* - имя списка временного диапазона применяемого к данному правилу. Длина: 1 – 32 символа.
- **log-input** – задает отправку информационного сообщения в SYSLOG о пакете, который соответствует записи. Так как пересылка/отбрасывание пакетов осуществляется на аппаратном уровне, а регистрация сообщений выполняется программным обеспечением, при большом количестве пакетов соответствующих правилу, содержащему данный параметр не все сообщения могут быть записаны в журнал

Состояние по умолчанию:

Списки доступа не заданы.

Режим ИКС:

Режим конфигурации списка доступа MAC

Примечания:

1. Список доступа MAC определяется уникальным именем. Списки доступа IPv4, IPv6, MAC или карты политик (**policy maps**) не могут иметь одинаковые имена.
2. Если для правила **ace-priority** не указан, то система устанавливает приоритет для него приоритет ACE на 20 больше, чем текущее максимальное значение. Приоритет для правила должен быть уникальным в текущем списке доступа. Если указанный приоритет уже существует, то команда отвергается.

Пример:

```
console(config)# mac access-list extended farm
```

```
console(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff  
any
```

3.6. Команда deny (MAC)

Команда **deny** (MAC) предназначена для создания запрещающих правил списка доступа MAC. Использование префикса «**no**» удаляет правило.

Синтаксис:

```
deny { any | source source-wildcard } { any | destination destination-wildcard } [ ace-priority  
priority ] [ { aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 } ] [ vlan  
vlan-id ] [ cos cos cos-wildcard ] [ time-range time-range-name ] [ log-input ]
```

```
no deny { any | source source-wildcard } { any | destination destination-wildcard } [ ace-  
priority priority ] [ { aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 } ]  
[ vlan vlan-id ] [ cos cos cos-wildcard ] [ time-range time-range-name ] [ log-input ]
```

Параметры:

- *source* – MAC-адрес источника пакетов
- *source-wildcard* – обратная маска MAC-адреса источника
- *destination* – MAC-адрес назначения пакета
- *destination-wildcard* – обратная маска MAC-адреса назначения
- **ace-priority** *priority* – задает приоритет правила в списке. «1» указывает на наивысший приоритет, а «2147483647» - наименьший. Диапазон: 1 – 2147483647
- **aarp** - EtherType: AppleTalk ARP
- **amber** - EtherType: DEC-Amber
- **dec-spanning** - EtherType: DEC-Spanning-Tree
- **diagnostic** - EtherType: DEC-Diagnostic
- **decnet-iv** - EtherType: DECnet Phase IV
- **dsm** - EtherType: DEC-DSM
- **etype-6000** - EtherType: 0x6000
- *vlan-id* – тэг VLAN пакета. Диапазон: 1 – 4094
- *cos* – класс обслуживания пакета (CoS). Диапазон: 0 – 7
- *cos-wildcard* – обратная маска применяемая к пакету CoS
- *time-range-name* - имя списка временного диапазона применяемого к данному правилу. Длина: 1 – 32 символа.
- **log-input** – задает отправку информационного сообщения в SYSLOG о пакете, который соответствует записи. Так как пересылка/отбрасывание пакетов осуществляется на аппаратном уровне, а регистрация сообщений выполняется программным обеспечением, при большом количестве пакетов соответствующих правилу, содержащему данный параметр не все сообщения могут быть записаны в журнал

Состояние по умолчанию:

Списки доступа не определены.

Режим ИКС:

Режим конфигурации списка доступа MAC

Примечания:

1. Список доступа MAC определяется уникальным именем. Списки доступа IPv4, IPv6, MAC или карты политик (**policy maps**) не могут иметь одинаковые имена.
2. Если для правила **ace-priority** не указан, то система устанавливает приоритет для него приоритет ACE на 20 больше, чем текущее максимальное значение. Приоритет для правила должен быть уникальным в текущем списке доступа. Если указанный приоритет уже существует, то команда отвергается.

Пример:

```
console(config)# mac access-list extended farm
console(config-mac-al)# deny 00:00:00:00:00:01 00:00:00:00:00:ff
any
```

3.7. Команда service-acl input

Команда **service-acl input** предназначена для привязки списка доступа к интерфейсу. Использование префикса «**no**» удаляет привязку к интерфейсу.

Синтаксис:

service-acl input *acl-name* [**default-action** { **deny-any** | **permit-any** }]

no service-acl input

Параметры:

- *acl-name* – имя списка доступа, применяемого к интерфейсу. См. пояснения. Длина: 1 – 32 символа.
- **deny-any** – отбрасывает все пакеты не соответствующие правилам данного списка.
- **permit-any** – пропускает все пакеты не соответствующие правилам данного списка.

Состояние по умолчанию:

Списки доступа не назначены.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port-Channel, VLAN)

Примечание:

- Нижеперечисленные правила определяют порядок назначения списков доступа на интерфейс:
- MAC список не может использоваться на интерфейсе, которому уже назначен IPv4 список;
- список доступа не может быть привязан к порту, которому уже назначен другой список, без предварительного удаления текущего списка.
- MAC списки, которые включают в себя параметры VLAN не могут быть привязаны к интерфейсам VLAN;

- списки имеющие в своем составе правила основанные на временном диапазоне не могут быть привязаны к интерфейсу VLAN;
- списки имеющие правила с отключением интерфейса не могут быть привязаны к интерфейсу VLAN;
- для обработки правил списка используются ресурсы TCAM. Для MAC или IP правила - одна запись TCAM. Выделение ресурсов TCAM всегда равно четному числу, поэтому в случае нечетного количества правил ресурсы будут увеличены на 1;
- список привязанный к входящему трафику не может быть применен к исходящему трафику.

Пример:

```
console(config)# mac access-list extended srv-acl-mac
console(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff
any
console(config-mac-al)# exit
console(config)# interface GigabitEthernet 1/0/15
console(config-if)# service-acl input srv-acl-mac default-action
deny-any
```

3.8. Команда service-acl output

Команда **service-acl output** применяется для привязки списка доступа к интерфейсу, для контроля исходящего трафика через порт. Использование префикса «**no**» удаляет привязку.

Синтаксис:

service-acl output *acl-name*

no service-acl output

Параметры:

- *acl-name* – имя списка доступа применяемого к интерфейсу. См. примечания. Длина: 1 – 32 символа.

Состояние по умолчанию:

Списки доступа не назначены.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port-Channel)

Примечания:

- Параметр **log-input** не поддерживается. Попытка его использовать приведет к ошибке.
- Параметр **disable-port** в запрещающем правиле не поддерживается. Попытка его использования приведет к ошибке.
- Список MAC не может использоваться одновременно со списками IPv4.

- Список доступа не может быть привязан к порту, которому уже назначен другой список, без предварительного удаления текущего списка.
- Список не может быть использован как исходящий, если уже применен как входящий.

Пример:

```
console(config)# mac access-list extended srv-acl-mac
console(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff
any
console(config-mac-al)# exit
console(config)# interface GigabitEthernet 1/0/15
console(config-if)# service-acl output srv-acl-mac
```

3.9. Команда `time-range`

Команда **time-range** предназначена для создания временного диапазона для различных функций. Кроме этого служит для входа в режим конфигурации временного диапазона. Все вводимые команды в этом режиме относятся к созданному временному диапазону.

Данная команда также задает имя диапазона.

Команды **absolute** и **periodic** используются для конфигурирования диапазона.

Использование префикса **no** удаляет созданный диапазон с устройства.

Синтаксис:

time-range *time-range-name*

no time-range *time-range-name*

Параметры:

- *time-range-name* – имя временного диапазона. Длина: 1 – 32 символа.

Состояние по умолчанию:

Временные диапазоны не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. После задания имени диапазона и перехода в режим его конфигурации, команды **absolute** и **periodic** используются для фактической его настройки. Допускается множественное использование команды **periodic** и только одно использование команды **absolute**.
2. Если в диапазоне используются как абсолютные, так и периодические значения, то периодические элементы оцениваются только после достижения абсолютного начала времени и не оцениваются снова после достижения абсолютного конца времени.
3. Все заданные значения времени интерпретируются как местное время.

4. Чтобы гарантировать правильное выполнение диапазона (в требуемые значения времени), часы на устройстве должны быть предварительно настроены администратором или с помощью протокола SNTP. Если часы предварительно не установлены, правила диапазона не активируются.
5. Диапазон не может быть удален, пока связан с какой-либо используемой функцией.
6. Созданный временной диапазон можно использовать в следующих командах:
 - **dot1x port-control**
 - **operation time**
 - **permit (IP)**
 - **deny (IP)**
 - **permit (MAC)**
 - **deny (MAC)**

Пример:

```
console(config)# time-range http-allowed
console(config-time-range)# periodic mon 12:00 to wed 17:00
```

3.10. Команда absolute

Команда **absolute** используется для указания абсолютного времени действия временного диапазона. Использование префикса «**no**» снимает ограничение по времени.

Синтаксис:

absolute start *hh:mm day month year*

no absolute start

absolute end *hh:mm day month year*

no absolute end

Параметры:

- **start** – установить время и дату начала действия (разрешения или запрета) связанной функции. Если время начала действия не указано – функция начинает действовать немедленно;
- **end** – установить время и дату окончания действия (разрешения или запрета) связанной функции. Если время окончания действия не указано – функция действует бесконечно;
- *hh:mm* – часы и минуты (24-х часовой формат). Диапазон: часы: 0 – 23, минуты: 0 – 59;
- *day* – день месяца, диапазон: 1 – 31;
- *month* – месяц (три первые буквы названия (англ.)). Возможные значения: **Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec**;
- *year* – год, диапазон: 2000-2097.

Состояние по умолчанию:

При создании временного интервала, правило для абсолютного времени не определено.

Режим ИКС:

Режим конфигурации временного диааназона

Пример:

```
console(config)# time-range http-allowed
console(config-time-range)# absolute start 12:59 1 mar 2018
console(config-time-range)# absolute end 13:00 10 mar 2018
```

3.11. Команда periodic

Команда **periodic** предназначена для указания повторяющегося (недельного) диапазона в создаваемом временном диапазоне. Использование префикса «**no**» удаляет ограничение по времени.

Синтаксис:

periodic *day-of-the-week hh:mm to day-of-the-week hh:mm*

no periodic *day-of-the-week hh:mm to day-of-the-week hh:mm*

periodic list *hh:mm to hh:mm day-of-the-week1 [day-of-the-week2... day-of-the-week7]*

no periodic list *hh:mm to hh:mm day-of-the-week1 [day-of-the-week2... day-of-the-week7]*

periodic list *hh:mm to hh:mm all*

no periodic list *hh:mm to hh:mm all*

Параметры:

- *day-of-the-week* – день недели начала действия диапазона. Второе вхождение – день окончания действия. День окончания может быть на следующей неделе (см. Пояснения). Возможные значения: **mon, tue, wed, thu, fri, sat** и **sun**.
- *hh:mm* – часы и минуты начала действия. Второе вхождение – время окончания. Второе вхождение может быть на следующий день
- **list** *day-of-the-week* - список дней, в течение которых действует временной диапазон.
- Ключ **all** в конце команды означает все дни недели.

Состояние по умолчанию:

В созданном временном диапазоне повторяющиеся правила отсутствуют.

Режим ИКС:

Режим конфигурации временного диааназона

Примечания:

1. Второе вхождение дня недели может приходиться на следующую неделю. Например может быть создан диапазон, которые действует с четверга до понедельника (четверг, пятница, суб-бота, воскресенье и понедельник).
2. Второе вхождение времени может приходиться на следующие сутки. Например диапазон с «22:00 – 2:00».

Пример:

```
console(config)# time-range http-allowed  
console(config-time-range)# periodic mon 12:00 to wed 12:00
```

3.12. Команда show time-range

Команда **show time-range** отображает на экране информацию о созданных временных диапазонах.

Синтаксис:

show time-range *time-range-name*

Параметры:

- *time-range-name* – имя временного диапазона

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show time-range  
time-range http-allowed  
absolute start 12:59 1 Mar 2018 end 13:00 10 Mar 2018  
periodic Monday 12:00 to Wednesday 17:00
```

3.13. Команда show access-list

Команда **show access-list** служит для отображения на экране информации о созданных списках доступа.

Синтаксис:

show access-list [*name*]

show access-list time-range-active [*name*]

Параметры:

- *name* – имя списка доступа, длина: 1 – 32.
- **time-range-active** – отображает только те правила из списка, чей временной диапазон активен (включая те, которые не привязаны к созданным диапазонам созданным командой **time-range**)

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1

```
console#show access-lists
```



```
Extended MAC access list farm
  permit 00:00:00:00:00:01 00:00:00:00:00:ff any ace-priority 20
Extended MAC access list srv-acl-mac
  permit 00:00:00:00:00:01 00:00:00:00:00:ff any ace-priority 20
```

Пример 2

```
console#show access-lists time-range-active
Extended MAC access list farm
  permit 00:00:00:00:00:01 00:00:00:00:00:ff any ace-priority 20
Extended MAC access list srv-acl-mac
  permit 00:00:00:00:00:01 00:00:00:00:00:ff any ace-priority 20
```

3.14. Команда show interfaces access-lists

Команда **show interfaces access-lists** отображает на экране списки доступа привязанные к интерфейсам.

Синтаксис:

show interfaces access-lists [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Доступны следующие типы: **Ethernet**, **Port-Channel**, **VLAN**.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show interfaces access-lists
Interface                               ACLs
-----
gil/0/15                                Ingress: srv-acl-mac
```

3.15. Команда show interfaces access-lists trapped packets

Команда **show interfaces access-lists trapped packets** отображает на экране информацию по всем захваченным пакетам всех существующих списков доступа.

Синтаксис:

show interfaces access-lists trapped packets [{ *interface-id* | *port-channel-number* | *VLAN* }]

Параметры:

- *interface-id* – идентификатор интерфейса Ethernet;
- *port-channel* – номер агрегированного канала;
- *VLAN* – номер VLAN.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Команда показывает количество пакетов, захваченных в случае соответствия условиям записей АСЕ и если включена запись в журнал.

Пример:

```
console# show interfaces access-lists trapped packets
Ports/LAGs: tel/0/1-tel/0/3, ch1-ch3, ch4
VLANs: VLAN1, VLAN12-VLAN15
Packets were trapped globally due to lack of resources
```

3.16. Команда clear access-lists counters

Команда **clear access-lists counters** применяется для очистки значений счетчиков список доступа.

Синтаксис:

clear access-lists counters [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса (Ethernet или Port-channel).

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear access-lists counters GigabitEthernet 1/0/15
```

3.17. Команда ip access-list (IP standard)

Команда **ip access-list** (IP standard) предназначена для создания стандартного IP списка доступа. Использование префикса «**no**» удаляет список.

Синтаксис:

ip access-list *access-list-name* { **deny** | **permit** } { *src-addr*[/*src-len*] | **any** }

no ip access-list *access-list-name*

Параметры:

- *access-list-name* – имя стандартного IP списка доступа. Максимальная длина: 32 символа.
- **deny** | **permit** – запрет/разрешение доступа при совпадении условий.
- { *src-addr*[/*src-len*] | **any** } – IP-адрес источника, с не обязательным указанием маски подсети. Либо в качестве источника принимается любой адрес/сеть (**any**).

Состояние по умолчанию:

Списки доступа не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

- Стандартный список доступа предназначен только для фильтрации по IP-адресам.
- Проверка входящего пакета осуществляется с первого правила списка и продолжается до тех пор, пока не будет найдено совпадений. Если совпадение найдено, то дальнейшая проверка списка прекращается. Если входящий пакет не соответствует ни одному правилу, то его прохождение запрещается.
- В дополнении к фильтрации IP-трафика по портам, стандартный список доступа может использоваться для фильтрации обновлений маршрутов в протоколе RIP (Routing Information Protocol).

Пример:

```
console(config)# ip access-list 1 permit 10.0.0.13/24  
console(config)# ip access-list 1 deny 10.0.0.35/24
```

4. КОМАНДЫ АДРЕСНЫХ ТАБЛИЦ

4.1. Команда bridge multicast filtering

Команда **bridge multicast filtering** применяется для включения фильтрации адресов многоадресной рассылки. Использование префикса «**no**» выключает фильтрацию.

Синтаксис:

bridge multicast filtering

no bridge multicast filtering

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Фильтрация отключена. Все адреса многоадресной рассылки отправляются на все порты.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Когда фильтрация включена, незарегистрированный многоадресный трафик будет отброшен.
2. Все зарегистрированные мультикастовые адреса будут перенаправленный в группы многоадресной рассылки. Существует два способа управления многоадресными группами, одна из которых функция IGMP Snooping, а вторая: команда **bridge multicast forward-all**.

Пример:

```
console(config)# bridge multicast filtering
```

4.2. Команда bridge multicast mode

Команда **bridge multicast mode** предназначена для настройки режима моста многоадресной рассылки. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

bridge multicast mode { mac-group | ipv4-group | ipv4-src-group }

no bridge multicast mode

Параметры:

- **mac-group** – указывает, что многоадресная пересылка основана на VLAN и MAC-адресе пакета.

- **ipv4-group** – указывает, что многоадресная пересылка основана на VLAN и MAC-адресе пакета для пакетов отличных от IPv4, а также на VLAN и IPv4 адресе назначения, для пакетов IPv4.
- **ipv4-src-group** – указывает, что многоадресная пересылка основана на VLAN и MAC-адресе пакета для пакетов отличных от IPv4, и для пакетов IPv4 основана на VLAN, IPv4 адресе источника и IPv4 адресе назначения.

Состояние по умолчанию:

По умолчанию применяется режим **bridge multicast mode mac-group**.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Примечания:

1. Режим mac-group применяется при использовании системы сетевого управления, которая использует MIB на основе MAC-адреса многоадресной передачи. В противном случае рекомендуется использовать режим IPv4, поскольку в этих режимах нет перекрытия адресов много-адресной передачи IPv4.
2. Для каждого режима FDB (Forwarding Data Base) используются разные команды для настройки статических записей FDB, как указано в таблице ниже.

Команды для настройки статических записей FDB:

Режим FDB	Команды ИКС	
mac-group	bridge multicast address	bridge multicast forbidden address
ipv4-group	bridge multicast ip-address	bridge multicast forbidden ip-address
ipv4-src-group	bridge multicast source group	bridge multicast forbidden source group

3. В таблице ниже описаны фактические данные, которые записываются в FDB, согласно версии IGMP, используемой в сети:

Данные, которые записываются в FDB:

FDB mode	IGMP version 2	IGMP version 3
mac-group	MAC group address	MAC group address
ipv4-group	IP group address	IP group address
ipv4-src-group	(*)	IP source and group addresses

(*) Маршрут типа (*, G) нельзя записать в FDB, если выбран режим **ipv4-src-group**. В этом случае новая запись в FDB не создается, но порт добавляется в записи (S, G) (если они существуют), принадлежащие запрашиваемой группе. Для IGMP версии 2 рекомендуется использовать режимы **ipv4-group** или **mac-group**.

Если приложение на устройстве запрашивает (*, G), то рабочий режим FDB изменяется на **ipv4-group**.

Пример:

```
console(config)# interface vlan 2  
console(config-if)# bridge multicast mode mac-group
```

4.3. Команда bridge multicast address

Команда **bridge multicast address** предназначена для регистрации MAC-адреса многоадресной рассылки в таблице моста, а также для добавления портов в группу и удаления из нее. Использование префикса «**no**» удаляет адрес из таблицы.

Синтаксис:

```
bridge multicast address { mac-multicast-address | ipv4-multicast-address } [ [ { add | remove } ] { ethernet interface-list | port-channel port-channel-list } ]
```

```
no bridge multicast address mac-multicast-address
```

Параметры:

- *mac-multicast-address* | *ipv4-multicast-address* – адрес группы многоадресной рассылки;
- **add** – добавляет порт в группу;
- **remove** – удаляет порт из группы;
- **ethernet** *interface-list* – список портов Ethernet. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис;
- **port-channel** *port-channel-list* – список портов Port-channel. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис.

Состояние по умолчанию:

Адреса многоадресной рассылки не определены.

Если в команде указаны интерфейсы Ethernet или Port-channel без указания опций, то по умолчанию используется опция **add**.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Примечания:

1. Для регистрации группы в базе данных моста без добавления или удаления портов, указывается только параметр **mac-multicast-address**.
2. Статические адреса многоадресной рассылки могут быть определены только в статических VLAN.
3. Команда может быть выполнена перед созданием VLAN.

Примеры:

Пример 1: В этом примере регистрируется MAC-адрес без указания портов.

```
console(config)# interface vlan 19
```

```
console(config-if)# bridge multicast address 01:00:5e:02:02:03
```

Пример 2: В этом примере регистрируется MAC-адрес и добавляется порт в группу.

```
console(config)# interface vlan 19  
console(config-if)# bridge multicast address 01:00:5e:02:02:03 add  
gi1/0/10
```

4.4. Команда bridge multicast forbidden address

Команда **bridge multicast forbidden address** предназначена для ручного добавления или удаления адреса многоадресной рассылки, для его блокирования на определенных портах. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

```
bridge multicast forbidden address { mac-multicast-address | ipv4-multicast-address } { add | remove } { ethernet interface-list | port-channel port-channel-list }
```

```
no bridge multicast forbidden address mac-multicast-address
```

Параметры:

- { *mac-multicast-address* | *ipv4-multicast-address* } – адрес группы многоадресной рассылки;
- **add** – добавляет порт в группу;
- **remove** – удаляет порт из группы;
- **ethernet** *interface-list* – список портов Ethernet. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис;
- **port-channel** *port-channel-list* – список портов Port-channel. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис.

Состояние по умолчанию:

Запрещенные адреса не определены.

Опция по умолчанию: **add**.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Примечания:

1. Перед использованием данной команды, группа многоадресной рассылки должна быть зарегистрирована с помощью команды **bridge multicast address**.
2. Команда может быть выполнена перед созданием VLAN.

Пример:

```
console(config)# interface vlan 19  
console(config-if)# bridge multicast address 01:00:5e:02:02:03  
console(config-if)# bridge multicast forbidden address  
01:00:5e:02:02:03 add gi1/0/13
```

4.5. Команда `bridge multicast ip-address`

Команда **bridge multicast ip-address** предназначена для регистрации IP-адреса многоадресной рассылки в таблице моста, а также добавления или удаления портов в/из группы многоадресной рассылки. Использование префикса «**no**» удаляет IP адрес.

Синтаксис:

bridge multicast ip-address *ip-multicast-address* [[**add** | **remove**] { *interface-list* | **port-channel** *port-channel-list* }]

no bridge multicast ip-address *ip-multicast-address*

Параметры:

- *ip-multicast-address* – IP-адрес группы многоадресной рассылки;
- **add** – добавляет порт в группу;
- **remove** – удаляет порт из группы;
- **ethernet** *interface-list* – список портов Ethernet. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис;
- **port-channel** *port-channel-list* – список портов Port-channel. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис.

Состояние по умолчанию:

Адрес многоадресной рассылки не задан.

Опция по умолчанию: **add**.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Примечания:

1. Чтобы зарегистрировать группу без добавления или удаления портов, используется только параметр **ip-multicast-address**.
2. Статические адреса многоадресной рассылки могут быть определены только в статических VLAN.
3. Команда может быть выполнена перед созданием VLAN.

Примеры:

Пример 1

```
console(config)# interface vlan 19
console(config-if)# bridge multicast ip
console(config-if)# bridge multicast ip-address 239.2.2.2
```

Пример 2

```
console(config)# interface vlan 19
console(config-if)# bridge multicast ip
console(config-if)# bridge multicast ip-address 239.2.2.2 add
gi1/0/20
```


4.6. Команда `bridge multicast forbidden ip-address`

Команда **bridge multicast forbidden ip-address** предназначена для ручного добавления или удаления IP-адреса многоадресной рассылки, для его блокирования на определенных портах. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

```
bridge multicast forbidden ip-address ip-multicast-address { add | remove } { ethernet  
interface-list | port-channel port-channel-list }
```

```
no bridge multicast forbidden ip-address ip-multicast-address
```

Параметры:

- *ip-multicast-address* – IP-адрес группы многоадресной рассылки;
- **add** – добавляет порт в группу;
- **remove** – удаляет порт из группы;
- **ethernet** *interface-list* – список портов Ethernet. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис;
- **port-channel** *port-channel-list* – список портов Port-channel. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис.

Состояние по умолчанию:

Блокированные адреса не определены.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Примечания:

Перед блокированием портов группа многоадресной рассылки должна быть предварительно зарегистрирована.

Выполнение команды допускается до создания VLAN.

Пример:

```
console(config)# interface vlan 12  
console(config-if)# bridge multicast ip-address 239.2.2.2  
console(config-if)# bridge multicast forbidden ip-address 239.2.2.2  
add gil/0/21
```

4.7. Команда `bridge multicast source group`

Команда **bridge multicast source group** предназначена для регистрации пары IP адрес – IP адрес мультикаст в таблице моста и добавлению или удалению портов в группу-источник. Использование префикса «**no**» удаляет пару.

Синтаксис:

bridge multicast source *ip-address* **group** *ip-multicast-address* [[{ **add** | **remove** }] { **ethernet** *interface-list* | **port-channel** *port-channel-list* }]

no bridge multicast source *ip-address* **group** *ip-multicast-address*

Параметры:

- *ip-address* – IP-адрес источника;
- *ip-multicast-address* – IP-адрес группы многоадресной рассылки;
- **add** – добавляет порт в группу;
- **remove** – удаляет порт из группы;
- **ethernet** *interface-list* – список портов Ethernet. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис;
- **port-channel** *port-channel-list* – список портов Port-channel. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис.

Состояние по умолчанию:

Адреса не определены

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Примечание:

Выполнение команды допускается до создания VLAN.

Пример:

```
console(config)# interface vlan 21
console(config-if)# bridge multicast source 172.12.1.13 group
239.2.2.2
```

4.8. Команда **bridge multicast forbidden source group**

Команда **bridge multicast forbidden source group** предназначена для ручного добавления/удаления пары IP-адрес – IP-адрес мультикаст, для ее блокирования на определенных списках портов. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

bridge multicast forbidden source *ip-address* **group** *ip-multicast-address* { **add** | **remove** } { **ethernet** *interface-list* | **port-channel** *port-channel-list* }

no bridge multicast forbidden source *ip-address* **group** *ip-multicast-address*

Параметры:

- *ip-address* – IP-адрес источника;
- *ip-multicast-address* – IP-адрес группы многоадресной рассылки;
- **add** – добавляет порт в группу;

- **remove** – удаляет порт из группы;
- **ethernet interface-list** – список портов Ethernet. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис;
- **port-channel port-channel-list** – список портов Port-channel. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис.

Состояние по умолчанию:

Блокированные адреса не определены.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Примечания:

1. Перед блокированием портов группа многоадресной рассылки должна быть предварительно зарегистрирована.
2. Выполнение команды допускается до создания VLAN.

Пример:

```
console(config)# interface vlan 21
console(config-if)# bridge multicast source 172.12.1.13 group
239.2.2.2
console(config-if)# bridge multicast forbidden source 172.12.1.13
group add gil/0/21
```

4.9. Команда bridge multicast unregistered

Команда **bridge multicast unregistered** предназначена для настройки пересылки с незарегистрированных адресов многоадресной рассылки. Использование префикса **no** устанавливает значения по умолчанию.

Синтаксис:

bridge multicast unregistered { forwarding | filtering }

no bridge multicast unregistered

Параметры:

- **forwarding** – разрешает пересылку незарегистрированных мультикастовых пакетов;
- **filtering** – отфильтровывает незарегистрированные мультикастовые пакеты.

Состояние по умолчанию:

Незарегистрированные мультикастовые пакеты разрешены для пересылки.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечание:

Не рекомендуется включать фильтрацию незарегистрированной рассылки на портах, подключенных к маршрутизаторам, поскольку диапазон адресов 224.0.0.x не должен фильтроваться. Также следует иметь в виду, что маршрутизаторы не всегда отправляют отчеты IGMP для диапазона 224.0.0.x.

Пример:

```
console(config)# interface gi 1/0/24
console(config-if)# bridge multicast unregistered filtering
```

4.10. Команда bridge multicast forward-all

Команда **bridge multicast forward-all** предназначена для включения пересылки всех многоадресных пакетов на портах или агрегированных каналах. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

bridge multicast forward-all { add | remove } { ethernet *interface-list* | port-channel *port-channel-list* }

no bridge multicast forward-all

Параметры:

- **add** – добавляет порт в группу;
- **remove** – удаляет порт из группы;
- **ethernet *interface-list*** – список портов Ethernet. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис;
- **port-channel *port-channel-list*** – список портов Port-channel. Для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис.

Состояние по умолчанию:

Пересылка всех мультикастовых пакетов запрещена.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Пример:

```
console(config)# interface vlan 200
console(config-if)# bridge multicast forward-all add gi1/0/5
```

4.11. Команда bridge multicast forbidden forward-all

Команда **bridge multicast forbidden forward-all** предназначена для запрета динамического включения порта или диапазона портов в группу многоадресной рассылки. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

bridge multicast forbidden forward-all [{ **add** | **remove** }] { **ethernet** *interface-list* | **port-channel** *port-channel-list* }

no bridge multicast forbidden forward-all

Параметры:

- **add** – добавляет порт в группу;
- **remove** – удаляет порт из группы;
- **ethernet** *interface-list* – список портов Ethernet, для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис;
- **port-channel** *port-channel-list* – список портов Port-channel, для перечисления портов используется запятая и пробел, для задания диапазона портов – дефис.

Состояние по умолчанию:

Запрет динамического включения порта в группу не задан.

Опция по умолчанию: **add**.

Режим ИКС:

Режим конфигурации интерфейса (VLAN)

Пример:

```
console(config)# interface vlan 202
console(config-if)# bridge multicast forbidden forward-all add
gi1/0/7
```

4.12. Команда bridge unicast unknown

Команда **bridge unicast unknown** предназначена для включения фильтрации исходящих одноадресных пакетов с коммутатора к устройству с неизвестным MAC-адресом. Использование префикса «**no**» отключает фильтрацию.

Синтаксис:

bridge unicast unknown { **filtering** | **forwarding** }

no bridge unicast unknown

Параметры:

- **forwarding** – разрешает пересылку одноадресных пакетов на неизвестный MAC адрес;
- **filtering** – запрещает пересылку одноадресных пакетов на неизвестный MAC адрес.

Состояние по умолчанию:

Пересылка разрешена.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Пример:

```
console(config)# interface tel/0/1  
console(config-if)# bridge unicast unknown filtering
```

4.13. Команда show bridge unicast unknown

Команда **show bridge unicast unknown** предназначена для отображения на экране конфигурации фильтрации одноадресных пакетов на неизвестный MAC-адрес.

Синтаксис:

show bridge unicast unknown [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса (Ethernet или Port Channel).

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show bridge unicast unknown  
  
tel/0/1      Filter  
tel/0/2      Forward
```

4.14. Команда mac address-table static

Команда **mac address-table static** предназначена для добавления MAC-адреса источника в таблицу MAC-адресов. Использование префикса «**no**» удаляет адрес из таблицы.

Синтаксис:

mac address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-id* [{ **permanent** | **delete-on-reset** | **delete-on-timeout** | **secure** }]

no mac address-table static [*mac-address*] **vlan** *vlan-id*

Параметры:

- *mac-address* – MAC-адрес источника;
- *vlan-id* – идентификатор VLAN;
- *interface-id* – идентификатор интерфейса (Ethernet или Port Channel);
- **permanent** – постоянный статический MAC-адрес. Опция применяется по умолчанию;
- **delete-on-reset** – MAC-адрес удаляется из таблицы после перезагрузки коммутатора;
- **delete-on-timeout** – MAC-адрес удаляется из таблицы по истечению времени;
- **secure** – безопасный MAC-адрес. Может использоваться только в безопасном режиме порта.

Состояние по умолчанию:

Статические MAC-адреса не определены.

Без указания опций используется параметр **permanent**.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Команда используется для добавления статического MAC-адреса с атрибутом **time-to-live** в любом режиме. При добавлении адреса в безопасном режиме порта применяется параметр **secure**.
2. Каждому MAC-адресу в таблице адресов присваиваются два атрибута: **type** и **time-to-live**.
3. Для атрибута **time-to-live** поддерживаются следующие значения:
 - **permanent** – MAC-адрес хранится в таблице до тех пор, пока не будет удален вручную.
 - **delete-on-reset** – MAC-адрес хранится в таблице до перезагрузки коммутатора.
 - **delete-on-timeout** – MAC-адрес хранится в таблице до истечения значения таймера. Значение выставляется командой `mac address-table aging-time`.
4. Статический MAC-адрес может быть добавлен в любом режиме порта, кроме режима **secure**.
 - **secure** – MAC-адрес добавленный вручную или выученный на защищенном порту. Такой MAC-адрес не может быть выучен повторно.
 - **dynamic** – MAC-адрес выученный на порту в небезопасном режиме. Значение его атрибута **time-to-live** – **delete-on-timeout**.

Пример:

```
console(config)# mac address-table static 00:3f:bd:45:5a:b1 vlan 1
in-terface gil/0/12 permanent
```

4.15. Команда `clear mac address-table`

Команда **clear mac address-table** предназначена для удаления из FDB (forwarding database) выученных или безопасных MAC-адресов.

Синтаксис:

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

clear mac address-table secure interface *interface-id*

Параметры:

- **dynamic interface *interface-id*** – удаление всех динамических (выученных) MAC адресов полученных с определенного интерфейса (Ethernet или Port Channel). Если идентификатор интерфейса не указан, то удаляются все динамические адреса;

- **secure interface** *interface-id* – удаление всех защищенных адресов полученных с определенного интерфейса. Защищенный MAC-адрес – адрес полученный на порту работающем в защищенном режиме.

Состояние по умолчанию:

Для динамических адресов, если не указан идентификатор интерфейса, удаляются все адреса в таблице.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear mac address-table dynamic interface gi1/0/1
```

4.16. Команда mac address-table aging-time

Команда **mac address-table aging-time** предназначена для установки времени старения таблицы адресов. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

mac address-table aging-time *seconds*

no mac address-table aging-time

Параметры:

- *seconds* – количество секунд. Диапазон: 10 – 630

Состояние по умолчанию:

Время старения таблицы 300 секунд.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# mac address-table aging-time 600
```

4.17. Команда port security

Команда **port security** предназначена для включения на порту режима безопасности и перевода его в состояние обучения. Использование префикса **no** устанавливает значения по умолчанию.

Синтаксис:

port security [{ **forward** | **discard** | **discard-shutdown** }] [**trap** *seconds*]

no port security

Параметры:

- **forward** – пересылает пакеты от невыученных адресов и не запоминает адрес источника;
- **discard** – отбрасывает пакеты от невыученных адресов;
- **discard-shutdown** – отбрасывает пакеты от невыученных адресов и административно отключает порт;
- **trap seconds** – отправляет SNMP trap и задает минимальный интервал времени между последовательными отправками, в секундах. Диапазон: 1 – 1000000.

Состояние по умолчанию:

Функция по умолчанию отключена.

Режим порта по умолчанию установлен в **discard**.

По умолчанию количество секунд равно 0, но если используется параметр **trap**, то количество секунд также необходимо указать.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

1. Команда может использоваться только когда интерфейс находится в обычном режиме (не безопасном, без ограничения на обучение MAC-адресам).
2. Для получения информации об атрибутах MAC-адресов (тип и время жизни) см. команду **mac address-table static**.
3. Когда команда **port security** включает режим блокировки на порту, все динамические адреса, полученные ранее, изменяются на постоянные защищенные адреса.
4. В случае когда на порту включается режим отличный от блокировки, все динамические адреса выученные на этом порту удаляются.
5. При использовании команды **no port security**, все защищенные адреса, полученные на порту изменяются на динамические.

Пример:

```
console(config)# interface gil/0/14
console(config-if)# port security mode lock
console(config-if)# port security forward trap 100
```

4.18. Команда port security mode

Команда **port security mode** предназначена для выбора режима безопасности порта. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

```
port security mode { max-addresses | lock | secure permanent | secure delete-on-reset }  
no port security mode
```

Параметры:

- **max-addresses** – небезопасный режим, с ограниченным изучением динамических MAC-адресов, статические адреса могут быть добавлены на порт вручную, с помощью команды **mac address-table static**;
- **lock** – безопасный режим без обучения MAC-адресам, статические адреса могут быть добавлены на порт вручную, с помощью команды **mac address-table static**;
- **secure-permanent** – безопасный режим с ограниченным доступом к постоянным безопасным MAC-адресам с постоянным временем жизни, статические и безопасные MAC-адреса могут быть добавлены на порт вручную, с помощью команды **mac address-table static**;
- **secure delete-on-reset** – безопасный режим с ограниченным доступом к защищенным MAC-адресам, со временем жизни до перезагрузки коммутатора. Статические и безопасные MAC-адреса могут быть добавлены на порт вручную, с помощью команды **mac address-table static**.

Состояние по умолчанию:

По умолчанию режим защищенного порта – **lock**.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

1. Режим порта по умолчанию называется регулярным. В этом режиме порт не имеет ограничений на изучение динамических адресов.
2. Статические MAC-адреса могут быть добавлены на порт вручную, с помощью команды **mac address-table static**.
3. Команда может быть использована только тогда, когда интерфейс находится в регулярном режиме.
4. Данная команда применяется для изменения режима безопасного порта по умолчанию.

Пример:

```
console(config)# interface gil/0/14
console(config-if)# port security mode lock
console(config-if)# port security
```

4.19. Команда port security max

Команда **port security max** предназначена для задания максимального значения количества изученных адресов на порту. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

port security max *max-addr*

no port security max

Параметры:

- *max-addr* – максимальное количество адресов допустимых для изучения на порту. Диапазон: 0 – 256.

Состояние по умолчанию:

Максимальное количество адресов: 1

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечание:

Команда может быть использована только тогда, когда интерфейс находится в регулярном режиме. Данная команда применяется для изменения режима безопасного порта по умолчанию.

Пример:

```
console(config)# interface gil/0/10
console(config-if)# port security mode max-addresses
console(config-if)# port security max 20
```

4.20. Команда port security routed secure-address

Команда **port security routed secure-address** предназначена для добавления безопасного MAC-адреса на маршрутизируемый порт (порт, на который назначен IP-адрес). Использование префикса «**no**» удаляет MAC-адрес с порта.

Синтаксис:

port security routed secure-address *mac-address*

no port security routed secure-address *mac-address*

Параметры:

- *mac-address* – MAC-адрес добавляемый на порт.

Состояние по умолчанию:

MAC-адрес не определен.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel).

Примечания:

1. Команда не может быть выполнена для списка интерфейсов.
2. Команда позволяет добавлять защищенные MAC-адреса к маршрутизируемому порту, когда он находится в безопасном режиме. MAC-адрес удаляются, если порт переводится в регулярный режим или больше не является маршрутизируемым портом.

Пример:

```
console(config)# interface gil/0/10
console(config-if)# port security routed secure-address
00:66:66:66:66:66
```

4.21. Команда show mac address-table

Команда **show mac address-table** предназначена для отображения на экране таблицы MAC адресов.

Синтаксис:

```
show mac address-table [ { dynamic | static | secure } ] [ vlan vlan ] [ interface interface-id ] [ address mac-address ]
```

Параметры:

- **dynamic** – отображает только динамические MAC-адреса;
- **static** – отображает только статические MAC-адреса;
- **secure** – отображает только защищенные MAC-адреса;
- **vlan** – отображает адреса полученные с определенного VLAN;
- **interface** *interface-id* – отображает адреса полученные интерфейса с заданным идентификатором;
- **address** *mac-address* – отображает только заданный MAC-адрес.

Состояние по умолчанию:

Команда без параметров выводит все адреса в таблице.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Внутренние VLAN, которые автоматически выделяются на маршрутизируемых портах, представлены в таблице номером порта, а не идентификатором VLAN.

Пример:

```
console# show mac address-table
Flags: I - Internal usage VLAN
Aging time is 300 sec
```

Vlan	Mac Address	Port	Type
1	00:13:19:63:47:f8	gil/0/1	dynamic
1	00:19:0f:25:c5:38	gil/0/1	dynamic
1	00:19:0f:29:1d:36	gil/0/1	dynamic
1	00:19:0f:29:1d:3b	gil/0/1	dynamic
1	00:19:0f:29:1e:be	0	self
1	00:1b:53:f0:c8:3c	gil/0/1	dynamic
1	00:1b:d4:2a:42:fc	gil/0/1	dynamic
1	00:1e:4a:34:82:ba	gil/0/1	dynamic
1	00:1e:4a:a8:eb:02	gil/0/1	dynamic

1	00:23:5e:18:2f:53	gi1/0/1	dynamic
1	02:19:b4:0f:d4:f0	gi1/0/1	dynamic
1	02:19:b4:0f:d4:f1	gi1/0/1	dynamic
1	04:62:73:6d:43:4c	gi1/0/1	dynamic
1	08:00:27:80:8c:7c	gi1/0/1	dynamic
1	0c:c4:7a:ca:b4:35	gi1/0/1	dynamic
1	0c:c4:7a:ca:b4:46	gi1/0/1	dynamic
1	0c:c4:7a:ca:b4:e4	gi1/0/1	dynamic
1	1c:17:d3:40:66:11	gi1/0/1	dynamic
1	2c:23:3a:76:0e:56	gi1/0/1	dynamic
1	2c:23:3a:76:0e:79	gi1/0/1	dynamic
1	2c:4d:54:d0:90:ed	gi1/0/1	dynamic

4.22. Команда show mac address-table count

Команда **show mac address-table count** предназначена для отображения на экране общего количества адресов находящихся FDB (Forwarding Data Base).

Синтаксис:

show mac address-table count [{ vlan *vlan* | interface *interface-id* }]

Параметры:

- **vlan *vlan*** – выводит адреса относящиеся к заданному VLAN
- **interface *interface-id*** – выводит адреса принятые на заданном интерфейсе.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show mac address-table count
Capacity : 128001
Free      : 127969
Used      : 32
Secure    : 0
Dynamic   : 31
Static    : 0
Internal  : 1
```

4.23. Команда show bridge multicast mode

Команда **show bridge multicast mode** предназначена для отображения на экране режима многоадресной передачи для всех VLAN или заданного VLAN.

Синтаксис:

show bridge multicast mode [vlan *vlan-id*]

Параметры:

- ***vlan-id*** – идентификатор VLAN

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show bridge multicast mode
```

VLAN	IPv4 Multicast mode		IPv6 Multicast mode	
	Admin	Oper	Admin	Oper
1	mac-group	IPv4-Src-Group	mac-group	IPv6-Group

4.24. Команда show bridge multicast address-table

Команда **show bridge multicast address-table** предназначена для отображения на экране MAC-адреса многоадресной рассылки или информацию о таблице IP-адресов многоадресной рассылки.

Синтаксис:

show bridge multicast address-table [vlan *vlan-id*]

show bridge multicast address-table [vlan *vlan-id*] [address *mac-multicast-address*] [format { ip | mac }]

show bridge multicast address-table [vlan *vlan-id*] [address *ipv4-multicast-address*] [source *ipv4-source-address*]

Параметры:

- **vlan *vlan-id*** – идентификатор VLAN;
- **address** – отображает записи для указанного адреса многоадресной рассылки. Допустимы следующие значения:
 - *mac-multicast-address* – MAC-адрес многоадресной рассылки;
 - *ipv4-multicast-address* – IPv4-адрес многоадресной рассылки;
- **format** – применяется, если выбран параметр *mac-multicast-address*. В этом случае отображается либо MAC-адрес, либо IP. Отображает записи для указанного формата многоадресной рассылки. Допустимые значения:
 - **ip** – IP-адрес многоадресной рассылки;
 - **mac** – MAC-адрес многоадресной рассылки.
- **source** – задает адрес источника. Допустимые значения:
 - *ipv4-address* – IPv4-адрес;

Состояние по умолчанию:

Если опция **format** не задана, то по умолчанию выбирается mac (только при использовании параметра *mac-multicast-address*).

Если идентификатор VLAN не задан, то выводится информация для всех VLAN.

Если MAC или IP адрес не указаны, то выводится информация для всех адресов.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. MAC-адрес может отображаться в формате IP, только если он находится в диапазоне от 0100.5e00.0000 до 0100.5e7f.ffff.
2. Порты многоадресной рассылки маршрутизатора (заданные статически или обнаруженные динамически) являются членами во всех MAC-группах.
3. Порты заданные с помощью команды **bridge multicast forbidden forward-all** отображаются во всех запрещенных MAC-записях.
4. Изменение режима многоадресной передачи позволяет перемещать статические мультикаст адреса, записанные в FDB в теньевую конфигурацию из-за хэш коллизий FDB.

Пример:

```
console# show bridge multicast address-table

Multicast address table for VLANs in MAC-GROUP bridging mode:

Vlan      Mac Address          Type                Ports
-----  -
4         01:00:5e:02:02:03   Static              gil/1/1-5
8         01:00:5e:02:02:02   Dynamic
8         33:33:00:04:00:01   Dynamic

Forbidden ports for multicast addresses:

Vlan      Mac Address          Ports
-----  -
4         01:00:5e:02:02:03

Multicast address table for VLANs in IPv4-GROUP bridging mode:
Vlan  IP/Mac Address      Type                Ports
-----  -
-----

Forbidden ports for multicast addresses:

Vlan  IP/Mac Address      Ports
-----  -
-----

Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:
Vlan  Group Address      Source address      Type                Ports
```

```
-----  
-----  
  
Forbidden ports for multicast addresses:  
  
Vlan  Group Address  Source address          Ports  
-----  
-----  
  
-----  
  
Multicast address table for VLANs in IPv6-GROUP bridging mode:  
  
Vlan  IP/Mac Address      Type                    Ports  
-----  
-----  
-----  
  
-----  
  
Forbidden ports for multicast addresses:  
  
Vlan  IP/Mac Address          Ports  
-----  
-----  
  
-----  
  
Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:  
  
Vlan  Group Address  Source address      Type          Ports  
-----  
-----  
-----  
  
-----  
  
Forbidden ports for multicast addresses:  
  
Vlan  Group Address  Source address          Ports  
-----  
-----  
-----  
-----
```

4.25. Команда show bridge multicast address-table static

Команда **show bridge multicast address-table static** предназначена для отображения статических настроенных адресов многоадресной рассылки.

Синтаксис:

```
show bridge multicast address-table static [ vlan vlan-id ] [ all ]
```

```
show bridge multicast address-table static [ vlan vlan-id ] [ address mac-multicast-address ] [ { mac | ip } ]
```

```
show bridge multicast address-table static [ vlan vlan-id ] [ address ipv4-multicast-address ] [ source ipv4-source-address ]
```

Параметры:

- **vlan *vlan-id*** – идентификатор VLAN

- **address** – отображает записи для указанного адреса многоадресной рассылки. Допустимы следующие значения:
 - *mac-multicast-address* – MAC-адрес многоадресной рассылки;
 - *ipv4-multicast-address* – IPv4-адрес многоадресной рассылки;
- **format** – применяется, если выбран параметр *mac-multicast-address*. В этом случае отображается либо MAC-адрес, либо IP. Отображает записи для указанного формата многоадресной рассылки. Допустимые значения:
 - **ip** – IP-адрес многоадресной рассылки;
 - **mac** – MAC-адрес многоадресной рассылки;
- **source** – задает адрес источника. Допустимые значения:
 - *ipv4-address* – IPv4-адрес;

Состояние по умолчанию:

Если параметры **all/mac/ip** не указан, отображаются все записи (MAC и IP).

Режим ИКС:

Привилегированный режим управления.

Примечание:

MAC-адрес может отображаться в формате IP, только если он находится в диапазоне от 0100.5e00.0000 до 0100.5e7f.ffff.

Пример:

```
console# show bridge multicast address-table static

MAC-GROUP table:
Vlan      Mac Address                               Ports
-----  -
4         01:00:5e:02:02:03  gi1/1/1-5

Forbidden ports for multicast addresses:
Vlan      Mac Address                               Ports
-----  -
4         01:00:5e:02:02:03

IPv4-GROUP table:
Vlan      IP/Mac Address                             Ports
-----  -
8         239.2.2.2

Forbidden ports for multicast addresses:
Vlan      IP/Mac Address                             Ports
-----  -
8         239.2.2.2          gi1/1/9

IPv6-GROUP table:
Vlan      IP/Mac Address                             Ports
-----  -
```

```
8 ff00::4:4:4:1

Forbidden ports for multicast addresses:

Vlan  IP/Mac Address                               Ports
-----
8     ff00::4:4:4:1      gil1/1/9

IPv4-SRC-GROUP table:

Vlan  Group Address  Source address  Ports
-----
8     239.2.2.2      13.16.1.1

Forbidden ports for multicast addresses:

Vlan  Group Address  Source address  Ports
-----
8     239.2.2.2      13.16.1.1

IPv6-SRC-GROUP table:

Vlan  Group Address  Source address  Ports
-----
8     ff00::4:4:4:1  2001::4:4:4:4

Forbidden ports for multicast addresses:

Vlan  Group Address  Source address  Ports
-----
      ff00::4:4:4:1  2001::4:4:4:4  gil1/1/9
```

4.26. Команда show bridge multicast filtering

Команда **show bridge multicast filtering** предназначена для отображения конфигурацию фильтрации многоадресной рассылки.

Синтаксис:

show bridge multicast filtering *vlan-id*

Параметры:

- *vlan-id* – идентификатор VLAN

Состояние по умолчанию:

Отсутствует.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show bridge multicast filtering 1

Filtering: Disabled

VLAN: 1

Forward-All

Port          Static          Status
-----          -          -
gil/0/1       -             Filter
gil/0/2       -             Filter
gil/0/3       -             Filter
gil/0/4       -             Filter
gil/0/5       -             Filter
gil/0/6       -             Filter
gil/0/7       -             Filter
gil/0/8       -             Filter
gil/0/9       -             Filter
gil/0/10      -             Filter
gil/0/11      -             Filter
gil/0/12      -             Filter
```

4.27. Команда show bridge multicast unregistered

Команда **show bridge multicast unregistered** предназначена для отображения на экране конфигурации фильтрации незарегистрированной многоадресной рассылки.

Синтаксис:

show bridge multicast unregistered [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса (Ethernet или Port Channel).

Состояние по умолчанию:

Без указания идентификатора выводит информацию по всем интерфейсам.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show bridge multicast unregistered

Port          Unregistered
-----          -
gil/0/1       Forward
gil/0/2       Forward
gil/0/3       Forward
gil/0/4       Forward
gil/0/5       Forward
```

gil/0/6	Forward
gil/0/7	Forward
gil/0/8	Forward
gil/0/9	Forward
gil/0/10	Forward
gil/0/11	Forward
gil/0/12	Forward
gil/0/13	Forward
gil/0/14	Forward
gil/0/15	Forward
gil/0/16	Forward
gil/0/17	Forward
gil/0/18	Forward

4.28. Команда show ports security

Команда **show ports security** предназначена для отображения на экране статуса блокировки портов.

Синтаксис:

show ports security [{ *interface-id* | **detailed** }]

Параметры:

- *interface-id* – идентификатор интерфейса (Ethernet или Port Channel)
- **detailed** - отображает информацию о неучтенных портах в дополнение к текущим

Состояние по умолчанию:

Отображает информацию для всех интерфейсов. Если параметр **detailed** опущен, то информация отображается только по текущим портам.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ports security
```

Port	status	Learning	Action	Maximum	Trap	Frequency
gil/0/1	Disabled	Lock	-	1	-	-
gil/0/2	Disabled	Lock	-	1	-	-
gil/0/3	Disabled	Lock	-	1	-	-
gil/0/4	Disabled	Lock	-	1	-	-
gil/0/5	Disabled	Lock	-	1	-	-
gil/0/6	Disabled	Lock	-	1	-	-
gil/0/7	Disabled	Lock	-	1	-	-
gil/0/8	Disabled	Lock	-	1	-	-
gil/0/9	Disabled	Lock	-	1	-	-
gil/0/10	Disabled	Secure	-	0	-	-
		permanent				
gil/0/11	Disabled	Lock	-	1	-	-

Поля вывода:

Поле	Описание
Port	Номер порта.
Status	Статус безопасности порта. Допустимые значения: Enabled или Disabled.
Action	Действие, предпринятое при нарушении.
Maximum	Максимальное кол-во адресов, которые могут быть связаны с этим портом в режиме max-addresses.
Trap	Статус SNMP trap. Допустимые значения: Enable или Disable.
Frequency	Минимальный временной интервал между отправками SNMP trap.

4.29. Команда show ports security addresses

Команда **show ports security addresses** предназначена для отображения динамических адресов на заблокированных портах.

Синтаксис:

show ports security addresses [{ *interface-id* | **detailed }]**

Параметры:

- *interface-id* – идентификатор интерфейса (Ethernet или Port Channel);
- **detailed** - отображает информацию о неучтенных портах в дополнение к текущим.

Состояние по умолчанию:

Отображает информацию для всех интерфейсов. Если параметр **detailed** опущен, то информация отображается только по текущим портам.

Режим ИКС:

Привилегированный режим управления.

Пример:

```

console# show ports security addresses

Port      status      Learning      Current      Maximum
-----
gi1/0/1   Disabled    Lock          0            1
gi1/0/2   Disabled    Lock          0            1
gi1/0/3   Disabled    Lock          0            1
gi1/0/4   Disabled    Lock          0            1
gi1/0/5   Disabled    Lock          0            1
gi1/0/6   Disabled    Lock          0            1
gi1/0/7   Disabled    Lock          0            1
gi1/0/8   Disabled    Lock          0            1
gi1/0/9   Disabled    Lock          0            1
gi1/0/10  Disabled    Secure
                    permanent

```

4.30. Команда `bridge multicast reserved-addresses`

Команда **bridge multicast reserved-addresses** предназначена для определения действия на пакеты от зарезервированных адресов многоадресной передачи. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

bridge multicast reserved-address *mac-multicast-address* [{ **ethernet-v2** *ethtype* | **llc sap** | **llc-snap** *pid* }] [{ **discard** | **bridge** }

no bridge multicast reserved-address *mac-multicast-address* [{ **ethernet-v2** *ethtype* | **llc sap** | **llc-snap** *pid* }]

Параметры:

- *mac-multicast-address* – MAC-адрес многоадресной рассылки из зарезервированного диапазона: 01-80-C2-00-00-00, 01-80-C2-00-00-02 — 01-80-C2-00-00-2F;
- **ethernet-v2** *ethtype* – тип пакета Ethernet v2 и тип поля (16 цифр в шестнадцатеричном формате). Диапазон: 0x0600 – 0xFFFF;
- **llc sap** – тип пакета LLC и поля DSAP-SSAP (16 цифр в шестнадцатеричном формате). Диапазон: 0xFFFF;
- **llc-snap** *pid* - тип пакета LLC-SNAP и PID поля (40 цифр в шестнадцатеричном формате). Диапазон: 0x0000000000 - 0xFFFFFFFFFFFF;
- **discard** – отбрасывает пакет;
- **bridge** – переадресовывает пакет.

Состояние по умолчанию:

Если заданный пользователем MAC-адрес многоадресной рассылки, *ethtype* и инкапсуляция (LLC) указывает протокол, поддерживаемый на устройстве, то действие по умолчанию (**discard** или **bridge**) определяется протоколом.

Если нет, то действие по умолчанию выглядит следующим образом:

- для MAC-адресов в диапазоне 01-80-C2-00-00-00, 01-80-C2-00-00-02 — 01-80-C2-00-00-0F, по умолчанию **discard**.
- для MAC-адресов в диапазоне 00-80-C2-00-00-10 – 01-80-C2-00-00-2F, по умолчанию **bridge**.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

- Если тип для пакета/сервиса (*ethertype/encapsulation*) не указан, то конфигурация относится ко всем пакетам с настроенным MAC-адресом.
- Конфигурации содержащие тип сервисе имеют приоритет перед конфигурациями содержащими только MAC-адрес.
- Пакеты проходящие через мост подлежат обработке списками доступа (ACL).

- Действия, определяемые данной командой, имеют приоритет над правилами пересылки, определяемыми приложениями/протоколами (STP, LLDP и т.д.), поддерживаемыми на коммутаторе.

Пример:

```
console(config)# bridge multicast reserved-address 01-80-C2-00-00-10 bridge
```

4.31. Команда show bridge multicast reserved-addresses

Команда **show bridge multicast reserved-addresses** предназначена для отображения на экране правил резервирования адресов многоадресной рассылки.

Синтаксис:

show bridge multicast reserved-addresses

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show bridge multicast reserved-addresses
```

MAC Address	Frame type	Protocol	Action
01:80:c2:00:00:10	none	-	bridge

5. КОМАНДЫ УПРАВЛЕНИЯ ЗАГРУЗКОЙ ПО СЕТИ

5.1. Команда `boot host auto-config`

Команда **`boot host auto-config`** предназначена для автоматической настройки коммутатора посредством протокола DHCP. Использование префикса «**no**» отключает данную функцию.

Синтаксис:

`boot host auto-config [{ tftp | scp | auto [extension] }]`

`no boot host auto-config`

Параметры:

- **`tftp`** – используется протокол TFTP;
- **`scp`** – используется протокол SCP;
- **`auto`** – протокол выбирается в зависимости от расширения файла конфигурации. При указании этого параметра должно быть указано расширение файла, в противном случае используется расширение по умолчанию. Данный параметр применяется по умолчанию;
- *extension* – задает расширение для файла. Если опция не указана, то используется расширение «.scr». Диапазон: 1 – 16.

Состояние по умолчанию:

По умолчанию используется параметр **`auto`**.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Для загрузки/выгрузки файла конфигурации используется протокол TFTP или SCP.

Примеры:

Пример 1:

Используется параметр `auto`. Для файла указано расширение «.scon».

```
console(config)# boot host auto-config auto scon
```

Пример 2:

Используется параметр `auto`. Расширение не задано.

```
console(config)# boot host auto-config auto
```

Пример 3:

Используется протокол SCP.

```
console(config)# boot host auto-config scp
```


5.2. Команда boot host auto-update

Команда **boot host auto-update** предназначена для включения поддержки автоматического обновления через DHCP. Использование префикса «**no**» отключает функцию.

Синтаксис:

```
boot host auto-update [ { tftp | scp | auto [ extension ] } ]
```

no boot host auto-update

Параметры:

- **tftp** – используется протокол TFTP;
- **scp** – используется протокол SCP;
- **auto** – протокол выбирается в зависимости от расширения файла конфигурации. При указании этого параметра должно быть указано расширение файла, в противном случае используется расширение по умолчанию. Данный параметр применяется по умолчанию;
- *extension* – задает расширение для файла. Если опция не указана, то используется расширение «.scp». Диапазон: 1 – 16.

Состояние по умолчанию:

По умолчанию используется параметр **auto**.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Для загрузки/выгрузки файла конфигурации используется протокол TFTP или SCP.

Примеры:

Пример 1:

Используется параметр **auto**. Для файла указано расширение «.scon».

```
console(config)# boot host auto-update auto scon
```

Пример 2:

Используется параметр **auto**. Расширение не задано.

```
console(config)# boot host auto-update auto
```

Пример 3:

Используется протокол **SCP**.

```
console(config)# boot host auto-update scp
```

5.3. Команда show boot

Команда **show boot** предназначена для отображения на экране состояния процесса автоматической настройки IP DHCP.

Синтаксис:

show boot

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show boot
Auto Config
-----
Config Download via DHCP: enabled
Download protocol: auto
SCP protocol will be used for files with extension: scp
Next Boot Config Download via DHCP: default

Auto Update
-----
Image Download via DHCP: enabled
Download protocol: auto
SCP protocol will be used for files with extension: scp
```

5.4. Команда ip dhcp tftp-server address

Команда **ip dhcp tftp-server address** предназначена для задания IP-адреса резервного сервера. Использование префикса «no» устанавливает значения по умолчанию.

Синтаксис:

ip dhcp tftp-server ip address *ip-addr*

no ip dhcp tftp-server ip address

Параметры:

- *ip-addr* – IPv4, или DNS имя TFTP или SCP сервера.

Состояние по умолчанию:

IP адрес не задан.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Данный адрес используется коммутатором, если основной адрес не был получен с сервера DHCP.

Пример:

```
console(config)# ip dhcp tftp-server ip address 172.12.0.32
```

5.5. Команда ip dhcp tftp-server file

Команда **ip dhcp tftp-server file** предназначена для задания полного имени файла конфигурации. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip dhcp tftp-server file *file-path*

no ip dhcp tftp-server file

Параметры:

- *file-path* – полный путь и имя файла конфигурации на сервере.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Указывается полный путь и имя файла конфигурации для загрузки, если не было получено от DHCP сервера.

Пример:

```
console(config)# ip dhcp tftp-server file conf/bcp.scp
```

5.6. Команда ip dhcp tftp-server image file

Команда **ip dhcp tftp-server image file** предназначена для задания полного пути к имени файла прошивки на сервере резервного копирования. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip dhcp tftp-server image file *file-path*

no ip dhcp tftp-server image file

Параметры:

- *file-path* – полный путь и имя файла прошивки на сервере.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Указывается полный путь и имя файла прошивки для загрузки, если не было получено от DHCP сервера.

Пример:

```
console(config)# ip dhcp tftp-server image file image/412.img
```

5.7. Команда show ip dhcp tftp-server

Команда **show ip dhcp tftp-server** отображает на экране конфигурацию для резервного сервера.

Синтаксис:

show ip dhcp tftp-server

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp tftp-server
server address
active
manual          172.12.0.32
file path on server
active
manual          conf/bcp.scp
image indirect file path on server
manual          image/412.img
```

6. КОМАНДЫ УСТАНОВКИ ДАТЫ И ВРЕМЕНИ

6.1. Команда absolute

Команда **absolute** предназначена для задания абсолютного времени действия временного диапазона. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

absolute start *hh:mm day month year*

no absolute start

absolute end *hh:mm day month year*

no absolute end

Параметры:

- **start** – абсолютные дата и время, когда вступает в силу разрешение/запрет для связанной функции. Если время начала и дата не указаны, функция действует немедленно;
- **end** – абсолютные дата и время, когда разрешение/запрет для связанной функции прекращает свое действие. Если время начала и дата не указаны, функция действует бесконечно;
- *hh:mm* – время в часах и минутах (24-х часовой формат). Диапазон: 0 – 23 ч. 0 – 55 мин.
- *day* – день месяца (число). Диапазон: 1 – 31.
- *month* – месяц (первые три буквы названия (англ.)). Возможные значения: **Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec**.
- *year* – год. Диапазон: 2000-2097.

Состояние по умолчанию:

Абсолютное время не задано.

Режим ИКС:

Режим конфигурации временного диапазона

Пример:

```
console(config)# time-range http-allowed
console(config-time-range)# absolute start 23:55 1 jan 2009
console(config-time-range)# absolute end 00:00 1 dec 2009
```

6.2. Команда `clock dhcp timezone`

Команда **clock dhcp timezone** предназначена для установки летнего времени и временной зоны в системных часах коммутатора, при помощи опции `Timezone` сервера DHCP. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

clock dhcp timezone

no clock dhcp timezone

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Временная зона полученная от сервера DHCP имеет приоритет над статической временной зоной.
2. Летнее время полученное от сервера DHCP имеет приоритет над статическим летним временем.
3. Временная зона и летнее время остаются в силе после истечения аренды IP-адреса.
4. Временная зона и летнее время полученные от сервера DHCP очищаются после перезагрузки устройства.
5. При использовании префикса по установки летнего времени и временной зоны полученные от сервера DHCP сбрасываются.
6. В случае использования нескольких интерфейсов использующих DHCP применяется следующий приоритет:
 - информация полученная от DHCPv6 имеет больший приоритет, чем информация полученная от DHCPv4.
 - информация полученная от клиента DHCP, работающего на нижнем интерфейсе имеет больший приоритет, чем информация полученная от клиента DHCP работающего на более высоко-ком интерфейсе.
7. Отключение DHCP-клиента, на котором была выбрана опция **DHCP-TimeZone** очищает динамическую конфигурацию временной зоны и летнего времени.

Пример:

```
console(config)# clock dhcp timezone
```

6.3. Команда `clock set`

Команда **clock set** предназначена для установки системных часов вручную.

Синтаксис:

clock set *hh:mm:ss* { *day month* | *month day* } *year*

Параметры:

- *hh:mm:ss* – текущее время в часах (24-х часовой формат), минутах и секундах. Диапазон: hh: 0 – 23, mm: 0 – 59, ss: 0 – 59.

- *day* – день месяца (число). Диапазон: 1 – 31.
- *month* – месяц (первые три буквы англ. названия). Возможные значения: **Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec**.
- *year* – год. Диапазон: 2000 – 2037.

Состояние по умолчанию:

Отсчет начинается от времени обновления ПО коммутатора.

Режим ИКС:

Привилегированный режим управления.

Примечание:

После загрузки системные часы устанавливаются на аппаратное время.

Пример:

```
console# clock set 12:13:00 jan 23 2018
```

6.4. Команда clock source

Команда **clock source** предназначена для установки внешнего источника времени для системных часов. Использование префикса «**no**» отключает внешний источник.

Синтаксис:

clock source { sntp | browser }

no clock source { sntp | browser }

Параметры:

- **sntp** – в качестве источника времени задает SNTP сервер.
- **browser** – в качестве источника времени задает локальное время браузера рабочей станции.

Состояние по умолчанию:

Внешний источник времени не задан.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

В случае, если системное время не установлено и сервер SNTP не задан, то в качестве источника времени будет использовано локальное время браузера, с которого будет осуществлен вход на коммутатор.

Пример:

```
console(config)# clock source sntp
```

6.5. Команда clock summer-time

Команда **clock summer-time** предназначена для настройки автоматического перехода на летнее время и обратно. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

clock summer-time *zone* **recurring** { **usa** | **eu** | *week day month hh:mm week day month hh:mm* } [*offset*]

clock summer-time *zone* **date** *day month year hh:mm date month year hh:mm* [*offset*]

clock summer-time *zone* **date** *month day year hh:mm month day year hh:mm* [*offset*]

no clock summer-time

Параметры:

- *zone* – аббревиатура временной зоны. До 4 символов;
- **recurring** – указывает что летнее время начинается и заканчивается в определенные дни каждый год;
- **date** – указывает дату начала (первая дата) и окончания летнего времени (вторая дата);
- **usa** – летнее время устанавливается по правилам США;
- **eu** – летнее время устанавливается по правилам Европейского союза;
- *week* – неделя месяца. Допустимые значения: 1 – 5, first, last;
- *day* – день недели. Используются первые три символа названия дня (англ.). Возможные значения: **mon, tue, wed, thu, fri, sat** и **sun**;
- *date* – день месяца (число). Диапазон: 1 – 31;
- *month* – месяц. Первые три символа названия. Возможные значения: **Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec**;
- *year* – год. Диапазон: 2000-2097;
- *hh:mm* – время (24-х часовой формат) в часах и минутах. Диапазон: hh: 0 – 23, mm: 0 – 59;
- *offset* – количество минут добавляемых к текущему времени при переходе на летнее (по умолчанию – 60 мин). Максимально: 1440 мин.

Состояние по умолчанию:

Переход на летнее время отключен.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

В параметрах **date** и **recurring** первая дата указывает на время начала периода, а вторая на окончание. Все установки относятся к текущей временной зоне. Время начала относительно стандартного времени, а время окончания – летнего. Если месяц начала периода хронологически хронологически после месяца окончания, то система предполагает, что вы находитесь в южном полушарии.

Правила перехода на летнее время принятые в США:

С 2007 года:

- начало – второе воскресенье марта;
- окончание – первое воскресенье ноября;
- время перехода – 2 часа ночи.

До 2007 года:

- начало – первое воскресенье апреля;
- окончание – последнее воскресенье октября;
- время перехода – 2 часа ночи.

Правила перехода на летнее время принятые в ЕС:

- начало – последнее воскресенье марта;
- окончание – последнее воскресенье октября;
- время перехода 1 час ночи по Гринвичу (GMT).

Пример:

```
console(config)# clock summer-time MSD date 31 mar 2017 03:00 31  
oct 2017 03:00
```

6.6. Команда clock timezone

Команда **clock timezone** предназначена для установки временной зоны. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

clock timezone *zone hours-offset [minutes-offset]*

no clock timezone

Параметры:

- *zone* – аббревиатура временной зоны. До 4 символов;
- *hours-offset* – сдвиг в часах относительно UTC. Диапазон: -12 – +13.
- *minutes-offset* – сдвиг в минутах относительно UTC. Диапазон: 0 – 59.

Состояние по умолчанию:

По умолчанию временная зона установлена в UTC или GMT, при сдвиге в 0 и пустой аббревиатурой.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Системное время внутри ПО хранится в UTC. Данная команда необходима для преобразования формата времени при выводе на экран.

Пример:

```
console(config)# clock timezone MSK +4
```

6.7. Команда `periodic`

Команда **periodic** предназначена для создания повторяющегося (недельного) диапазона времени используемого функциями с поддержкой временных диапазонов.

Синтаксис:

periodic *day-of-the-week* *hh:mm* **to** *day-of-the-week* *hh:mm*

no periodic *day-of-the-week* *hh:mm* **to** *day-of-the-week* *hh:mm*

periodic list *hh:mm* **to** *hh:mm* *day-of-the-week1* [*day-of-the-week2* ... *day-of-the-week7*]

no periodic list *hh:mm* **to** *hh:mm* *day-of-the-week1* [*day-of-the-week2* ... *day-of-the-week7*]

periodic list *hh:mm* **to** *hh:mm* **all**

no periodic list *hh:mm* **to** *hh:mm* **all**

Параметры:

- *day-of-the-week* – первое вхождение – день недели начала действия диапазона, второе вхождение – день окончания действия. Второе вхождение может приходиться на следующую неделю. Возможные значения: **mon, tue, wed, thu, fri, sat** и **sun**.
- *hh:mm* – первое вхождение – часы и минуты (в 24-х часовом формате) дня начала действия диапазона, второе вхождение – часы и минуты окончания действия. Второе вхождение может приходиться на следующие сутки. Допустимые значения: hh: 0 – 23, mm: 0 – 59.
- **list** *day-of-the-week* – задает список дней, в течении которых действует временной диапазон.

Состояние по умолчанию:

Повторяющиеся диапазоны не заданы.

Режим ИКС:

Режим конфигурации временного диапазона

Примечания:

1. Второе вхождения дня может приходиться на следующую неделю. Например диапазон «четверг – понедельник» будет действовать четверг, пятницу, субботу, воскресенье и понедельник.
2. Второе вхождение часов и минут может приходиться на следующие сутки. Например: «22:00 – 3:00».

Пример:

```
console(config)# time-range ssh-allowed
```

```
console(config-time-range)# periodic mon 09:00 to fri 19:00
```

6.8. Команда `sntp anycast client enable`

Команда **sntp anycast client enable** предназначена для включения клиента SNTP anycast. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

sntp anycast client enable

no sntp anycast client enable

Состояние по умолчанию:

SNTP Anycast клиент отключен.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# sntp anycast client enable
```

6.9. Команда `sntp authenticate`

Команда **sntp authenticate** предназначена для включения аутентификации трафика с SNTP серверов. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

sntp authenticate

no sntp authenticate

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Аутентификация отключена.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# sntp authenticate
console(config)# sntp authentication-key 1 md5 CmdKey
console(config)# sntp trusted-key 1
```

6.10. Команда `sntp authentication-key`

Команда **sntp authentication-key** предназначена для задания ключа аутентификации для SNTP сервера. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

sntp authentication-key *key-number* **md5** *key-value*

no sntp authentication-key *key-number*

Параметры:

- *key-number* – задает номер ключа. Диапазон: 1 – 4294967295.
- *key-value* – задает значение ключа. Длина: 1 – 8 символов.

Состояние по умолчанию:

Ключи аутентификации не заданы.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)#sntp authenticate
console(config)#sntp authentication-key 1 md5 CmdKey
console(config)#sntp trusted-key 1
```

6.11. Команда `sntp broadcast client enable`

Команда **sntp broadcast client enable** предназначена для включения широковещательного SNTP клиента. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

sntp broadcast client enable

no sntp broadcast client enable

Состояние по умолчанию:

Широковещательный SNTP клиент отключен.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Для включения широковещательного клиента на определенном интерфейсе необходимо выполнить команду в режиме конфигурации интерфейса.
2. После выполнения команды, необходимо выполнить команду **clock source** с параметром **sntp**. Если эта команда не будет выполнена, то коммутатор не сможет синхронизироваться с широковещательными SNTP серверами.

Пример:

```
console(config)# sntp broadcast client enable  
console(config)# clock source sntp
```

6.12. Команда sntp client enable

Команда предназначена для включения широковещательного или anycast клиента SNTP. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

sntp client enable *interface-id*

no sntp client enable *interface-id*

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые значения: Ethernet, Port channel или VLAN.

Состояние по умолчанию:

SNTP клиент отключен.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# sntp client enable vlan 120
```

6.13. Команда sntp client enable (interface)

Команда **sntp client enable** (interface) предназначена для включения широковещательного или anycast клиента SNTP на интерфейсе. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

sntp client enable

no sntp client enable

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

SNTP клиент на интерфейсе отключен.

Режим ИКС:

Режим конфигурации интерфейса

Пример:

```
console(config)# interface vlan 130
console(config-if)# sntp client enable
```

6.14. Команда sntp server

Команда **sntp server** предназначена для настройки устройства на использование SNTP запросов и принятия трафика NTP с указанного сервера. Использование префикса «**no**» удаляет сервер из списка.

Синтаксис:

```
sntp server { ip-address | hostname } [ poll ] [ key keyid ]
```

```
no sntp server [ { ip-address | hostname } ]
```

Параметры:

- *ip-address* – задает IP адрес сервера. Может использовать IPv4, IPv6 или IPv6z;
- *hostname* – сетевое имя сервера. Поддерживается трансляция только для IPv4 адресов. Длина: 1 -158 символов. Максимальная длина части имени хоста: 63 символа;
- **poll** – включает опрос;
- **key** *keyid* – указывает ключ аутентификации, который будет использовать при отправке пакетов на данный сервер. Диапазон: 1 – 4294967295.

Состояние по умолчанию:

SNTP сервера не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Поддерживается до 8 SNTP серверов.
2. Команда **no sntp server** заданная без параметров удаляет все SNTP сервера из конфигурации.

Пример:

```
console(config)#sntp server ntp.kraftway.ru poll
```

6.15. Команда sntp source interface

Команда **sntp source interface** предназначена для указания интерфейса источника, IPv4 адрес которого будет использоваться для связи с серверами SNTP IPv4. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

```
sntp source-interface interface-id
```

no sntp source-interface

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые значения: Ethernet, Port channel или VLAN.

Состояние по умолчанию:

IPv4 адрес на исходящем интерфейсе должен принадлежать подсети следующего узла.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Если интерфейс источника является исходящим интерфейсом, применяется IPv4-адрес интерфейса, принадлежащий подсети IPv4 следующего узла.
2. Если интерфейс источника не является исходящим, то применяется минимальный IPv4 адрес, заданный на интерфейсе.
3. Если IPv4 адрес источника отсутствует, то при попытке связаться с сервером SNTP выдается сообщение в SYSLOG.
4. ООВ интерфейс не может быть определен как источник.

Пример:

```
console(config)# sntp source-interface vlan 10
```

6.16. Команда sntp trusted-key

Команда **sntp trusted-key** предназначена для выбора доверенного ключа. Использование префикса «**no**» удаляет доверенный ключ.

Синтаксис:

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

Параметры:

- *key-number* – номер доверенного ключа, используемого для аутентификации. Диапазон: 1 – 4294967295.

Состояние по умолчанию:

Доверенные ключи не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Доверенный ключ используется для аутентификации всех серверов, не имеющих персональных ключей, назначенных командой **sntp server**.

Пример:

```
console(config)# sntp authenticate
console(config)# sntp authentication-key 1 md5 CmdKey
console(config)# sntp trusted-key 1
```

6.17. Команда sntp unicast client enable

Команда **sntp unicast client enable** предназначена для включения одноадресного SNTP клиента. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

sntp unicast client enable

no sntp unicast client enable

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Одноадресный SNTP клиент отключен.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Для определения SNTP серверов используется команда **sntp server**.

Пример:

```
console(config)# sntp unicast client enable
```

6.18. Команда sntp unicast client poll

Команда **sntp unicast client poll** предназначена для включения запросов одноадресных SNTP клиентов. Использование префикса «**no**» отключает запросы.

Синтаксис:

sntp unicast client poll

no sntp unicast client poll

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Функция отключена.

Примечание:

Интервал запросов составляет 1024 с.

Пример:

```
console(config)#sntp unicast client poll
```

6.19. Команда show clock

Команда **show clock** предназначена для отображения на экране текущей даты и времени системных часов.

Синтаксис:

show clock [detail]

Параметры:

- **detail** – отображает временную зону и конфигурацию летнего времени.

Режим ИКС:

Пользовательский режим управления.

Примечание:

Перед временем дополнительно выводятся следующие символы:

- * (звездочка) – время не установлено;
- . (точка) – время установлено вручную;
- _ (пробел) – время получено по протоколу SNTP.

Примеры:

Пример 1:

```
console# show clock
.16:26:03 MSK Mar 16 2018
Time source is sntp
Time from Browser is disabled
```

Пример 2:

```
console# show clock detail
.16:29:17 MSK Mar 16 2018
Time source is sntp
Time from Browser is disabled

Time zone (Static):
Acronym is MSK
Offset is UTC+4

Summertime (Static):
Acronym is MSD
Starting and ending on a specific date.
Begins at Mar 31, 2017, at 03:00.
```

```
Ends at Oct 31, 2017, at 03:00.  
Offset is 60 minutes.
```

```
DHCP timezone: Enabled
```

6.20. Команда show sntp configuration

Команда **show sntp configuration** предназначена для вывода на экран конфигурацию SNTP на коммутаторе.

Синтаксис:

show sntp configuration

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show sntp configuration  
SNTP destination port : 123 .  
Polling interval: 1024 seconds.  
MD5 authentication keys.(Encrypted)  
-----  
1          x5zGqv2kpWwupkpax73H75n1hg+uPc9clFuGKveumFY=  
-----  
Authentication is required for synchronization.  
No trusted keys.  
  
Unicast Clients: Disabled  
Unicast Clients Polling: Disabled  
  
Broadcast Clients: enabled for IPv4  
Anycast Clients: disabled  
Broadcast Interfaces: Vlans(120,130)  
Source IPv4 interface: vlan 10  
Source IPv6 interface: gil/0/12
```

6.21. Команда show sntp status

Команда **show sntp status** предназначена для вывода на экран информации о текущем статусе серверов SNTP.

Синтаксис:

show sntp status

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is afe2525e.70597b34 (00:10:22.438 PDT Jul 5 1993)
Unicast servers:
Server: 176.1.1.8
Source: DHCPv4 on VLAN 1
Status: Up
Last response: 19:58:22.289 PDT Feb 19 2005
Stratum Level: 1
Offset: 7.33mSec
Delay: 117.79mSec
Server: dns_server.comapany.com
Source: static
Status: Unknown
Last response: 12:17.17.987 PDT Feb 19 2005
Stratum Level: 1
Offset: 8.98mSec
Delay: 189.19mSec
Server: 3001:1:1::1
Source: DHCPv6 on VLAN 2
Status: Unknown
Last response:
Offset: mSec
Delay: mSec
Server: dns1.company.com
Source: DHCPv6 on VLAN 20
Status: Unknown
Last response:
Offset: mSec
Delay: mSec
Anycast servers:
Server: 176.1.11.8
Interface: VLAN 112
Status: Up
Last response: 9:53:21.789 PDT Feb 19 2005
Stratum Level: 10
Offset: 9.98mSec
Delay: 289.19mSec
Broadcast servers:
Server: 3001:1:1:12
Interface: VLAN 101
Last response: 9:53:21.789 PDT Feb 19 2005
Stratum Level: 255
```

6.22. Команда `show time-range`

Команда **show time-range** предназначена для вывода на экран информации о временных диапазонах.

Синтаксис:

show time-range *time-range-name*

Параметры:

- *time-range-name* – имя существующего временного диапазона.

Состояние по умолчанию:

Использование команды без параметра *time-range-name* отображает все существующие временные диапазоны.

Режим ИКС:

Пользовательский режим управления.

Пример:

```
console# show time-range
time-range http-allowed
absolute start 23:55 1 Jan 2019 end 00:00 1 Dec 2019
time-range ssh-allowed
periodic Monday 09:00 to Friday 19:00
```

6.23. Команда `time-range`

Команда **time-range** создает временной диапазон и выполняет вход в режим его настройки (режим конфигурации временного диапазона). Использование префикса «**no**» удаляет временной диапазон.

Синтаксис:

time-range *time-range-name*

no time-range *time-range-name*

Параметры:

- *time-range-name* – задает имя временного диапазона. Длина: 1 – 32 символа.

Состояние по умолчанию:

Временные диапазоны не определены.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. После задания имени диапазона и перехода в режим его конфигурации, команды **absolute** и **periodic** используются для фактической его настройки. Допускается множественное использование команды **periodic** и только одно использование команды **absolute**.
2. Если в диапазоне используются как абсолютные, так и периодические значения, то периодические элементы оцениваются только после достижения абсолютного начала времени и не оцениваются снова после достижения абсолютного конца времени.
3. Все заданные значения времени интерпретируются как местное время.
4. Чтобы гарантировать правильное выполнение диапазона (в требуемые значения времени), часы на устройстве должны быть предварительно настроены администратором или с помощью протокола SNTP. Если часы предварительно не установлены, правила диапазона не активируются.

Пример:

```
console(config)# time-range http-allowed  
console(config-time-range)# periodic mon 12:00 to wed 17:00
```

7. КОМАНДЫ ОТСЛЕЖИВАНИЯ DHCP

7.1. Команда ip dhcp snooping

Команда **ip dhcp snooping** предназначена для общего включения функции отслеживания DHCP. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip dhcp snooping

no ip dhcp snooping

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Отслеживание DHCP отключено.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Для использования любых функций отслеживания DHCP необходимо чтобы механизм был включен глобально.
2. Отслеживание DHCP в VLAN не будет активно до тех пор, пока не будет применена команда **ip dhcp snooping vlan**.

Пример:

```
console(config)# ip dhcp snooping
```

7.2. Команда ip dhcp snooping vlan

Команда **ip dhcp snooping vlan** предназначена для включения функции отслеживания DHCP на VLAN. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping vlan *vlan-id*

Параметры:

- *vlan-id* – идентификатор VLAN.

Состояние по умолчанию:

Отслеживание DHCP на VLAN отключено.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Функция отслеживания DHCP должна быть предварительно включена глобально, до включения ее на VLAN.

Пример:

```
console(config)# ip dhcp snooping
console(config)# ip dhcp snooping vlan 121
```

7.3. Команда ip dhcp snooping trust

Команда **ip dhcp snooping trust** предназначена для настройки порта в качестве доверенного, для отслеживания DHCP. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip dhcp snooping trust

no ip dhcp snooping trust

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Интерфейс не является доверенным.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

- Доверенными назначаются порты, подключенные к DHCP-серверу или другим коммутаторам и маршрутизаторам.
- Состояние клиентских портов остается недоверенным.

Пример:

```
console(config)# interface tel/0/1
console(config-if)# ip dhcp snooping trust
```

7.4. Команда ip dhcp snooping information option allowed-untrusted

Команда **ip dhcp snooping information option allowed-untrusted** предназначена для включения разрешения принимать DHCP-пакеты с Option-82 от недоверенного порта. Использование префикса «**no**» отключает функцию и данные пакеты отбрасываются.

Синтаксис:

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Прием пакетов с Option-82 запрещен.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip dhcp snooping information option allowed-untrusted
```

7.5. Команда ip dhcp snooping verify

Команда **ip dhcp snooping verify** предназначена для включения режима проверки того, что исходный MAC-адрес в пакете DHCP, полученный на недоверенном порту, соответствует аппаратному адресу клиента. Использование префикса «**no**» отключает проверку.

Синтаксис:

ip dhcp snooping verify

no ip dhcp snooping verify

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Коммутатор проверяет соответствие полученного MAC-адреса в пакете DHCP полученным на недоверенном порту с аппаратным адресом клиента.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip dhcp snooping verify
```

7.6. Команда ip dhcp snooping database

Команда **ip dhcp snooping database** предназначена для создания файла базы данных (БД) отслеживания привязки DHCP. Использование префикса «**no**» удаляет файл.

Синтаксис:

ip dhcp snooping database

no ip dhcp snooping database

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Файл базы данных отсутствует.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Файл базы данных создается во Flash-памяти.
2. Чтобы обеспечить точное время аренды в базе данных, необходимо включить и настроить протокол SNTP (Simple Network Time Protocol).
3. Устройство записывает изменения привязки в базу данных только в том случае, если системные часы синхронизируются по SNTP.

Пример:

```
console(config)# ip dhcp snooping database
```

7.7. Команда ip dhcp snooping binding

Команда **ip dhcp snooping binding** предназначена для настройки базы данных привязки DHCP и добавления статических записей привязки в базу данных. Использование префикса «**no**» удаляет запись из базы.

Синтаксис:

ip dhcp snooping binding *mac-address* *vlan-id* *ip-address* *interface-id* **expiry** { *seconds* | **infinite** }

no ip dhcp snooping binding *mac-address* *vlan-id*

Параметры:

- *mac-address* – MAC-адрес;
- *vlan-id* – идентификатор VLAN;
- *ip-address* – IP-адрес;
- *interface-id* – идентификатор интерфейса. Допустимы следующие типы: Ethernet, Port-channel;
- **expiry**
 - *seconds* - интервал времени в секундах, по истечении которого привязка считается не действительной;
 - **infinite** – бесконечное время аренды.

Состояние по умолчанию:

Записи о статических привязках отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Команда используется для добавления статических записей в базу данных DHCP.
2. После ввода команды, запись добавляется в БД отслеживания DHCP. Если файл БД существует, запись также добавляется и в файл.
3. Добавленная запись не будет добавлена в файлы конфигурации. Запись будет отображаться в выводах команд `show` как запись “DHCP Snooping”.
4. Запись, добавленная этой командой, может переопределить аналогичную динамическую запись.
5. Запись, добавленная этой командой, не может переопределить аналогичную статическую запись добавленную командой **ip source-guard binding**.
6. Команда **no ip dhcp snooping binding** удаляет все записи из БД DHCP.
7. Динамические записи, у которых IP-адрес 0.0.0.0, не могут быть удалены.

Пример:

```
console# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1  
tel1/0/2 expiry 900
```

7.8. Команда `clear ip dhcp snooping database`

Команда **clear ip dhcp snooping database** предназначена для очистки базы данных привязок DHCP.

Синтаксис:

clear ip dhcp snooping database

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear ip dhcp snooping database
```

7.9. Команда `show ip dhcp snooping`

Команда **show ip dhcp snooping** предназначена для отображения конфигурации отслеживания DHCP для всех интерфейсов или для заданного.

Синтаксис:

show ip dhcp snooping [interface-id]

Параметры:

- *interface-id* – идентификатор интерфейса.

Режим ИКС:

Пользовательский режим управления.

Пример:

```
console# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 121
DHCP snooping database is Enabled
Relay agent Information option 82 is Disabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled

  Interface      Trusted
  -----
te1/0/1          Yes
```

7.10. Команда show ip dhcp snooping binding

Команда **show ip dhcp snooping binding** предназначена для отображения на экране данных о привязке в БД DHCP и информации о конфигурации для всех интерфейсов или указанного.

Синтаксис:

show ip dhcp snooping binding [mac-address *mac-address*] [ip-address *ip-address*] [vlan *vlan-id*] [interface-id]

Параметры:

- *mac-address* – аппаратный адрес клиента;
- *ip-address* – IP-адрес клиента;
- *vlan-id* – идентификатор VLAN;
- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port-channel.

Режим ИКС:

Пользовательский режим управления.

Пример:

```
console# show ip dhcp snooping binding
Total number of binding: 2

  MAC Address      IP Address  Lease (sec)  Type   VLAN  Inter-face
  -----
00:60:70:4c:73:ff  172.17.18.1  -            snooping  1     gi1/0/1
00:60:70:4c:7b:c1  172.17.18.4  -            snooping  1     gi1/0/1
```

7.11. Команда ip source-guard

Команда **ip source-guard** предназначена для включения функции IP Source Guard. В зависимости от режима ИКС команда выполняется как глобально, так и для отдельного интерфейса (Ethernet, Port-channel, VLAN). Использование префикса «**no**» отключает функцию защиты.

Синтаксис:

ip source-guard

no ip source-guard

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Функция IP Source Guard отключена.

Режим ИКС:

Режим глобальной конфигурации

Режим конфигурации интерфейса (Ethernet, Port-channel, VLAN)

Примечания:

1. Прежде чем применить команду на интерфейсе, необходимо ее выполнить в общем режиме конфигурации.
2. Механизм IP Source Guard будет активен только на недоверенных интерфейсах, и если по крайней мере одна из интерфейсов VLAN поддерживает DHCP Snooping.

Пример:

```
console(config)# ip source-guard
console(config)# interface vlan 1
console(config-if)# ip source-guard
```

7.12. Команда ip source-guard binding

Команда **ip source-guard binding** предназначена для задания статических привязок IP источника на коммутаторе. Использование префикса «**no**» удаляет привязку.

Синтаксис:

ip source-guard binding mac-address mac-address vlan vlan-id ip-address ip-address
interface interface-id

no ip source-guard binding mac-address mac-address vlan vlan-id

Параметры:

- *mac-address* – аппаратный адрес клиента.
- *ip-address* – IP-адрес клиента.

- *vlan-id* – идентификатор VLAN.
- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port-channel.

Состояние по умолчанию:

Статические привязки не определены.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Запись, добавленная этой командой, может переопределить существующую запись.

Пример:

```
console(config)# ip source-guard binding 0060.704C.73FF 23  
172.17.18.21 gil/0/1
```

7.13. Команда ip source-guard tcam retries-freq

Команда предназначена для установки частоты повторных попыток опроса TCAM, с целью выявления неактивных IP-адресов источников. Использование префикса «по» устанавливает значения по умолчанию.

Синтаксис:

ip source-guard tcam retries-freq { *seconds* | **never** }

no ip source-guard tcam retries-freq

Параметры:

- *seconds* – частота повтора в секундах, диапазон: 10 – 600;
- **never** – отключает автоматический поиск ресурсов в TCAM.

Состояние по умолчанию:

Интервал опроса по умолчанию: 60 с.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Так как механизм IP Source Guard использует ресурсы TCAM, могут возникнуть ситуации, когда некоторые IP-адреса неактивны по причине нехватки ресурсов TCAM.
2. По умолчанию, каждые 60 сек программа проводит поиск доступного пространства в TCAM для неактивных адресов. Данная команда используется для изменения частоты поиска или полного отключения автоматического сканирования TCAM.
3. Команда **ip source-guard tcam locate** служит для ручного сканирования ресурсов TCAM.

4. Команда **show ip source-guard inactive** отображает неактивные IP-адреса источников.

Пример:

```
console(config)# ip source-guard tcam retries-freq 120
```

7.14. Команда ip source-guard tcam locate

Команда **ip source-guard tcam locate** предназначена для ручного поиска ресурсов TCAM, для неактивных IP-адресов Source Guard.

Синтаксис:

ip source-guard tcam locate

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Так как механизм IP Source Guard использует ресурсы TCAM, могут возникнуть ситуации, когда некоторые IP-адреса неактивны по причине нехватки ресурсов TCAM.
2. По умолчанию, каждые 60 сек программа проводит поиск доступного пространства в TCAM для неактивных адресов.
3. Для отключения автоматического сканирования ресурсов TCAM необходимо выполнить команду **ip source-guard retries-freq** с параметром **never**. После этого можно выполнить данную команду для ручного поиска ресурсов.
4. Команда **show ip source-guard inactive** отображает неактивные IP-адреса источников.

Пример:

```
console# ip source-guard tcam locate
```

7.15. Команда show ip source-guard configuration

Команда предназначена для отображения на экране конфигурации IP Source Guard, для всех интерфейсов или только заданного.

Синтаксис:

show ip source-guard configuration [interface-id]

Параметры:

- *interface-id* – идентификатор интерфейса. Доступные типы: Ethernet, Port-channel.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip source-guard configuration
IP Source Guard is Enabled

Interface      State
-----
tel/0/2        Enabled
```

7.16. Команда show ip source-guard status

Команда **show ip source-guard status** предназначена для вывода на экран статуса IP Source Guard.

Синтаксис:

show ip source-guard status [*mac-address mac-address*] [*ip-address ip-address*] [*vlan vlan*] [*interface-id*]

Параметры:

- *mac-address* – аппаратный адрес клиента;
- *ip-address* – IP-адрес клиента;
- *vlan-id* – идентификатор VLAN;
- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port-channel.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip source-guard status
IP Source Guard: Enabled

Interface  Filter  Status  IP address  MAC address  VLAN  Type
-----
tel/0/2    IP      inactive
tel/0/1    IP      active   172.16.0.32  0060.704C.7BC3  4     DHCP
```

7.17. Команда show ip source-guard inactive

Команда **show ip source-guard inactive** предназначена для отображения на экране неактивных IP-адресов Source Guard.

Синтаксис:

show ip source-guard inactive

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Так как механизм IP Source Guard использует ресурсы TCAM, могут возникнуть ситуации, когда некоторые IP-адреса неактивны по причине нехватки ресурсов TCAM.
2. По умолчанию, каждые 60 сек программа проводит поиск доступного пространства в TCAM для неактивных адресов.
3. Команда **ip source-guard tcam retries-freq** применяется для изменения частоты опроса или запрета на автоматический опрос TCAM для поиска неактивных ресурсов.
4. Команда **ip source-guard tcam locate** применяется для ручного сканирования TCAM.

Пример:

```
console# show ip source-guard inactive
TCAM resources search frequency: 2 minutes

Interface Filter  IP address      MAC address     VLAN  Type  Reason
-----
tel1/0/2    IP      172.16.0.32    0060.704C.7BC3  4     DHCP  Resource
problem
```

7.18. Команда show ip source-guard statistics

Команда **show ip source-guard statistics** предназначена для отображения на экране динамической информации Source Guard (разрешенные устройства).

Синтаксис:

show ip source-guard statistics [vlan *vlan-id*]

Параметры:

- *vlan-id* – идентификатор VLAN, для которого выводится статистика.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip source-guard statistics

Vlan  statically permitted stations  DHCP Snooping permitted
stations
-----
```


1	0	2
23	1	0

7.19. Команда ip arp inspection

Команда **ip arp inspection** предназначена для глобального включения использования функции проверки протокола ARP. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip arp inspection

no ip arp inspection

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Функция проверки ARP отключена.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Если порт находится в режиме не доверенного порта, на нем также должен быть настроен DHCP Snooping или привязка IP-адрес – MAC-адрес должна быть настроена статически. В противном случае, устройства подключенные к этому порту не смогут отвечать на ARP.

Пример:

```
console(config)# ip arp inspection
```

7.20. Команда ip arp inspection vlan

Команда **ip arp inspection vlan** предназначена для включения проверки ARP в VLAN на основе базы данных DHCP Snooping. Использование префикса «**no**» отключает проверку.

Синтаксис:

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan *vlan-id*

Параметры:

vlan-id – идентификатор VLAN.

Состояние по умолчанию:

Проверка ARP в VLAN отключена.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Для включения проверки статических ARP-записей используется команда **ip arp inspection list assign**.

Пример:

```
console(config)# ip arp inspection vlan 23
```

7.21. Команда ip arp inspection trust

Команда **ip arp inspection trust** предназначена для перевода состояния интерфейса в доверенный, которое определяет проверяются ли входящие ARP пакеты. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip arp inspection trust

no ip arp inspection trust

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port-channel)

Примечания:

1. После применения данной команды, коммутатор не проверят ARP пакеты полученные на доверенном интерфейсе, а только пересылает их.
2. Для недоверенных интерфейсов, коммутатор перехватывает все ARP запросы и ответы. Он проверяет, что полученные пакеты соответствуют привязке IP-МАС-адресов перед обновлением локального кэша и дальнейшей пересылкой пакета получателю. Устройство отбрасывает недействительные пакеты и делает запись в системный журнал, в соответствии с конфигурацией ведения журнала, указанной в команде **ip arp inspection logging interval**.

Пример:

```
console(config)# interface gil/0/20  
console(config-if)# ip arp inspection trust
```

7.22. Команда ip arp inspection validate

Команда **ip arp inspection validate** предназначена для выполнения специальных проверок динамических ARP запросов. Использование префикса «**no**» отключает данную функцию.

Синтаксис:

ip arp inspection validate

no ip arp inspection validate

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Проверка отключена.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Выполняются следующие проверки:

- Source MAC address – сравнивается MAC-адрес источника в заголовке Ethernet пакета с MAC-адресом в теле ARP пакета. Данная проверка производится как по ARP-запросам, так и по ответам;
- Destination MAC address – сравнивается MAC-адрес получателя в заголовке Ethernet пакета с MAC-адресом в теле ARP пакета. Данная проверка производится как по ARP-запросам, так и по ответам;
- IP address – сравнивает тело ARP пакета с неверными и непредвиденными IP-адресами. Это адреса, которые включают в себя 0.0.0.0, 255.255.255.255 и все IP адреса многоадресной рассылки.

Пример:

```
console(config)# ip arp inspection validate
```

7.23. Команда ip arp inspection list create

Команда предназначена для создания листа статических ARP-записей и перехода в режим конфигурации списка ARP. Использование префикса «**no**» удаляет список.

Синтаксис:

ip arp inspection list create *name*

no ip arp inspection list create *name*

Параметры:

- *name* – наименование списка. Длина: 1 – 32 символа.

Состояние по умолчанию:

Списки ARP-записей не определены.

Режим ИКС:

Режим глобальной конфигурации

Примечание. Для назначения созданного списка на VLAN используется команда **ip arp inspection assign**.

Пример:

```
console(config)# ip arp inspection list create servers
console(config-arp-list)#
```

7.24. Команда `ip mac`

Команда **ip mac** предназначена для создания статической записи привязки ARP. Использование префикса «**no**» удаляет запись.

Синтаксис:

ip *ip-address* **mac** *mac-address*

no ip *ip-address* **mac** *mac-address*

Параметры:

- *ip-address* – IP-адрес.
- *mac-address* – MAC-адрес

Состояние по умолчанию:

Записи отсутствуют.

Режим ИКС:

Режим конфигурации списка ARP

Пример:

```
console(config)# ip arp inspection list create servers
console(config-arp-list)# ip 172.16.1.2 mac 0060.704C.7322
```

7.25. Команда `ip arp inspection list assign`

Команда **ip arp inspection list assign** предназначена для назначения листа статических привязок ARP на VLAN. Использование префикса «**no**» удаляет назначение.

Синтаксис:

ip arp inspection list assign *vlan-id* *name*

no ip arp inspection list assign *vlan-id*

Параметры:

- *vlan-id* – идентификатор VLAN;
- *name* – имя листа.

Состояние по умолчанию:

Привязка листа отсутствует.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip arp inspection list assign 111 servers
```

7.26. Команда ip arp inspection logging interval

Команда **ip arp inspection logging interval** предназначена для установки минимального интервала между отправкой последовательных сообщений ARP SYSLOG. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip arp inspection logging interval { *seconds* | **infinite** }

no ip arp inspection logging interval

Параметры:

- *seconds* – интервал в секундах. Значение 0 означает что сообщение генерируется немедленно. Диапазон: 0 – 86400;
- **infinite** – генерация сообщений отключена.

Состояние по умолчанию:

Интервал между отправкой составляет 5 с.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip arp inspection logging interval 120
```

7.27. Команда show ip arp inspection

Команда **show ip arp inspection** предназначена для вывода на экран конфигурации проверки ARP для всех интерфейсов или только для заданного.

Синтаксис:

show ip arp inspection [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet или Port-channel.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip arp inspection  
IP ARP inspection is Enabled
```

```
IP ARP inspection is configured on following VLANs: 23
Verification of packet header is Enabled
IP ARP inspection logging interval is: 120 seconds

Interface      Trusted
-----
gil/0/20      Yes
```

7.28. Команда show ip arp inspection list

Команда **show ip arp inspection list** предназначена для вывода на экран статических ARP списков.

Синтаксис:

show ip arp inspection list

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip arp inspection list
List name: servers
Assigned to VLANs:

      IP                MAC
-----
172.16.1.2            00:60:70:4c:73:22
```

7.29. Команда show ip arp inspection statistics

Команда **show ip arp inspection statistics** предназначена для вывода на экран статистики, которые были обработаны этой функцией, по следующим типам: Forwarded, Dropped, IP/MAC Vali-dation Failure.

Синтаксис:

show ip arp inspection statistics [vlan *vlan-id*]

Параметры:

- *vlan-id* – идентификатор VLAN.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Для сброса счетчика используется команда **clear ip arp inspection statistics**. При отключении функции проверки ARP значения счетчиков сохраняются.

Пример:

```
console# show ip arp inspection statistics
```

Vlan	Forwarded Packets	Dropped Packets	IP/MAC Failures
23	1500100	121	0

7.30. Команда clear ip arp inspection statistics

Команда **clear ip arp inspection statistics** предназначена для сброса счетчика статистики проверки ARP.

Синтаксис:

clear ip arp inspection statistics [vlan *vlan-id*]

Параметры:

- *vlan-id* – идентификатор VLAN.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear ip arp inspection statistics
```

8. КОМАНДЫ СЕРВЕРА DHCP

8.1. Команда address (DHCP Host)

Команда **address** (DHCP Host) предназначена для создания статической привязки IP-адреса к DHCP-клиенту. Использование префикса «**no**» удаляет привязку.

Синтаксис:

address *ip-address* { *mask* | *prefix-length* } { **client-identifier** *unique-identifier* | **hardware-address** *mac-address* }

no address

Параметры:

- *ip-address* – IP-адрес выдаваемый клиенту;
- *mask* – маска сети;
- *prefix-length* – количество бит, которые содержатся в префиксе адреса. Указывается через косую черту (/);
- *unique-identifier* – особый идентификатор клиента в шестнадцатеричной форме. Каждый байт в шестнадцатеричной строке символов содержит две шестнадцатеричные цифры. Например: **01b7.0813.8811.66**;
- *mac-address* – MAC-адрес клиента.

Состояние по умолчанию:

Статических привязок нет.

Режим ИКС:

Режим конфигурации хостового пула DHCP

Примечание:

Для идентификации клиент DHCP-сервер использует либо идентификатор клиента, переданный в Option 61, при указании параметра **hardware-address**, либо MAC-адрес клиента.

Пример:

```
console(config)# ip dhcp pool host one
console(config-dhcp)# address 10.10.10.99 /24 client-id
01b7.0813.8811.66
console(config-dhcp)# exit
console(config)# ip dhcp pool host two
console(config-dhcp)# address 10.10.10.101 /24 hardware-add
d0:50:99:97:17:2d
```


8.2. Команда `address` (DHCP Network)

Команда **address** (DHCP Network) предназначена для указания подсети и маски подсети DHCP-пуле адресов. Использование префикса «**no**» удаляет подсеть из пула.

Синтаксис:

address { *network-number* | **low** *low-address* **high** *high-address* } { *mask* | *prefix-length* }

no address

Параметры:

- *network-number* – указывает IP-подсеть;
- *mask* – маска заданной подсети;
- *prefix-length* – префикс заданной подсети (указывается как альтернатива маски подсети);
- *low-address* – младший IP-адрес заданного диапазона подсети;
- *high-address* – старший IP-адрес заданного диапазона подсети.

Состояние по умолчанию:

DHCP-пул адресов не задан.

Если *low-address* не указан, по умолчанию используется первый адрес заданной подсети.

Если *high-address* не указан, по умолчанию используется последний адрес подсети.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Пример:

```
console(config)# ip dhcp pool network 23
console(config-dhcp)# address 172.16.100.0 /24
```

8.3. Команда `bootfile`

Команда **bootfile** предназначена для указания файла загрузочного образа для DHCP клиента, по умолчанию. Использование префикса «**no**» удаляет запись о файле.

Синтаксис:

bootfile *filename*

no bootfile

Параметры:

- *filename* – имя файла загрузочного образа. Длина: 1 – 128 символов.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Пример:

```
console(config-dhcp)# bootfile boot_image_file
```

8.4. Команда clear ip dhcp binding

Команда **clear ip dhcp binding** предназначена для удаления динамических привязок из базы данных DHCP-сервера.

Синтаксис:

clear ip dhcp binding { *address* | * }

Параметры:

- *address* – удаляет запись с соответствующим IP-адресом.
- * - удаляет все динамические привязки.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Указанный IP-адрес обозначает адрес клиента. При указании звездочки (*) удаляются все динамические привязки.

Пример:

```
console# clear ip dhcp binding *
```

8.5. Команда client-name

Команда **client-name** предназначена для указания имени DHCP-клиента. Использование префикса «no» удаляет запись.

Синтаксис:

client-name *name*

no client-name

Параметры:

- *name* – имя клиента, используются стандартные ASCII символы. Имя клиента не включает в себя доменное имя. Например имя mars не должно указываться как mars.yahoo.com. Длина: 1 – 32 символа.

Состояние по умолчанию:

Имя клиента не задано.

Режим ИКС:

Режим конфигурации хостового пула DHCP

Пример:

```
console(config-dhcp)# client-name Client1
```

8.6. Команда default-router

Команда **default-router** предназначена для задания маршрутизатора по умолчанию для DHCP-клиентов. Использование префикса «**no**» удаляет маршрутизатор.

Синтаксис:

default-router *ip-address* [*ip-address2* ... *ip-address8*]

no default-router

Параметры:

- *ip-address* [*ip-address2* ... *ip-address8*] – задает IP-адрес (адреса) маршрутизаторов по умолчанию. Существует возможность задать до 8 маршрутизаторов в одной команде.

Состояние по умолчанию:

Маршрутизаторы не заданы.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Примечания:

1. IP-адрес маршрутизатора должен находиться в той же подсети, что и клиентская подсеть.
2. DHCP-сервер возвращает IP-адрес заданный на входящем интерфейсе в качестве маршрутизатора по умолчанию, если маршрутизатор не указан в следующих случаях:
 - маршрутизатор по умолчанию не указан;
 - DHCP-клиент подключен напрямую;
 - включена служба IP-routing;
 - маршрутизатор был запрошен самим клиентом.

Пример:

```
console(config-dhcp)# default-router 172.16.10.1
```

8.7. Команда dns-server

Команда предназначена для задания списка DNS-серверов для DHCP-клиентов. Использование префикса «**no**» удаляет список.

Синтаксис:

dns-server *ip-address* [*ip-address2* ... *ip-address8*]

no dns-server

Параметры:

- *ip-address* [*ip-address2* ... *ip-address8*] – задает IP-адрес (адреса) DNS серверов. Существует возможность задать до 8 маршрутизаторов в одной команде.

Состояние по умолчанию:

DNS сервера не заданы.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Примечание:

Если DNS-серверы не заданы для DHCP-клиентов, то клиенты не могут производить сопоставление имен узлов с IP-адресами.

Пример:

```
console(config-dhcp)# dns-server 172.16.100.25
```

8.8. Команда domain-name

Команда **domain-name** предназначена для задания доменного имени используемого DHCP клиентами. Использование префикса «**no**» удаляет доменное имя.

Синтаксис:

domain-name *domain*

no domain-name

Параметры:

- *domain* – доменное имя. Длина: 1 – 32 символа.

Состояние по умолчанию:

Доменное имя не задано.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Пример:

```
console(config-dhcp)# domain-name yahoo.com
```

8.9. Команда `ip dhcp excluded-address`

Команда **`ip dhcp excluded-address`** предназначена для указания диапазона адресов, которые не предназначены для выдачи DHCP-клиентам. Использование префикса «**no**» удаляет диапазон.

Синтаксис:

`ip dhcp excluded-address` *low-address* [*high-address*]

`no ip dhcp excluded-address` *low-address* [*high-address*]

Параметры:

- *low-address* – младший адрес из диапазона;
- *high-address* – старший адрес из диапазона.

Состояние по умолчанию:

По умолчанию назначаются все адреса диапазона.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

DHCP-сервер предполагает, что из выделенного диапазона могут быть назначены все адреса. Данная команда используется для исключения из диапазона одного или нескольких адресов.

Пример:

```
console(config)# ip dhcp excluded-address 172.20.20.1 172.20.20.50
```

8.10. Команда `ip dhcp pool host`

Команда **`ip dhcp pool host`** предназначена для настройки статического адреса DHCP на DHCP-сервере и перехода в режим конфигурации хостового DHCP-пула. Использование префикса «**no**» удаляет пул адресов.

Синтаксис:

`ip dhcp pool host` *name*

`no ip dhcp pool host` *name*

Параметры:

- *name* – имя адресного пула. Может включать буквы и цифры. Длина: 1 – 32 символа.

Состояние по умолчанию:

DHCP пул для узлов не задан.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

После выполнения данной команды режим конфигурации переключается в режим конфигурации хостового пула DHCP. В этом режиме становятся доступны функции настройки параметров узла, такие как номер подсети и список маршрутов по умолчанию.

Пример:

```
console(config)# ip dhcp pool host Two
console(config-dhcp)#
```

8.11. Команда ip dhcp pool network

Команда **ip dhcp pool network** предназначена для создания адресного пула DHCP на DHCP сервере и перехода в режим его настройки. Использование префикса «**no**» удаляет адресный пул.

Синтаксис:

ip dhcp pool network *name*

no ip dhcp pool network *name*

Параметры:

- *name* – имя адресного пула. Может включать буквы и цифры. Длина: 1 – 32 символа.

Состояние по умолчанию:

Адресный пул DHCP не задан.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

После выполнения данной команды режим конфигурации переключается в режим конфигурации сетевого пула DHCP. В этом режиме становятся доступны функции настройки параметров пула, такие как номер подсети и список маршрутов по умолчанию.

Пример:

```
console(config)# ip dhcp pool network Thief
console(config-dhcp)#
```

8.12. Команда ip dhcp server

Команда **ip dhcp server** предназначена для включения функции DHCP-сервера на коммутаторе. Использование префикса «**no**» отключает сервер.

Синтаксис:

ip dhcp server

no ip dhcp server

Состояние по умолчанию:

DHCP сервер отключен.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip dhcp server
```

8.13. Команда lease

Команда **lease** предназначена для изменения параметров аренды IP-адреса для DHCP клиента. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lease *days* [*hours* [*minutes*]] | **infinite**

no lease

Параметры:

- *days* – количество дней аренды;
- *hours* – (Дополнительно). Количество часов аренды. Перед указанием значения необходимо предварительно указать значение *days*;
- *minutes* – (Дополнительно). Количество минут аренды. Перед указанием значения необходимо предварительно указать значение *days* и *hours*;
- **infinite** – срок аренды не ограничен.

Состояние по умолчанию:

По умолчанию срок аренды составляет 1 день.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Пример:

```
console(config-dhcp)# lease 10 12 30
```

8.14. Команда netbios-name-server

Команда **netbios-name-server** предназначена для указания списка NetBIOS WINS (Windows Internet Naming Service) серверов, доступных для Microsoft DHCP-клиентов. Использование префикса «**no**» удаляет список.

Синтаксис:

netbios-name-server *ip-address* [*ip-address2* ... *ip-address8*]

no netbios-name-server

Параметры:

- *ip-address* [*ip-address2* ... *ip-address8*] – IP-адреса WINS серверов. В одной команде может быть задано до 8 серверов.

Состояние по умолчанию:

Сервера не заданы.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Пример:

```
console(config-dhcp)# netbios-name-server 172.20.0.5
```

8.15. Команда netbios-node-type

Команда **netbios-node-type** предназначена для установки типа узла NetBIOS для Microsoft DHCP клиентов. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

netbios-node-type { **b-node** | **p-node** | **m-node** | **h-node** }

no netbios-node-type

Параметры:

- **b-node** – широковещательный тип NetBIOS узла;
- **p-node** – пиринговый (peer-to-peer) тип NetBIOS узла;
- **m-node** – смешанный тип NetBIOS узла;
- **h-node** – гибридный тип NetBIOS узла.

Состояние по умолчанию:

Тип узла NetBIOS – **h-node** (гибридный)

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Пример:

```
console(config-dhcp)# netbios-node-type p-node
```


8.16. Команда next-server

Команда **next-server** предназначена для указания следующего сервера (siaddr) используемого в процессе сетевой загрузки DHCP-клиента. К данному серверу клиент будет подключаться по протоколам SCP/TFTP, для скачивания загрузочного файла (bootfile). Использование префикса «no» удаляет сервер из конфигурации.

Синтаксис:

next-server *ip-address*

no next-server

Параметры:

- *ip-address* – адрес сервера сетевой загрузки.

Состояние по умолчанию:

Если данная команда не используется для настройки списка серверов загрузки, сервер DHCP использует входящий вспомогательный (helper) интерфейс в качестве загрузочных серверов.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Пример:

```
console(config-dhcp)# next-server 172.20.0.8
```

8.17. Команда next-server-name

Команда **next-server-name** предназначена для задания имени (sname) сервера загрузки. Использование префикса «no» удаляет имя сервера.

Синтаксис:

next-server-name *name*

no next-server-name

Параметры:

- *name* – имя сервера загрузки. Длина: 1 – 64 символа.

Состояние по умолчанию:

Имя сервера не задано.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Пример:

```
console(config-dhcp) # next-server-name www.name.com
```

8.18. Команда option

Команда **option** предназначена для указания опций DHCP сервера. Использование префикса «**no**» удаляет опции.

Синтаксис:

```
option code { boolean { false | true } | integer value | ascii string | hex { string | none } | ip  
address | ip-list { ip-address1 [ ip-address2 ... ] } } [ description text ]
```

no option code

Параметры:

- *code* – код DHCP опции (поддерживаемые значения указаны в примечании);
- **boolean** { **false** | **true** } – определяет логическое значение (указываются целые значения: 0 = false, 1 = true);
- **integer** – целочисленное значение. Размер зависит от кода опции;
- **ascii** – строка символов виртуального терминала (NVT). Символьные строки содержащие пробелы должны быть взяты в кавычки. Длина строки усекается до первых 160 символов;
- *ip-address* – указывает IP-адрес;
- **ip-list** – список IP-адресов (до 8);
- **hex** – шестнадцатеричная строка. Значение усекается до первых 320 введенных символов. Каждый байт имеет две шестнадцатеричных цифры. Байты отделяются друг от друга точкой, двоеточием или пробелом;
- **description** – описание пользователя.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Примечания:

1. Команда позволяет определить любую опцию, которая не может быть определена другими командами ИКС. Новое определение опции переопределяет предыдущее значение параметра.
2. Параметр **boolean** используется для задания следующих опций: 19, 20, 27, 29-31, 34, 36 и 39.
3. Параметр **integer** используется для задания следующих опций: 2, 13, 22-26, 35, 37-38, 132-134 и 211. Коммутатор проверяет диапазон значений и устанавливает размер поля значения в соответствии с определением опций.
4. Параметр **ascii** используется для задания следующих опций: 14, 17-18, 40, 64, 130, 209 и 210.

5. Параметр **ip address** используется для задания следующих опций: 16, 28, 32, 128-129, 131, 135 и 136.
6. Параметр **ip-list** используется для задания следующих опций: 5, 7-11, 33, 41, 42, 45, 48, 49, 65, 68-76 и 150.
7. Параметр **hex** может быть использован для любой опции в диапазоне 1 – 254, за исключением следующих: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82 и 255. Коммутатор не проверяет синтаксис параметра, определяемого этим форматом.

Пример:

```
console(config-dhcp)# option 2 integer 3600
console(config-dhcp)# option 19 boolean true description "IP
Forwarding Enable"
```

8.19. Команда show ip dhcp

Команда **show ip dhcp** предназначена для отображения на экране конфигурации DHCP.

Синтаксис:

show ip dhcp

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp
DHCP server is enabled.
```

8.20. Команда show ip dhcp allocated

Команда **show ip dhcp allocated** предназначена для отображения на экране назначенных DHCP-сервером IP-адресов.

Синтаксис:

show ip dhcp allocated [ip-address]

Параметры:

- *ip-address* – заданный IP-адрес (дополнительно).

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp allocated
DHCP server enabled.
The number of allocated entries is 0

IP address      Hardware address  Lease expiration  Type
```

172.16.1.11	00a0.9802.32de	Feb 01 2018 12:00 AM	Dynamic
172.16.3.253	02c7.f800.0422	Infinite	
Automatic			
172.16.3.254	02c7.f800.0310	Infinite	Static

Значения полей:

Поле	Описание
IP address	IP-адрес хоста, записанный на DHCP-сервере.
Hardware address	MAC-адрес или идентификатор клиента, записанный на DHCP-сервере.
Lease expiration	Дата истечения срока аренды IP-адреса.
Type	Способ при помощи которого IP-адрес был назначен хосту.

8.21. Команда show ip dhcp binding

Команда **show ip dhcp binding** предназначена для отображения на экране конкретной привязки или всех привязок IP-адресов на DHCP-сервере.

Синтаксис:

show ip dhcp binding [*ip-address*]

Параметры:

- *ip-address* – Заданный IP-адрес (дополнительно).

Режим ИКС:

Привилегированный режим управления.

Пример:

```

console# show ip dhcp binding
DHCP server enabled.
The number of used (all types) entries is 6
The number of preallocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1

IP address  Client Identifier  Lease expiration  Type  State
-----
172.16.1.11  00a0.9802.32de  Feb 01 1998 12:00AM  dynamic
allocated
172.16.3.23  02c7.f801.0422  dynamic  expired
172.16.3.24  02c7.f802.0422  dynamic
declined

```

172.16.3.25	02c7.f803.0422	dynamic pre-allocated
172.16.3.26	02c7.f804.0422	dynamic declined

Значения полей:

Поле	Описание
IP address	IP-адрес хоста, записанный на DHCP-сервере.
Client Identifier	MAC-адрес или идентификатор клиента, записанный на DHCP-сервере.
Lease expiration	Дата истечения срока аренды IP-адреса.
Type	Способ при помощи которого IP-адрес был назначен хосту.
State	Статус IP-адреса

8.22. Команда show ip dhcp declined

Команда **show ip dhcp declined** предназначена для отображения на экране сведений об IP адресах, которым отказано в аренде.

Синтаксис:

show ip dhcp declined [ip-address]

Параметры:

- **ip-address** – (Дополнительно) Заданный IP-адрес.

Режим ИКС:

Привилегированный режим управления.

Пример:

```

console# show ip dhcp declined
DHCP server enabled.
The number of declined entries is 2

  IP address      Hardware address
  -----
172.16.1.11      00a0.9802.32de
172.16.3.254     02c7.f800.0422
    
```

8.23. Команда show ip dhcp excluded-addresses

Команда **show ip dhcp excluded-addresses** предназначена для отображения на экране IP адресов исключенных из адресного DHCP-пула.

Синтаксис:

show ip dhcp excluded-addresses

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp excluded-addresses
The number of excluded addresses ranges is 1
Excluded addresses:
172.20.20.1 - 172.20.20.50
```

8.24. Команда show ip dhcp expired

Команда предназначена для отображения на экране информации о IP-адресах с истекшим сроком аренды.

Синтаксис:

show ip dhcp expired [*ip-address*]

Параметры:

- *ip-address* – Заданный IP-адрес (дополнительно).

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp expired
DHCP server enabled.
The number of expired entries is 1

  IP address      Hardware address
  -----
172.16.1.11      00a0.9802.32de
```

8.25. Команда show ip dhcp pool host

Команда **show ip dhcp pool host** предназначена для отображения конфигурации хостового DHCP пула.

Синтаксис:

show ip dhcp pool host [{ *address* | *name* }]

Параметры:

- *address* – (дополнительно) IP-адрес клиента;
- *name* – (дополнительно) имя DHCP пула.

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1.

```
console# show ip dhcp pool host
The number of host pools is 1
Name          IP Address Hardware Address Client Identifier
-----
station       172.16.1.11                               01b7.0813.8811.66
```

Пример 2.

```
console# show ip dhcp pool host station
Name          IP Address Hardware Address Client Identifier
-----
station       172.16.1.11                               01b7.0813.8811.66
Mask: 255.255.0.0
Default router: 172.16.1.1
Client name: client1
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:
Code  Type  Len  Value          Description
-----
--
 2  integer  4   3600
14  ascii   16  qq/aaaa/bbb.txt
19  boolean  1   false          "IP Forwarding Enable/Disable
Option"
21  ip       4   134.14.14.1
31  ip-list  8   1.1.1.1, 12.23.45.2
47  hex      5   02af00aa00
```

8.26. Команда show ip dhcp pool network

Команда **show ip dhcp pool network** предназначена для отображения конфигурации сетевого DHCP пула.

Синтаксис:

show ip dhcp pool network [name]

Параметры:

- *name* – имя DHCP пула.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp pool network
The number of network pools is 1

      Name                Address range           Mask
-----
Lease
-----
      One                172.20.20.1-172.20.20.254  255.255.255.0
1d:0h:0m
```

8.27. Команда show ip dhcp pre-allocated

Команда **show ip dhcp pre-allocated** предназначена для отображения предварительно выделенных адресов DHCP пула.

Синтаксис:

show ip dhcp pre-allocated [*ip-address*]

Параметры:

- *ip-address* – предварительно выданный IP-адрес.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp pre-allocated
DHCP server enabled.
The number of preallocated entries is 2

      IP address           Hardware address
-----
172.16.1.11              00a0.9802.32de
172.16.3.254            02c7.f800.0422
```

8.28. Команда show ip dhcp server statistics

Команда **show ip dhcp server statistics** предназначена для отображения статистики сервера DHCP.

Синтаксис:

show ip dhcp server statistics

Режим ИКС:

Привилегированный режим управления.

Пример:


```
console# show ip dhcp server statistics
The number of network pools is 7
The number of excluded pools is 2
The number of used (all types) entries is 7
The number of preallocated entries is 1
The number of allocated entries is 3
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
```

8.29. Команда time-server

Команда **time-server** предназначена для указания сервера времени для DHCP-клиентов. Использование префикса «**no**» удаляет список серверов.

Синтаксис:

time-server *ip-address* [*ip-address2 ... ip-address8*]

no time-server

Параметры:

- *ip-address* [*ip-address2 ... ip-address8*] – IP-адрес сервера времени. Возможно указать до 8 серверов.

Состояние по умолчанию:

Сервера времени не определены.

Режим ИКС:

Режим конфигурации сетевого пула DHCP

Режим конфигурации хостового пула DHCP

Примечание:

IP-адрес сервера времени должен находиться в той же подсети, что и клиентская подсеть.

Пример:

```
console(config-dhcp)# time-server 172.20.20.100
```

8.30. Команда ip dhcp ping enable

Команда **ip dhcp ping enable** режима общей настройки, разрешает отправку DHCP-серверу ping-пакетов перед назначением запрашиваемого клиентом адреса. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip dhcp ping enable

no ip dhcp ping enable

Состояние по умолчанию:

Пинг выключен.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

DHCP-сервер пингует запрашиваемый клиентом адрес. Если ответ не получен, DHCP-сервер предполагает, что адрес не используется и назначает его клиенту.

Пример:

```
console(config)# ip dhcp ping enable
```

8.31. Команда ip dhcp ping count

Команда **ip dhcp ping count** режима общей настройки, задает количество пинг пакетов, отправляемых DHCP-сервером на адреса пула. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip dhcp ping count *number*

no ip dhcp ping count

Параметры:

- *number* - количество пакетов (диапазон: 1 - 10).

Состояние по умолчанию:

По умолчанию DHCP сервер посылает 2 пакета.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip dhcp ping count 10
```

8.32. Команда ip dhcp ping timeout

Команда **ip dhcp ping timeout** режима общей настройки, задает временной интервал, в течение которого DHCP-сервер ожидает ответа на пинг со стороны пула адресов. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip dhcp ping timeout *milliseconds*

no ip dhcp ping timeout

Параметры:

- *milliseconds* - время отклика, в миллисекундах. Диапазон: 300 - 10000.

Состояние по умолчанию:

По умолчанию время ответа 500 миллисекунд.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Команда определяет временной диапазон, в течение которого DHCP-сервер ожидает ответа на пинг, после чего прекращает попытки пинговать адрес.

Пример:

```
console(config)# ip dhcp ping timeout 1000
```

8.33. Команда ping enable

Команда ping enable режима настройки пула DHCP разрешает отправку DHCP-серверу ping-пакетов перед назначением запрашиваемого клиентом адреса. Использование префикса «no» отключает функцию.

Синтаксис:

ping enable

no ping enable

Состояние по умолчанию:

По умолчанию разрешено.

Режим ИКС:

Режим конфигурации сетевого пула DHCP.

Примечание:

DHCP-сервер пингует запрашиваемый клиентом адрес. Если ответ не получен, DHCP-сервер предполагает, что адрес не используется и назначает его клиенту.

Пример:

```
console(config-dhcp)# ping enable
```

9. КОМАНДЫ ПОСРЕДНИКА DHCP

9.1. Команда ip dhcp relay enable (Global)

Команда **ip dhcp relay enable** (Global) предназначена для включения режима посредника DHCP на коммутаторе. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip dhcp relay enable

no ip dhcp relay enable

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip dhcp relay enable
```

9.2. Команда ip dhcp relay enable (Interface)

Команда **ip dhcp relay enable** (Interface) предназначена для включения режима посредника DHCP на интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip dhcp relay enable

no ip dhcp relay enable

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим конфигурации интерфейса

Примечание:

Функция будет активна на интерфейсе, если выполнено одно из условий:

- DHCP посредник включен на коммутаторе глобально и на интерфейсе назначен IP-адрес;
- DHCP посредник включен на коммутаторе глобально, на интерфейсе IP-адрес не назначен и разрешена DHCP опция 82.

Пример:

```
console(config)# interface vlan 100  
console(config-if)# ip dhcp relay enable
```

9.3. Команда ip dhcp relay address (Global)

Команда **ip dhcp relay address** (Global) предназначена для задания IP-адреса сервера DHCP для настройки посредника. Использование префикса «**no**» удаляет запись.

Синтаксис:

ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

Параметры:

- *ip-address* – IP-адрес DHCP сервера. Возможно задание до 8 серверов.

Состояние по умолчанию:

Сервера не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Для указания нескольких серверов, команда применяется несколько раз с разными IP адресами.
2. Для удаления конкретного сервера используется команда с указанием IP-адреса.
3. Применение команды без указания IP-адреса удаляет все записи о DHCP-серверах.

Пример:

```
console(config)# ip dhcp relay address 172.20.0.3
```

9.4. Команда ip dhcp relay address (Interface)

Команда **ip dhcp relay address** (Interface) предназначена для задания IP-адреса сервера DHCP для клиентов DHCP подключенных к интерфейсу. Использование префикса «**no**» удаляет запись.

Синтаксис:

ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

Параметры:

- *ip-address* – IP-адрес DHCP сервера. Возможно задание до 8 серверов.

Состояние по умолчанию:

Сервера не заданы.

Режим ИКС:

Режим конфигурации интерфейса

Примечания:

1. Для указания нескольких серверов, команда применяется несколько раз с разными IP адресами.
2. Для удаления конкретного сервера используется команда с указанием IP-адреса.
3. Применение команды без указания IP-адреса удаляет все записи о DHCP-серверах.

Пример:

```
console(config)# interface vlan 21
console(config-if)# ip dhcp relay address 172.20.0.3
```

9.5. Команда show ip dhcp relay

Команда **show ip dhcp relay** предназначена для отображения информации о DHCP посреднике.

Синтаксис:

show ip dhcp relay

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp relay
DHCP relay is Disabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 256
Number of DHCP Relays enabled on VLANs without IP Address is 1
DHCP relay is not configured on any port.
DHCP relay is enabled on Vlans: 100
Active:
Inactive: 100
Servers: 172.20.0.3
```

9.6. Команда ip dhcp information option

Команда **ip dhcp information option** предназначена для включения опции 82 в данные DHCP. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip dhcp information option

no ip dhcp information option

Состояние по умолчанию:

Добавление опции 82 запрещено.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Функция будет задействована только при включении DHCP snooping или DHCP relay.

Пример:

```
console(config)# ip dhcp information option
```

9.7. Команда show ip dhcp information option

Команда **show ip dhcp information option** предназначена для вывода состояния конфигурации опции 82 DHCP.

Синтаксис:

show ip dhcp information option

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip dhcp information option  
Relay agent Information option is Enabled
```

10. КОМАНДЫ DNS КЛИЕНТА

10.1. Команда clear host

Команда **clear host** предназначена для удаления динамических записей соответствия имени узла и IP-адреса из DNS кэша.

Синтаксис:

clear host { *hostname* | * }

Параметры:

- *hostname* – имя узла в DNS кэше;
- * - удаляются все записи в кэше.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Для удаления динамической записи для одного узла используется параметр **hostname**. При указании в качестве параметра звездочки (*) удаляются все динамические записи.
2. Для создания в кэше статической записи соответствия имени и IP-адреса используется команда **ip host**.
3. Для удаления статической записи из кэша используется команда **no ip host**.

Пример:

```
console# clear host *
```

10.2. Команда ip domain lookup

Команда **ip domain lookup** предназначена для включения использования протокола DNS (Domain Name System). Использование префикса «**no**» отключает функцию.

Синтаксис:

ip domain lookup

no ip domain lookup

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Включено.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip domain lookup
```

10.3. Команда ip domain name

Команда **ip domain name** предназначена для задания имени домена, которое коммутатор использует по умолчанию для завершения невалифицированных имен узлов (имена без имени домена, разделенные точкой). Использование префикса «**no**» удаляет имя.

Синтаксис:

ip domain name *name*

no ip domain name

Параметры:

- *name* – имя домена по умолчанию, используемое для невалифицированных имен узлов. Диапазон: 1 - 158 символов. Максимальная длина части каждого уровня домена составляет 63 символа. Точка, которая отделяет невалифицированное имя от имени домена не используется.

Состояние по умолчанию:

Имя домена не задано.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Любое имя хоста, которое не содержит доменное имя, будет дополнено точкой и именем домена по умолчанию и добавлено в таблицу хостов.
2. Доменные имена и имена хостов ограничены буквами ASCII от A до Z (без учета регистра), цифрами от 0 до 9, подчеркиванием и дефисом. Для разделения частей имени используется точка.
3. Максимальный размер каждой части имени составляет 63 символа. Максимальный размер всего имени – 158 символов.

Пример:

```
console(config)# ip domain name website.com
```

10.4. Команда ip domain pooling-interval

Команда **ip domain pooling-interval** предназначена для задания интервала опроса. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

ip domain pooling-interval seconds

no ip domain pooling-interval

Параметры:

- **seconds** – интервал опроса в секундах. Диапазон: от $2*(R+1)*T$ до 3600.

Состояние по умолчанию:

Значение по умолчанию: $2 * (R+1) * T$,

где:

- R – значение, заданное командой **ip domain retry**;
- T – значение, заданное командой **ip domain timeout**.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Некоторые приложения постоянно взаимодействуют с определенным IP-адресом. DNS-клиенты для таких приложений, которые не получили разноименование IP-адреса или не обнаружили DNS-сервер с использованием фиксированного количества повторных передач возвращают ошибку в приложение и продолжают отправлять DNS-запрос для IP-адреса, используя заданный интервал опроса.

Пример:

```
console(config)# ip domain polling-interval 100
```

10.5. Команда ip domain retry

Команда **ip domain retry** предназначена для задания количества DNS-запросов до получения ответа. Использование префикса **no** устанавливает значение по умолчанию.

Синтаксис:

ip domain retry number

no ip domain retry

Параметры:

- *number* – количество DNS-запросов к DNS-серверу. Диапазон: 0 – 16.

Состояние по умолчанию:

Количество запросов: 1

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Аргумент *number* определяет количество запросов к DNS-серверу, пока коммутатор не решит, что сервера не существует.

Пример:

```
console(config)#ip domain retry 10
```

10.6. Команда ip domain timeout

Команда **ip domain timeout** предназначена для задания времени ожидания на DNS-запрос. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

ip domain timeout *seconds*

no ip domain timeout

Параметры:

- *seconds* – время ожидания ответа на DNS-запрос (в секундах), диапазон: 1 – 60.

Состояние по умолчанию:

Значение по умолчанию: 2 с.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Данная команда служит для изменения значения времени ожидания по умолчанию.

Пример:

```
console(config)# ip domain timeout 30
```

10.7. Команда ip host

Команда **ip host** предназначена для создания статической записи соответствия имени узла и IP-адреса в DNS-кэше. Использование префикса «**no**» удаляет статическую запись.

Синтаксис:

ip host *hostname address [address2 ... address8]*

no ip host *hostname address [address2 ... address8]*

Параметры:

- *hostname* – имя узла. Длина: 1 – 158.
- *address* – ассоциированный с именем IP-адрес (IPv4 или IPv6). На одно имя можно указывать до 8 IP-адресов.

Состояние по умолчанию:

Статические записи не определены.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Имя узла состоит из ASCII символов от A до Z (без учета регистра), цифр от 0 до 9, символов подчеркивания и дефиса. Для разделения частей имени используется точка.
2. Приложение будет получать IP-адреса в следующем порядке:
 - a. IPv6-адреса в порядке перечисления аргументов;
 - b. IPv4-адреса в порядке перечисления аргументов.
3. Использование префикса «**no**» с аргументами [*address ... address8*] удаляет указан-ные адреса из записи. При удалении всех адресов запись будет также удалена. Применение команды без указания адресов удаляет запись.

Пример:

```
console(config)# ip host www.termo.ru 172.18.20.1 172.20.3.1  
172.34.7.1
```

10.8. Команда ip name-server

Команда **ip name-server** предназначена для задания одного или нескольких IP-адресов DNS серверов. Использование префикса «**no**» удаляет запись.

Синтаксис:

ip name-server *server-address1* [*server-address2 ... server-address8*]

no ip name-server [*server-address1 ... server-address8*]

Параметры:

- *server-address* – IPv4 или IPv6 адрес сервера.
- *server-address2 ... server-address8* – IPv4 или IPv6 адреса дополнительных серверов.

Состояние по умолчанию:

DNS сервера не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Предпочтения серверов определяется порядком задания их IP-адресов.
2. Повторный ввод команды заменяет предыдущую конфигурацию.

Пример:

```
console(config)# ip name-server 172.16.100.52 172.18.100.52
```

10.9. Команда show hosts

Команда **show hosts** предназначена для отображения на экране имени домена по умолчанию, тип и имя службы поиска имен, список DNS-серверов и кэшированного списка имени хостов и адресов.

Синтаксис:

show hosts [{ **all** | *hostname* }]

Параметры:

- **all** – отображает информацию о всех настроенных DNS представлениях. Аргумент по умолчанию.
- *hostname* – отображается информация для заданного имени узла.

Режим ИКС:

Привилегированный режим управления.

Состояние по умолчанию:

Используется аргумент **all**.

Пример:

```
console# show hosts

Name/address lookup is enabled
Domain Timeout: 30 seconds
Domain Retry: 10 times
Domain Polling Interval: 660 seconds

Default Domain Table

          Domain                               Source  Interface
Prefer-ence
-----
website.com                               static

Name Server Table

          IP Address                           Source  Interface
Prefer-ence
-----
172.16.100.52                             static      1
172.18.100.52                             static      2

Cache Table
Flags: (STA/DYN, OK/NE/??)
```

STA - Static, DYN - Dynamic				
OK - Okay, NE - Negative Cache, ?? - No Response				
Remain-ing	Host	Addresses	Type	State
TTL				

w		172.20.3.1	IPv4	STA,OK
w		172.34.7.1	IPv4	STA,OK

11. КОМАНДЫ ЗАЩИТЫ ОТ DOS (DENIAL OF SERVICE)

11.1. Команда `security-suite enable`

Команда **`security-suite enable`** предназначена для включения функционала защиты от DoS атак глобально. После выполнения данной команды для защиты задействуются аппаратные ресурсы коммутатора. Использование префикса «**no**» отключает функционал.

Функционал обеспечения безопасности может быть включен двумя способами:

- **`global-rules-only`** – включает только глобальные правила, функционал для интерфейсов отключен.
- **`all`** – весь функционал, включая функционал для интерфейсов, параметр в команде не задается.

После включения функционала безопасности становятся доступными следующие команды:

- **`security-suite dos protect`**
- **`security-suite dos syn-attack`**
- **`security-suite deny martian-addresses`**
- **`security-suite deny syn`**
- **`security-suite deny icmp`**
- **`security-suite deny fragmented`**
- **`show security-suite configuration`**
- **`security-suite dos protect`**

Синтаксис:

`security-suite enable [global-rules-only]`

`no security-suite enable`

Параметры:

- **`global-rules-only`** – все команды функционала применяются глобально, а не для каждого интерфейса в отдельности. Это позволяет сэкономить ресурсы TCAM (троичная ассоциативная память).

Состояние по умолчанию:

Функционал безопасности отключен.

Если параметр **`global-rules-only`** не указан, то команда применяется глобально и к каждому интерфейсу.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. MAC ACL должны быть удалены перед включением функционала. Необходимые правила MAC ACL могут быть введены повторно, после применения команды.
2. Если на интерфейсе назначены ACL или Policy map, то правила функционала не могут быть применены на интерфейсе.

Пример:

```
console(config-if)# security-suite enable global-rules-only
```

11.2. Команда security-suite deny fragmented

Команда **security-suite deny fragmented** предназначена для включения функции отбрасывания фрагментированных IP-пакетов на заданном интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

```
security-suite deny fragmented { add { ip-address | any } { mask | !prefix-length } | remove { ip-address | any } { mask | !prefix-length } }
```

no security-suite deny fragmented

Параметры:

- **add** { *ip-address* | **any** } – добавляет IP-адрес с которого отбрасываются пакеты в список на интерфейсе. Использование any запрещает пакеты со всех адресов;
- *mask* – сетевая маска для указанного IP-адреса;
- *prefix-length* – префикс сети.
- **remove** { *ip-address* | **any** } – удаляет указанный IP-адрес из списка. Использование параметра any отключает функцию на интерфейсе

Состояние по умолчанию:

Фрагментированные IP-пакеты разрешены на всех интерфейсах.

Если параметр **mask** не задан, то по умолчанию принимается 255.255.255.255.

Если параметр **prefix-length** не указан, то по умолчанию принимается /32.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечание:

Данная команда доступна после включения режима **security-suite** глобально.

Пример:

```
console(config)# security-suite enable  
console(config)# interface GigabitEthernet 1/0/10
```



```
console(config-if)# security-suite deny fragmented add 172.20.12.23  
/24
```

11.3. Команда security-suite deny icmp

Команда **security-suite deny icmp** предназначена для включения функции отбрасывания пакетов ICMP echo request на заданном интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

```
security-suite deny icmp { add { ip-address | any } { mask | prefix-length } | remove { ip-address | any } { mask | prefix-length } }
```

no security-suite deny icmp

Параметры:

- **add** { *ip-address* | **any** } – добавляет IP-адрес с которого отбрасываются пакеты в список на интерфейсе. Использование any запрещает пакеты со всех адресов;
- *mask* – сетевая маска для указанного IP-адреса;
- *prefix-length* – префикс сети;
- **remove** { *ip-address* | **any** } – удаляет указанный IP-адрес из списка. Использование параметра any отключает функцию на интерфейсе.

Состояние по умолчанию:

Фрагментированные IP-пакеты разрешены на всех интерфейсах.

Если параметр **mask** не задан, то по умолчанию принимается 255.255.255.255.

Если параметр **prefix-length** не указан, то по умолчанию принимается /32.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

1. Данная команда доступна после включения режима **security-suite** глобально.
2. Команда отбрасывает ICMP-пакеты с “ICMP type = Echo request” входящие на указанный интерфейс.

Пример:

```
console(config)# security-suite enable  
console(config)# interface GigabitEthernet 1/0/10  
console(config-if)# security-suite deny icmp add any
```

11.4. Команда `security-suite deny martian-addresses`

Команда `security-suite deny martian-addresses` предназначена для включения запрета на входящие пакеты содержащие IP-адреса, зарезервированные системой. Использование префикса «**no**» отключает функцию.

Синтаксис:

`security-suite deny martian-addresses { add { ip-address { mask | /prefix-length } } | remove { ip-address { mask | /prefix-length } }` (Добавляет или удаляет пользовательские IP-адреса)

`security-suite deny martian-addresses reserved { add | remove }` (Добавляет или удаляет IP адреса зарезервированные системой)

`no security-suite deny martian-addresses`

Параметры:

- `add { ip-address | any }` – добавляет IP-адрес с которого отбрасываются пакеты в список на интерфейсе. Использование `any` запрещает пакеты со всех адресов;
- `mask` – сетевая маска для указанного IP-адреса;
- `prefix-length` – префикс сети;
- `reserved add/remove` – добавляет/удаляет зарезервированные адреса из списка;
- `remove { ip-address | any }` – удаляет указанный IP-адрес из списка. Использование параметра `any` отключает функцию на интерфейсе;
- `reserved` – отбрасывает пакеты с исходным или целевым IP-адресом из блока зарезервированных (марсианских) адресов. Список зарезервированных IP-адресов см. ниже.

Состояние по умолчанию:

Разрешены все пакеты с зарезервированных (марсианских) адресов.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Данная команда доступна после включения режима `security-suite` глобально.

Зарезервированные системой адреса:

Блок адресов	Назначение
0.0.0.0/8 (исключая 0.0.0.0/32 в качестве адреса источника)	Адреса в этом блоке относятся к исходным узлам "этой" сети.
127.0.0.0/8	Используется в качестве адреса обратной петли.
192.0.2.0/24	Используется в качестве «TEST-NET» в документации, например, в примерах исходных кодов.
224.0.0.0/4 в качестве источника	Блок, ранее известный как сеть класса D, используется для IPv4 многоадресной рассылки.

240.0.0.0/4 (кроме случаев, когда 255.255.255.255/32 выступает как адрес получателя.)	Блок, ранее известный как сеть класса E, зарезервирован.
---	--

Если зарезервированные подсети включены, то удалить отдельные зарезервированные адреса невозможно.

Пример:

```
console(config)# security-suite deny martian-addresses add  
172.18.0.21 /24
```

11.5. Команда security-suite deny syn

Команда **security-suite deny syn** предназначена для блокировки создания TCP соединения на заданном интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

```
security-suite deny syn { add { tcp-port | any } { ip-address | any } { mask | prefix-length } |  
remove { tcp-port | any } { ip-address | any } { mask | prefix-length } }
```

no security-suite deny syn

Параметры:

- **add** { *ip-address* | **any** } – добавляет IP-адрес с которого отбрасываются пакеты в список на интерфейсе. Использование **any** запрещает пакеты со всех адресов;
- *mask* – сетевая маска для указанного IP-адреса;
- *prefix-length* – префикс сети;
- { *tcp-port* | **any** } – Задаёт определенный TCP порт. Возможны следующие значения: **http**, **ftp-control**, **ftp-data**, **ssh**, **telnet**, **smtp** или задать номер порта. Использование **any** указывает на все порты.

Состояние по умолчанию:

Создание TCP соединений разрешено на всех интерфейсах.

Если параметр *mask* не задан, то по умолчанию принимается 255.255.255.255.

Если параметр *prefix-length* не указан, то по умолчанию принимается /32.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

1. Данная команда доступна после включения режима **security-suite** глобально.
2. Блокировка создания TCP соединений осуществляется путем отбрасывания входящих TCP-пакетов с флагами «SYN=1», «ACK=0» и «FIN=0», для указанных IP-адресов и TCP-портов назначения.

Пример:

```
console(config-if)# security-suite deny syn add any any
```

11.6. Команда security-suite deny syn-fin

Команда **security-suite deny syn-fin** предназначена для включения функции отбрасывания всех входящих TCP пакетов с установленными влагами SYN и FIN. Использование префикса «**no**» отключает функцию.

Синтаксис:

security-suite deny syn-fin

no security-suite deny syn-fin

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

По умолчанию функция отключена.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# security-suite deny syn-fin
```

11.7. Команда security-suite dos protect

Команда **security-suite dos protect** предназначена для включения защиты устройства от DoS (Denial of Service) атак. Существует три типа атак данного класса от которых можно применить данную команду (см. параметры). Использование префикса «**no**» отключает механизм защиты.

Синтаксис:

security-suite dos protect {add *attack* | remove *attack*}

no security-suite dos protect

Параметры:

- **add/remove *attack*** – добавляет или удаляет тип атаки. Допустимые типы:
 - **stacheldraht** - отбрасывает все пакеты с источником TCP порта 16660;
 - **invasor-trojan** - отбрасывает все пакеты с назначением TCP порта 1024;
 - **back-orifice-trojan** - отбрасывает все UDP пакеты с назначением на порт 31337 и источником порта 1024.

Состояние по умолчанию:

Защита отключена.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Данная команда доступна после включения режима **security-suite** глобально.

Пример:

```
console(config)# security-suite dos protect add back-orifice-trojan
```

11.8. Команда security-suite dos syn-attack

Команда **security-suite dos syn-attack** предназначена для ограничения скорости потока при DoS SYN атаке. Использование префикса «**no**» снимает ограничение.

Синтаксис:

```
security-suite dos syn-attack syn-rate { any | ip-address } { mask | prefix-length }
```

```
no security-suite dos syn-attack { any | ip-address } { mask | prefix-length }
```

Параметры:

- *syn-rate* – задает максимальное количество соединений в секунду. Диапазон: 199 – 1000;
- { **any** | *ip-address* } – IP-адрес назначения. Параметр *any* указывает на все IP-адреса;
- *mask* – сетевая маска адреса назначения;
- *prefix-length* – величина префикса IP-адреса назначения.

Состояние по умолчанию:

Ограничение на количество соединений отсутствует.

Если параметр *mask* не задан, то по умолчанию принимается 255.255.255.255.

Если параметр *prefix-length* не указан, то по умолчанию принимается /32.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

1. Данная команда доступна после включения режима **security-suite** глобально.
2. Команда ограничивает входящие TCP пакеты, включающие флаги «SYN=1», «ACK=0» и «FIN=0» для указанных IP-адресов назначения.
3. Ограничение скорости SYN атаки реализуется после применения правил безопасности к пакетам. Правила ACL и QoS не применяются к этим пакетам.
4. Поскольку аппаратные возможности ограничивают скорость подсчета байт, предполагается что размер SYN пакетов небольшой.

Пример:

```
console(config)# interface GigabitEthernet 1/0/15  
console(config-if)# security-suite dos syn-attack 300 any /10
```

11.9. Команда `security-suite syn protection mode`

Команда **`security-suite syn protection mode`** предназначена для включения режима защиты TCP SYN. Использование префикса «**no**» отключает режим.

Синтаксис:

`security-suite syn protection mode { disabled | report | block }`

`no security-suite syn protection mode`

Параметры:

- **`disabled`** – режим отключен.
- **`report`** – отчеты о характере трафика TCP SYN на порт (включая SYSLOG сообщение с ограничением скорости при обнаружении атаки).
- **`block`** – трафик TCP SYN атакующий порты предназначенные для локальной системы блокируется и генерируется SYSLOG сообщение (одно в минуту) об ограничении скорости.

Режим по умолчанию:

По умолчанию применяется блокировка трафика.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

На портах, на которых применен ACL данная функция не может блокировать пакеты TCP SYN. В этом случае, если режим защиты заблокирован, но SYN трафик не может быть заблокирован, будет создано соответствующее сообщение SYSLOG, например: «port gi1/0/1 is under TCP SYN attack. TCP SYN traffic cannot be blocked on this port since the port is bound to an ACL.»

Пример:

```
console(config)# security-suite syn protection mode report
```

11.10. Команда `security-suite syn protection recovery`

Команда **`security-suite syn protection recovery`** предназначена для установки временного периода для функции защиты SYN, по истечении которого атакуемый интерфейс блокируется. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

`security-suite syn protection recovery timeout`

`no security-suite syn protection recovery`

Параметры:

- *timeout* – определяет временной период (в секундах), по истечении которого разблокируется интерфейс на который поступают SYN пакеты. В случае, если атака еще активна, то порт блокируется снова. Диапазон: 10 – 600.

Состояние по умолчанию:

Временной период по умолчанию составляет 60 с.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Если временной диапазон изменен, то новое значение будет использоваться только для интерфейсов, которые в настоящее время не подвергаются атаке.

Пример:

```
console(config)# security-suite syn protection recovery 200
```

11.11. Команда `security-suite protection threshold`

Команда **security-suite protection threshold** предназначена для установления порога определения SYN атаки. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

security-suite syn protection threshold *syn-packet-rate*

no security-suite syn protection threshold

Параметры:

- *syn-packet-rate* – устанавливает скорость (количество пакетов в секунду) от каждого конкретного порта, которая является идентификатором атаки TCP SYN. Диапазон: 20 – 200.

Состояние по умолчанию:

По умолчанию порог составляет 80 пакетов в секунду (pps).

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# security-suite syn protection threshold 200
```

11.12. Команда `show security-suite configuration`

Команда **show security-suite configuration** предназначена для отображения на экране конфигурации функционала безопасности.

Синтаксис:

show security-suite configuration

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show security-suite configuration

Security suite is enabled (global-rules-only mode).

Denial Of Service Protect:

Denial Of Service SYN-FIN Attack is enabled
Denial Of Service SYN Attack

  Interface          IP Address          SYN Rate (pps)
  -----
Tel1/0/1             172.16.23.0/24     100

Martian addresses filtering
Reserved addresses: disabled
Configured addresses: 10.0.0.0/8, 192.168.0.0/16

SYN filtering

  Interface          IP Address          TCP port
  -----
tel1/0/2             172.16.23.0/24     FTP

ICMP filtering

  Interface          IP Address
  -----
tel1/0/2             172.16.23.0/24

Fragmented packets filtering

  Interface          IP Address
  -----
tel1/0/2             172.16.23.0/24
```


11.13. Команда show security-suite syn protection

Команда **show security-suite syn protection** предназначена для отображения на экране конфигурации функции SYN Protection и рабочего состояния для заданного интерфейса, включая время последней атаки на интерфейс.

Синтаксис:

show security-suite syn protection [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Используются идентификаторы портов Ethernet или Port Channel.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Параметр *interface-id* используется для указания конкретного интерфейса.

Пример:

```
console# show security-suite syn protection
Protection Mode: Report
Threshold: 200
Recovery: 200

Interface      Operational          Last Attack
Name           Status
-----
tel/0/1        Attacked            19:58:22.289 PDT Feb 19 2012 Blocked and
Reported
tel/0/2        Attacked            19:58:22.289 PDT Feb 19 2012 Reported
```

12. КОМАНДЫ КОНФИГУРИРОВАНИЯ ETHERNET

12.1. Команда interface

Команда **interface** предназначена для перехода в режим конфигурации интерфейса.

Синтаксис:

interface *interface-id*

Параметры:

- *interface-id* – Идентификатор интерфейса. Применим для следующих типов: Ethernet port, port-channel, VLAN, OOB, IP interface, Tunnel.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# interface gi1/0/10
```

12.2. Команда interface range

Команда **interface range** предназначена для перехода в режим конфигурации интерфейса для нескольких портов

Синтаксис:

interface range *interface-id-list*

Параметры:

- *interface-id-list* – список идентификаторов интерфейсов. Применим для следующих типов: Ethernet port, port-channel или VLAN.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Команды в контексте диапазона интерфейсов выполняются независимо на каждом интерфейсе. Если команда возвращает ошибку на одном интерфейсе, ее выполнение продолжается для остальных интерфейсов из списка.

Пример:

```
console(config)# interface range gi1/0/2-10  
console(config-if-range) #
```

12.3. Команда shutdown

Команда **shutdown** предназначена для отключения интерфейса. Использование префикса «**no**» приводит к рестарту отключенного интерфейса.

Синтаксис:

shutdown

no shutdown

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Интерфейсы находятся во включенном состоянии.

Режим ИКС:

Режим конфигурации интерфейса

Примечания:

1. Команда устанавливает значение `ifAdminStatus` (см. RFC 2863) в состояние DOWN. Если `ifAdminStatus` изменен на DOWN, то и `ifOperStatus` также будет изменен на DOWN.
2. Состояние DOWN в `ifOperStatus` означает что интерфейс не передает или не принимает сообщения с/на более высокие уровни. Например, если отключить VLAN, на который настроен IP интерфейс, то коммутатор не сможет передавать и принимать IP-трафик в VLAN.
3. Если отключить порт Ethernet, то коммутатор дополнительно отключает подуровень MAC порта.
4. Если отключить `port-channel`, то коммутатор отключит все порты входящие в интерфейс.

Пример:

```
console(config)# interface tel/0/1
console(config-if)# shutdown
```

12.4. Команда `operation time`

Команда **operation time** предназначена для установки временных ограничений работоспособности порта. Использование префикса «**no**» снимает ограничения.

Синтаксис:

operation time *time-range-name*

no operation time

Параметры:

- *time-range-name* – имя временного диапазона, в течение которого интерфейс находится во включенном состоянии. Когда диапазон не действует, интерфейс выключается.

Состояние по умолчанию:

Временной диапазон отсутствует.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

1. Рекомендуется отключать протокол STP или включать режим PortFast на 802.1x клиентских портах, для пропуска трафика сразу после успешной аутентификации.
2. Команда не будет иметь эффекта, если порт находится в выключенном состоянии по каким-либо другим причинам.

Пример:

```
console(config)# interface tel/0/1
console(config-if)# operation time morning
```

12.5. Команда description

Команда **description** предназначена для добавления описания к интерфейсу. Использование префикса **no** удаляет описание.

Синтаксис:

description *string*

no description

Параметры:

- *string* – комментарий или описание порта, для удобства администратора. Длина: 1 – 64 символа.

Состояние по умолчанию:

Описание отсутствует.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel, VLAN, Tunnel)

Пример:

```
console(config)# interface tel/0/1
console(config-if)# description UpLink
```

12.6. Команда `speed`

Команда **speed** предназначена для указания скорости передачи данных, если режим автоопределения не используется. Использование префикса «no» устанавливает режим по умолчанию.

Синтаксис:

speed { 10 | 100 | 1000 | 10000 }

no speed

Параметры:

- **10** – устанавливает скорость в 10 Мбит/с (только для OOB интерфейса).
- **100** – устанавливает скорость в 100 Мбит/с.
- **1000** – устанавливает скорость в 1 ГБ/с.
- **10000** – устанавливает скорость в 10 ГБ/с (только для SFP+ интерфейсов).

Состояние по умолчанию:

По умолчанию порт работает на максимально возможной скорости.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечание:

Использование команды **no speed** на интерфейсе Port-channel устанавливает на каждом порту канала режим максимально возможной скорости.

Пример:

```
console(config)# interface te1/0/1
console(config-if)# speed 1000
```

12.7. Команда `duplex`

Команда **duplex** предназначена для установки полно- или полудуплексного режима на интерфейсе, если режим автосогласования не используется или выключен. Использование префикса «no» устанавливает параметры по умолчанию.

Синтаксис:

duplex { half | full }

no duplex

Параметры:

- **half** – принудительно полудуплексный режим передачи;
- **full** – принудительно полнодуплексный режим передачи.

Состояние по умолчанию:

По умолчанию используется полнодуплексный режим.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Пример:

```
console(config)# interface gi1/0/10
console(config-if)# duplex full
```

12.8. Команда negotiation

Команда **negotiation** предназначена для включения автосогласования режима передачи и скорости интерфейса. Использование префикса **no** отключает автосогласование.

Синтаксис:

negotiation [*capability* [*capability2... capability5*]] [**preferred** { **master** | **slave** }]

no negotiation

Параметры:

- *capability* – устанавливает заявленные значения. Допустимые варианты:
 - **10h** – скорость 10 Мбит/с, полудуплексный режим;
 - **10f** – скорость 10 Мбит/с, полнодуплексный режим;
 - **100h** – скорость 100 Мбит/с, полудуплексный режим;
 - **100f** – скорость 100 Мбит/с, полнодуплексный режим;
 - **1000f** – скорость 1000 Мбит/с, полнодуплексный режим;
 - **10000f** – скорость 10000 Мбит/с, полнодуплексный режим;
- **preferred** – определяет предпочтения:
 - **master** – объявляет ведущим;
 - **slave** – объявляет ведомым.

Состояние по умолчанию:

Параметр *capability* не определен, по умолчанию используется список всех возможных состояний порта и предпочтительный режим - **master**.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Пример:

```
console(config)# interface gi1/0/10
console(config-if)# negotiation 1000f
```

12.9. Команда flowcontrol

Команда **flowcontrol** применяется для настройки управления потоком данных на интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

flowcontrol { auto | on | off }

no flowcontrol

Параметры:

- **auto** – устанавливает режим автоопределения управления потоком;
- **on** – включает управление потоком;
- **off** – отключает управление потоком.

Состояние по умолчанию:

Управление потоком отключено.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечание:

Применение команды **negotiation** включает автоматическое управление потоком.

Пример:

```
console(config)# interface gil/0/10
console(config-if)# flowcontrol on
```

12.10. Команда **mdix**

Команда **mdix** предназначена для включения возможности использования кроссовер кабеля на интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

mdix { on | auto }

no mdix

Параметры:

- **on** – принудительное включение MDIX;
- **auto** – автоматическая проверка MDI/MDIX.

Состояние по умолчанию:

По умолчанию используется режим **auto**.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Пример:

```
console(config)# interface gil/0/10
console(config-if)# mdix on
```

12.11. Команда back-pressure

Команда **back-pressure** предназначена для включения противоподавления на интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

back-pressure

no back-pressure

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Режим противоподавления отключен.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

При включенном режиме EEE противоподавления не может быть включен.

Пример:

```
console(config)# interface gil1/0/10
console(config-if)# back-pressure
```

12.12. Команда port jumbo-frame

Команда **port jumbo-frame** предназначена для разрешения использования jumbo frames на коммутаторе. Использование префикса «**no**» отключает режим.

Синтаксис:

port jumbo-frames

no port jumbo-frames

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Использование jumbo frames запрещено на устройстве.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Использование jumbo frames возможно только после выполнения команды, сохранения конфигурации и перезагрузки коммутатора.

Пример:

```
console(config)# port jumbo-frame
This setting will take effect only after copying running
configuration to startup configuration and resetting the device
```

12.13. Команда clear counters

Команда **clear counters** предназначена для очистки данных счетчиков все или заданного интерфейсе.

Синтаксис:

clear counters [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Доступны следующие типы: Ethernet, Port Channel, OOB.

Состояние по умолчанию:

Применение команды без указания идентификатора очищает счетчики всех интерфейсов.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear counters gi1/0/5
```

12.14. Команда set interface active

Команда **set interface active** предназначена для реактивации интерфейса после его отключения.

Синтаксис:

set interface active *interface-id*

Параметры:

- *interface-id* – идентификатор интерфейса. Доступны следующие типы: Ethernet, Port Channel.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Команда используется для повторной активации интерфейсов, которые были настроены как активные, но отключены системой.

Пример:

```
console# set interface active tel/0/1
```

12.15. Команда `errdisable recovery cause`

Команда **`errdisable recovery cause`** предназначена для автоматической реактивации интерфейса, выключенного после наступления события “Err-Disable”. Использование префикса «**no**» отключает данную функцию.

Синтаксис:

```
errdisable recovery cause { all | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | loopback-detection | storm-control | udld | link-flapping }
```

```
no errdisable recovery cause { all | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | loopback-detection | storm-control | udld | link-flapping }
```

Параметры:

- **all** – включает механизм реактивации для всех типов ошибок;
- **port-security** – включает механизм восстановления ошибки для состояния Err-Disable port-security;
- **dot1x-src-address** – включает механизм восстановления для состояния Err-Disable 802.1x;
- **acl-deny** – включает механизм восстановления только для состояния Err-Disable ACL Deny;
- **stp-bpdu-guard** – включает механизм восстановления для состояния Err-Disable STP BPDU Guard;
- **loopback-guard** – включает механизм восстановления для состояния Err-Disable Loopback Detection;
- **storm-control** – включает механизм восстановления для состояния Err-Disable Storm Control Shutdown;
- **udld** – включает механизм восстановления для состояния Err-Disable UDLD;
- **link-flapping** – включает механизм восстановления для состояния Err-Disable link-flapping.

Состояние по умолчанию:

Автоматическая реактивация отключена.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# errdisable recovery cause all
```

12.16. Команда `errdisable recovery interval`

Команда **`errdisable recovery interval`** предназначена для установки временного интервала, по истечении которого производится реактивация интерфейса. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

`errdisable recovery interval` *seconds*

`no errdisable recovery interval`

Параметры:

- *seconds* – временной интервал в секундах. Диапазон: 30 – 86400.

Состояние по умолчанию:

Временной интервал по умолчанию – 300 с.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# errdisable recovery interval 600
```

12.17. Команда `errdisable recovery reset`

Команда **`errdisable recovery reset`** предназначена для повторной активации одного или нескольких интерфейсов, отключенных при наступлении состояния Err-Disable.

Синтаксис:

`errdisable recovery reset` { **`all`** | **`port-security`** | **`dot1x-src-address`** | **`acl-deny`** | **`stp-bpdu-guard`** | **`loopback-detection`** | **`storm-control`** | **`interface`** *interface-id* }

Параметры:

- **`all`** – включает механизм реактивации для всех типов ошибок, описанных ниже;
- **`port-security`** – включает механизм восстановления ошибки для состояния Err-Disable port-security;
- **`dot1x-src-address`** – включает механизм восстановления для состояния Err-Disable 802.1x;
- **`acl-deny`** – включает механизм восстановления только для состояния Err-Disable ACL Deny;
- **`stp-bpdu-guard`** – включает механизм восстановления для состояния Err-Disable STP BPDU Guard;
- **`loopback-guard`** – включает механизм восстановления для состояния Err-Disable Loopback Detection;
- **`storm-control`** – включает механизм восстановления для состояния Err-Disable Storm Control Shutdown;

gil/0/5	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/6	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/7	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/8	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/9	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/10	1G-Fiber	Full	100	Enabled	On	Up
Enabled On						
gil/0/11	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/12	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/13	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/14	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/15	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/16	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/17	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/18	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/19	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/20	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/21	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/22	1G-Fiber	Full	100	Disabled	Off	Up
Disabled Auto						
gil/0/23	1G-Fiber	Full	1000	Disabled	Off	Up
Disabled Auto						
gil/0/24	1G-CopperSFP	Full	1000	Disabled	Off	Up
Disabled Auto						
tel/0/1	10G-Fiber	Full	1000	Disabled	Off	Down
Disabled Off						
tel/0/2	10G-Fiber	Full	10000	Disabled	Off	Up
Disabled Off						

12.19. Команда show interfaces status

Команда **show interfaces status** предназначена для отображения текущего статуса одного или всех интерфейсов.

Синтаксис:

show interfaces status [*interface-id* | **detailed**]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel.
- **detailed** – отображает информацию о неучтенных портах в дополнение к текущим портам.

Состояние по умолчанию:

Отображает информацию обо всех интерфейсах. Если параметр **detailed** не используется, то отображаются только текущие порты.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show interfaces status
```

Back	Mdix	Port	Type	Duplex	Speed	Neg	ctrl	Flow Link	State
		Pressure Mode							
		-----	-----	-----	-----	-----	-----	-----	-----

		gil/0/1	1G-CopperSFP	Full	1000	Disabled	Off	Up	
		Disabled	Off						
		gil/0/2	1G-Fiber	--	--	--	--	Down	--
		gil/0/3	1G-Fiber	--	--	--	--	Down	--
		gil/0/4	1G-Fiber	--	--	--	--	Down	--
		gil/0/5	1G-Fiber	--	--	--	--	Down	--
		gil/0/6	1G-Fiber	--	--	--	--	Down	--
		gil/0/7	1G-Fiber	--	--	--	--	Down	--
		gil/0/8	1G-Fiber	--	--	--	--	Down	--
		gil/0/9	1G-Fiber	--	--	--	--	Down	--
		gil/0/10	1G-Fiber	--	--	--	--	Down	--
		gil/0/11	1G-Fiber	--	--	--	--	Down	--
		gil/0/12	1G-Fiber	--	--	--	--	Down	--
		gil/0/13	1G-Fiber	--	--	--	--	Down	--
		gil/0/14	1G-Fiber	--	--	--	--	Down	--
		gil/0/15	1G-Fiber	--	--	--	--	Down	--

gil/0/16	1G-Fiber	--	--	--	--	Down	--

gil/0/17	1G-Fiber	--	--	--	--	Down	--

gil/0/18	1G-Fiber	--	--	--	--	Down	--

gil/0/19	1G-Fiber	--	--	--	--	Down	--

gil/0/20	1G-Fiber	--	--	--	--	Down	--

gil/0/21	1G-Fiber	--	--	--	--	Down	--

gil/0/22	1G-Fiber	--	--	--	--	Down	--

gil/0/23	1G-Fiber	--	--	--	--	Down	--

gil/0/24	1G-CopperSFP	Full	1000	Disabled	Off	Up	
Disabled	Off						
tel/0/1	10G-Fiber	--	--	--	--	Down	--

tel/0/2	10G-Fiber	--	--	--	--	Down	--

12.20. Команда show interfaces advertise

Команда **show interfaces advertise** предназначена для отображения на экране информации настроек автосогласования для одного или всех интерфейсов.

Синтаксис:

show interfaces advertise [{ *interface-id* | **detailed** }]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel;
- **detailed** – отображает информацию о неучтенных портах в дополнение к текущим портам.

Состояние по умолчанию:

Отображает информацию обо всех интерфейсах. Если параметр **detailed** не используется, то отображаются только текущие порты.

Режим ИКС:

Привилегированный режим управления.

Пример:

```

console# show interfaces advertise
Port      Type      Neg      Preferred  Operational Link
Advertisement
-----
-----
-----

```

gil/0/1	1G-CopperSFP	Disabled	--	--
gil/0/2	1G-Fiber	Disabled	--	--
gil/0/3	1G-Fiber	Disabled	--	--
gil/0/4	1G-Fiber	Disabled	--	--
gil/0/5	1G-Fiber	Disabled	--	--
gil/0/6	1G-Fiber	Disabled	--	--
gil/0/7	1G-Fiber	Disabled	--	--
gil/0/8	1G-Fiber	Disabled	--	--
gil/0/9	1G-Fiber	Disabled	--	--
gil/0/10	1G-Fiber	Enabled	Slave	--
gil/0/11	1G-Fiber	Disabled	--	--
gil/0/12	1G-Fiber	Disabled	--	--
gil/0/13	1G-Fiber	Disabled	--	--
gil/0/14	1G-Fiber	Disabled	--	--
gil/0/15	1G-Fiber	Disabled	--	--
gil/0/16	1G-Fiber	Disabled	--	--
gil/0/17	1G-Fiber	Disabled	--	--
gil/0/18	1G-Fiber	Disabled	--	--
gil/0/19	1G-Fiber	Disabled	--	--
gil/0/20	1G-Fiber	Disabled	--	--
gil/0/21	1G-Fiber	Disabled	--	--
gil/0/22	1G-Fiber	Disabled	--	--
gil/0/23	1G-Fiber	Disabled	--	--
gil/0/24	1G-CopperSFP	Disabled	--	--
te1/0/1	10G-Fiber	Disabled	--	--
te1/0/2	10G-Fiber	Disabled	--	--

12.21. Команда show interfaces description

Команда **show interfaces description** предназначена для отображения на экране описания одного или всех сконфигурированных портов.

Синтаксис:

show interfaces description [{ *interface-id* | **detailed** }]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel.
- **detailed** – отображает информацию о неучтенных портах в дополнение к текущим портам.

Состояние по умолчанию:

Отображает информацию обо всех интерфейсах. Если параметр **detailed** не используется, то отображаются только текущие порты.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show interfaces description
Port      Description
```



```
-----  
-----  
gi1/0/1  
gi1/0/2  
gi1/0/3  
gi1/0/4  
gi1/0/5  
gi1/0/6  
gi1/0/7  
gi1/0/8  
gi1/0/9  
gi1/0/10  
gi1/0/11  
gi1/0/12  
gi1/0/13  
gi1/0/14  
gi1/0/15  
gi1/0/16  
gi1/0/17  
gi1/0/18  
gi1/0/19  
gi1/0/20  
gi1/0/21  
gi1/0/22  
gi1/0/23  
gi1/0/24  
te1/0/1    UpLink  
te1/0/2
```

12.22. Команда show interfaces counters

Команда **show interfaces counters** предназначена для отображения на экране информации о трафике, проходящем через один или все интерфейсы.

Синтаксис:

```
show interfaces counters [ { interface-id | detailed } ]
```

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel;
- **detailed** – отображает информацию о неучтенных портах в дополнение к текущим портам.

Состояние по умолчанию:

Отображает информацию обо всех интерфейсах. Если параметр **detailed** не используется, то отображаются только текущие порты.

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1

```

console# show interfaces counters

```

Port	InUcastPkts	InMcastPkts	InBcastPkts	InOctets

gi1/0/1	1871858166	114	258250	
131086565485				
gi1/0/2	0	0	0	0
gi1/0/3	0	0	0	0
gi1/0/4	0	0	0	0
gi1/0/5	0	0	0	0
gi1/0/6	0	0	0	0
gi1/0/7	0	0	0	0
gi1/0/8	0	0	0	0
gi1/0/9	0	0	0	0
gi1/0/10	0	0	0	0
gi1/0/11	0	0	0	0
gi1/0/12	0	0	0	0
gi1/0/13	0	0	0	0
gi1/0/14	0	0	0	0
gi1/0/15	0	0	0	0
gi1/0/16	0	0	0	0
gi1/0/17	0	0	0	0
gi1/0/18	0	0	0	0
gi1/0/19	0	0	0	0
gi1/0/20	0	0	0	0
gi1/0/21	0	0	0	0
gi1/0/22	0	0	0	0
gi1/0/23	0	0	0	0
gi1/0/24	1905202975	233264	7009	
420100217306				
tel1/0/1	0	0	0	68
tel1/0/2	0	0	0	0
Port	OutUcastPkts	OutMcastPkts	OutBcastPkts	OutOctets

gi1/0/1	1905202761	245166	13939	
420100231369				
gi1/0/2	0	0	0	50
gi1/0/3	0	0	0	0
gi1/0/4	0	0	0	0
gi1/0/5	0	0	0	0
gi1/0/6	0	0	0	0
gi1/0/7	0	0	0	0
gi1/0/8	0	0	0	0
gi1/0/9	0	0	0	0
gi1/0/10	0	0	0	0
gi1/0/11	0	0	0	0
gi1/0/12	0	0	0	0
gi1/0/13	0	0	0	0
gi1/0/14	0	0	0	0

gi1/0/15	0	0	0	0
gi1/0/16	0	0	0	0
gi1/0/17	0	0	0	0
gi1/0/18	0	0	0	0
gi1/0/19	0	0	0	0
gi1/0/20	0	0	0	0
gi1/0/21	0	0	0	0
gi1/0/22	0	0	0	0
gi1/0/23	0	0	0	0
gi1/0/24	1871858167	25540	265062	
131089245312				
tel1/0/1	0	0	0	0
tel1/0/2	0	0	0	0

Пример 2

```

console# show interfaces counters gi1/0/24

```

Port	InUcastPkts	InMcastPkts	InBcastPkts	InOctets
-----	-----	-----	-----	-----
gi1/0/24	1905202975	233330	7010	
420100217353				13

Port	OutUcastPkts	OutMcastPkts	OutBcastPkts	OutOctets
-----	-----	-----	-----	-----
gi1/0/24	1871858167	25544	265130	
131089249992				

```

Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0

```

Поля вывода:

Поле	Описание
InOctets	Количество принятых октетов.
InUcastPkts	Количество принятых одноадресных пакетов.
InMcastPkts	Количество принятых многоадресных пакетов.

InBcastPkts	Количество принятых широковещательных пакетов.
OutOctets	Количество переданных октетов.
OutUcastPkts	Количество переданных одноадресных пакетов.
OutMcastPkts	Количество переданных многоадресных пакетов.
OutBcastPkts	Количество переданных широковещательных пакетов.
FCS Errors	Количество принятых кадров, которые являются частью октетов, но не прошедших проверку FCS.
Single Collision Frames	Количество кадров участвующих в одиночном столкновении (коллизии), но переданных успешно.
Multiple Collision Frames	Количество кадров участвующих в неоднократном столкновении (коллизии), но переданных успешно.
SQE Test Errors	Количество ошибок SQE TEST ERROR. Данная ошибка устанавливается в соответствии с механизмом проверки обнаружения SQE в функции Carrier Sense PLS, как описано в стандарте IEEE 802.3, редакции 2000г., раздел 7.2.4.6.
Deferred Transmissions	Количество кадров, для которых первая попытка передачи отложена из-за занятости среды передачи.
Late Collisions	Количество раз, когда коллизия обнаружена позднее, чем за один временной слот.
Excessive Collisions	Количество кадров для которых передача не удалась из-за чрезмерных коллизий.
Oversize Packets	Количество кадров, превышающих максимально разрешенный размер.
Internal MAC Rx Errors	Количество кадров, для которых прием невозможен из-за внутренней ошибки MAC подуровня.
Received Pause Frames	Количество полученных контрольных MAC кадров с кодом PAUSE.
Transmitted Pause Frames	Количество переданных контрольных MAC кадров с кодом PAUSE.

12.23. Команда show ports jumbo-frames

Команда **show ports jumbo-frames** предназначена для отображения информации о работе с большими кадрами (jumbo frames).

Синтаксис:

show ports jumbo-frames

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ports jumbo-frame
```

```
Jumbo frames are disabled  
Jumbo frames will be enabled after reset
```

12.24. Команда show errdisable recovery

Команда **show errdisable recovery** предназначена для отображения информации о настройках конфигурации Err-Disable устройства.

Синтаксис:

show errdisable recovery

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show errdisable recovery  
  
Timer interval: 600 Seconds  
  
          Reason                Automatic Recovery  
-----  
loopback_detection             Enable  
port-security                  Enable  
dot1x-src-address              Enable  
acl-deny                       Enable  
stp-bpdu-guard                 Enable  
stp-loopback-guard             Enable  
udld                           Enable  
storm-control                  Enable  
link-flapping                  Enable
```

12.25. Команда show errdisable interfaces

Команда **show errdisable interfaces** предназначена для отображения информации о статусе Err-Disable одного или всех интерфейсов.

Синтаксис:

show errdisable interfaces [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel.

Состояние по умолчанию:

Отображается информация обо всех интерфейсах.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show errdisable interfaces

  Interface          Reason
  -----
te1/0/1             stp-bpdu-guard
```

12.26. Команда clear switchport monitor

Команда **clear switchport monitor** предназначена для очистки контролируемой статистики по определенному интерфейсу.

Синтаксис:

clear switchport monitor [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear switchport monitor gi1/0/10
```

12.27. Команда show switchport monitor

Команда предназначена для отображения статистики, собираемой на указанном интерфейсе.

Синтаксис:

show switchport monitor *interface-id* { **seconds** | **minutes** | **hours** } [{ **utilization** | **tx** | **rx** | **frames** }]

show switchport monitor *interface-id* { **days** | **weeks** }

show switchport monitor utilization [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel.
- **seconds** – последние 20 образцов, отбираемые каждые 15 с;
- **minute** – последние 60 образцов, отбираемые каждые 60 с. (каждую минуту в соответствии с системным временем);

- **hours** – последние 24 образца, отбираемые каждые 60 мин. (каждый час в соответствии с системным временем);
- **days** – последние 7 образцов, отбираемые каждые 24 часа (от полуночи до полуночи в соответствии с системным временем);
- **weeks** – последние 12 образцов, отбираемые каждые 7 дней (от полуночи субботы до полуночи субботы в соответствии с системным временем);
- **utilization** – отображает расчет использования за прошедший период времени;
- **rx** – статистика приема;
- **tx** – статистика передачи;
- **frames** – собранная статистика по размерам пакетов.

Состояние по умолчанию:

Информация отображается для одного интерфейса, либо для всех в случае выбора команды **show switchport monitor utilization**.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Команда **show switchport monitor utilization** используется для отображения статистики об использовании в каждом временном интервале (т.е. за последнюю минуту, последний час, последний день или последнюю неделю).
2. Команда **show switchport monitor interface-id** используется для отображения выборок статистики, собранных за период времени и для типов счетчиков.

Примеры:

Пример 1

```
console# show switchport monitor utilization gil/0/24
```

Interface	Last Minute Utilization		Last Hour Utilization		Last Day Utilization		Last Week Utilization	
	RX	TX	RX	TX	RX	TX	RX	TX
gil/0/24	0	0	0	0	95	0	~75	~ 0

Пример 2

```
console# show switchport monitor gil/0/24 days
```

Sample Time	Tx Utilization	Rx Utilization
Thu 10/05/2018 00:00:00	0	0
Fri 11/05/2018 00:00:00	0	0
Sat 12/05/2018 00:00:00	~ 0	52
Sun 13/05/2018 00:00:00	0	98

Mon 14/05/2018 00:00:00	0	81
Tue 15/05/2018 00:00:00	0	39
Wed 16/05/2018 00:00:00	0	95

Описание полей вывода:

Поле	Описание
Time	Время текущего образца в системном формате. Например формат для часов, минут и секунд: hh:mm:ss. Формат для дней и недель <day of week>: dd/mm/yy.
Good Octets Received	Количество принятых октетов.
Good Unicast frames Received	Количество принятых unicast пакетов.
Good Multicast frames Received	Количество принятых multicast пакетов.
Good Broadcast frames Received	Количество принятых broadcast пакетов.
Good Octets Sent	Количество переданных октетов
Good Unicast frames Sent	Количество переданных unicast пакетов.
Good Multicast frames Sent	Количество переданных multicast пакетов.
Good Broadcast frames Sent	Количество принятых broadcast пакетов.
Frames of 64 bytes	Количество принятых пакетов размером 64 Б.
Frames of 65-127 bytes	Количество принятых пакетов размером 65 - 127 Б.
Frames of 128-255 bytes	Количество принятых пакетов размером 128 - 255 Б.
Frames of 256-511 bytes	Количество принятых пакетов размером 256 - 511 Б.
Frames of 512-1023 bytes	Количество принятых пакетов размером 512 - 1023 Б.
Frames of 1024-1518 bytes	Количество принятых пакетов размером 1024 - 1518 Б.
Rx Error Frames Received	Количество полученных кадров, которые являются целым числом октетов в длину, но не проходят проверку FCS.
Rx Utilization	Использование в процентах на получение кадров на интерфейсе.
Tx Utilization	Использование в процентах на передачу кадров на интерфейсе.
Rx/Tx Utilization	Среднее использование Rx и Tx в процентах на интерфейсе.

13. КОМАНДЫ НАСТРОЙКИ ПРОТОКОЛА GVRP (GARP VLAN REGISTRATION PROTOCOL)

13.1. Команда `clear gvrp statistics`

Команда **clear gvrp statistics** предназначена для очистки собранной статистики на одном или всех интерфейсах.

Синтаксис:

clear gvrp statistics [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимы следующие типы: Ethernet, Port Channel.

Состояние по умолчанию:

Очищается статистика на всех интерфейсах.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear gvrp statistics
```

13.2. Команда `gvrp enable (Global)`

Команда **gvrp enable (Global)** предназначена для общего включения протокола GVRP на коммутаторе. Использование префикса «**no**» отключает протокол.

Синтаксис:

gvrp enable

no gvrp enable

Состояние по умолчанию:

Протокол GVRP по умолчанию глобально выключен.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# gvrp enable
```

13.3. Команда `gvrp enable` (Interface)

Команда **`gvrp enable`** (Interface) предназначена для включения протокола GVRP на интерфейсе. Использование префикса «**no**» отключает протокол на интерфейсе.

Синтаксис:

`gvrp enable`

`no gvrp enable`

Состояние по умолчанию:

Протокол GVRP отключен на всех интерфейсах

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечание:

Порт доступа всегда является членом одной VLAN. Членство в нетегированной VLAN распространяется так же, как и в тегированной VLAN. Т.е. PVID должен быть определен вручную как не тегированный VLAN.

Пример:

```
console(config)# interface gil/0/15
console(config-if)# gvrp enable
```

13.4. Команда `garp timer`

Команда предназначена для установки значений таймеров **`join`**, **`leave`**, **`leaveall`** приложений GARP. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

`garp timer { join | leave | leaveall } timer-value`

`no garp timer`

Параметры:

1. Указывается тип таймера. Возможны следующие значения:
 - **`join`** – таймер подключения GARP. Значение для этого типа таймера указывает временной интервал между двумя сообщениями подключения отправленного приложением GARP.
 - **`leave`** – таймер отключения GARP. Значения для этого типа таймера указывает временной интервал между двумя сообщениями об отключении, прежде чем отменяется регистрация GARP.
 - **`leaveall`** – таймер отключения GARP. Значение для этого типа таймера указывает временной интервал между двумя сообщениями, которые побуждают объект GARP произвести перерегистрацию информации всех атрибутов объекта.

2. *timer-value* – устанавливает значение таймера в миллисекундах кратное 10.
Диапазон: 10 – 2147483640.

Состояние по умолчанию:

Значения таймера по умолчанию:

- **join** – 200 миллисекунд
- **leave** – 600 миллисекунд
- **leaveall** – 10000 миллисекунд

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

1. Значение *timer-value* должно быть кратно 10.
2. Между таймерами должно поддерживаться следующее соотношение:
 - значение **leave** таймера должно быть больше или равно трех значений **join** таймера;
 - значение **leaveall** таймера должно быть больше значения **leave** таймера;
3. Для правильной работы приложений GARP необходимо установить одинаковые значения для всех подключенных устройств 2 уровня.

Пример:

```
console(config)# interface tel/0/2  
console(config-if)# garp timer leave 900
```

13.5. Команда `gvrp registration-forbid`

Команда **gvrp registration-forbid** предназначена для отмены регистрации всех динамических VLAN на порту и предотвращает создание или регистрацию новых VLAN. Использование префикса «**no**» снимает запрет.

Синтаксис:

gvrp registration-forbid

no gvrp registration-forbid

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Разрешена регистрация динамических VLAN на всех портах.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel).

Пример:

```
console(config)# interface gil/0/15
```

```
console(config-if)# gvrp registration-forbid
```

13.6. Команда gvrp vlan-creation-forbid

Команда **gvrp vlan-creation-forbid** предназначена для запрета регистрации или модификации динамических VLAN. Использование префикса «**no**» снимает запрет.

Синтаксис:

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Создание и модификация динамических VLAN разрешена.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Пример:

```
console(config)# interface gil/0/15  
console(config-if)# gvrp vlan-creation-forbid
```

13.7. Команда show gvrp configuration

Команда **show gvrp configuration** предназначена для отображения на экране информацию о настройке GVRP, включая значения таймеров, разрешения на создание динамических VLAN и на каких портах включен протокол.

Синтаксис:

show gvrp configuration [{ *interface-id* | **detailed** }]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимы следующие типы: Ethernet, Port Channel.
- **detailed** - отображает информацию о неучтенных портах в дополнение к текущим портам.

Состояние по умолчанию:

Отображается вся информация по всем интерфейсам. Если параметр **detailed** не используется, то отображаются только текущие порты.

Режим ИКС:

Привилегированный режим управления.

10000	gil/0/20	Disabled	Normal	Enabled	200	600
10000	gil/0/21	Disabled	Normal	Enabled	200	600
10000	gil/0/22	Disabled	Normal	Enabled	200	600
10000	gil/0/23	Disabled	Normal	Enabled	200	600
10000	gil/0/24	Disabled	Normal	Enabled	200	600
10000	tel/0/1	Disabled	Normal	Enabled	200	600
10000	tel/0/2	Enabled	Normal	Enabled	200	600

13.8. Команда show gvrp error-statistics

Команда **show gvrp error-statistics** предназначена для отображения на экране информации об ошибках GVRP для одного или всех интерфейсов.

Синтаксис:

show gvrp error-statistics [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимы следующие типы: Ethernet, Port Channel.

Состояние по умолчанию:

Отображается статистика ошибок для всех интерфейсов.

Режим ИКС:

Привилегированный режим управления.

Пример:

```

console# show gvrp error-statistics

GVRP Error Statistics:
-----
Legend:
  INVPROT  : Invalid Protocol Id
  INVATYP  : Invalid Attribute Type  INVALEN  : Invalid Attribute
Length
  INVAVAL  : Invalid Attribute Value INVEVENT: Invalid Event

  Port    INVPROT  INVATYP  INVAVAL  INVALEN  INVEVENT
-----
gil/0/1   0         0        0         0         0
gil/0/2   0         0        0         0         0
gil/0/3   0         0        0         0         0
gil/0/4   0         0        0         0         0

```

13.9. Команда show gvrp statistics

Команда **show gvrp statistics** предназначена для отображения собранной статистики GVRP для всех или одного интерфейса.

Синтаксис:

show gvrp statistics [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимы следующие типы: Ethernet, Port Channel.

Состояние по умолчанию:

Отображается статистика для всех интерфейсов.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show gvrp statistics

GVRP Statistics:
-----
Legend:
  rJE  : Join Empty Received      rJIn: Join In Received
  rEmp : Empty Received           rLIn: Leave In Received
  rLE  : Leave Empty Received     rLA : Leave All Received
  sJE  : Join Empty Sent          sJIn: Join In Sent
  sEmp : Empty Sent               sLIn: Leave In Sent
  sLE  : Leave Empty Sent         sLA : Leave All Sent

  Port      rJE  rJIn  rEmp  rLIn  rLE  rLA  sJE  sJIn  sEmp  sLIn
sLE  sLA
-----
-----
 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0
```

14. КОМАНДЫ IGMP SNOOPING

14.1. Команда ip igmp snooping (Global)

Команда **ip igmp snooping** (Global) предназначена для глобального включения протокола IGMP (Internet Group Management Protocol) snooping. Использование префикса «**no**» отключает протокол.

Синтаксис:

ip igmp snooping

no ip igmp snooping

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip igmp snooping
```

14.2. Команда ip igmp snooping vlan

Команда **ip igmp snooping vlan** предназначена для включения IGMP snooping на заданном VLAN. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Параметры:

- *vlan-id* – идентификатор VLAN.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Режим IGMP snooping может быть включен только для статических VLAN.
2. Поддерживаемые версии протокола: IGMPv1, IGMPv2 и IGMPv3 snooping.
3. Для активации IGMP snooping необходимо предварительно выполнить команду **bridge multicast filtering**.

4. В команде **bridge multicast mode** описывается конфигурация записанная в FDB, в зависимости от режим FDB и версии протокола IGMP.

Пример:

```
console(config)# ip igmp snooping vlan 2
```

14.3. Команда ip igmp snooping vlan mrouter

Команда **ip igmp snooping vlan mrouter** предназначена для включения автоматического изучения портов маршрутизатора многоадресной передачи в VLAN. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip igmp snooping vlan *vlan-id* mrouter learn pim-dvmrp

no ip igmp snooping vlan *vlan-id* mrouter learn pim-dvmrp

Параметры:

- *vlan-id* – идентификатор VLAN.

Состояние по умолчанию:

Обучение pim-dvmrp включено

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Многоадресные порты распознаются в соответствии:
 - Queries получен на порт;
 - PIM/PIMv2 получен на порт;
 - DVMRP получен на порт;
 - MRDISC получен на порт;
 - MOSPF получен на порт.
2. Перед выполнением команды необходимо создать требуемый VLAN.

Пример:

```
console(config)# ip igmp snooping vlan 2 mrouter learn pim-dvmrp
```

14.4. Команда ip igmp snooping vlan mrouter interface

Команда **ip igmp snooping vlan mrouter interface** предназначена для определения порта, который подключен к порту многоадресной передачи маршрутизатора. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip igmp snooping vlan *vlan-id* mrouter interface *interface-id*

no ip igmp snooping vlan *vlan-id* mrouter interface *interface-id*

Параметры:

- *vlan-id* – идентификатор VLAN.
- *interface-id* – идентификатор интерфейса. Допустимы следующие типы: Ethernet, Port Channel.

Состояние по умолчанию:

Порты не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Порт, который определен как порт многоадресной передачи принимает все пакеты IGMP (отчеты и запросы), а также многоадресные данные.
2. Перед выполнением команды необходимо создать требуемый VLAN.

Пример:

```
console(config)# ip igmp snooping vlan 2 mrouter interface gi1/0/10
```

14.5. Команда ip igmp snooping vlan forbidden mrouter

Команда **ip igmp snooping vlan forbidden mrouter** предназначена для запрещения определения порта, как порта многоадресной передачи в автоматической или статической конфигурации. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip igmp snooping vlan *vlan-id* forbidden mrouter interface *interface-id*

no ip igmp snooping vlan *vlan-id* forbidden mrouter interface *interface-id*

Параметры:

- *vlan-id* – идентификатор VLAN;
- *interface-id* – идентификатор интерфейса. Допустимы следующие типы: Ethernet, Port Channel.

Состояние по умолчанию:

Порты не заданы.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Порт, который является запрещенным портом mrouter не может быть портом многоадресной рассылки (т.е. не может быть изучен динамически или назначен статически).

2. Перед выполнением команды необходимо создать требуемый VLAN.

Пример:

```
console(config)# ip igmp snooping vlan 2 forbidden mrouter  
interface gi1/0/10
```

14.6. Команда ip igmp snooping vlan static

Команда **ip igmp snooping vlan static** предназначена для регистрации IP-адреса многоадресной рассылки в таблице моста и добавления статических портов в группу, определенную этим адресом. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip igmp snooping vlan *vlan-id* **static** *ip-address* [**interface** *interface-id*]

no ip igmp snooping vlan *vlan-id* **static** *ip-address* [**interface** *interface-id*]

Параметры:

- *vlan-id* – идентификатор VLAN;
- *ip-address* – IP-адрес многоадресной рассылки;
- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel.

Состояние по умолчанию:

Адрес многоадресной рассылки не задан.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Статический адрес многоадресной рассылки может быть определен только в статическом VLAN.
2. Перед выполнением команды необходимо создать требуемый VLAN.
3. Команда позволяет зарегистрировать адрес без указания интерфейса.
4. Использование префикса «**no**» без указания порта удаляет запись из таблицы.

Пример:

```
console(config)# ip igmp snooping vlan 2 static 239.2.2.2 interface  
gi1/0/10
```

14.7. Команда ip igmp snooping vlan multicast-tv

Команда **ip igmp snooping vlan multicast-tv** предназначена для задания IP-адреса многоадресной рассылки ассоциируемого с многоадресной TV VLAN. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip igmp snooping vlan *vlan-id* multicast-tv *ip-multicast-address* [*count number*]

no ip igmp snooping vlan *vlan-id* multicast-tv *ip-multicast-address* [*count number*]

Параметры:

- *vlan-id* – идентификатор VLAN;
- *ip-multicast-address* – IP-адрес многоадресной рассылки;
- *number* – указывает количество смежных IP адресов многоадресной передачи. Если параметр не указан, по умолчанию используется 1 адрес. Диапазон: 1 – 256.

Состояние по умолчанию:

Адреса не ассоциированы.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Команда применяется для задания многоадресной передачи через многоадресную TV VLAN.
2. Конфигурация применима только для порта, который является членом настроенной VLAN, в качестве многоадресной TV VLAN.
3. Если сообщение IGMP получено на таком порту, то оно связывается с TV VLAN только в том случае, если оно относится к одному из указанных IP адресов.
4. Может быть сконфигурировано до 256 VLAN.

Пример:

```
console(config)# ip igmp snooping vlan 2 multicast-tv 239.2.2.2  
count 3
```

14.8. Команда ip igmp snooping map cpe vlan

Команда **ip igmp snooping map cpe vlan** предназначена для ассоциирования CPE (Customer Premises Equipment) VLAN к многоадресной TV VLAN. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip igmp snooping map cpe vlan *cpe-vlan-id* multicast-tv vlan *vlan-id*

no ip igmp snooping map cpe vlan *vlan-id*

Параметры:

- *cpe-vlan-id* – идентификатор CPE VLAN;
- *vlan-id* – идентификатор TV VLAN.

Состояние по умолчанию:

Не ассоциировано.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Если сообщение IGMP получено на порт являющийся членом CPE VLAN, то оно ассоциируется с многоадресным TV VLAN.

Пример:

```
console(config)# ip igmp snooping map cpe vlan 2 multicast-tv vlan
31
```

14.9. Команда ip igmp snooping querier

Команда **ip igmp snooping querier** предназначена для глобального включения IGMP snooping querier. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip igmp snooping querier

no ip igmp snooping querier

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Включено.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Чтобы разрешить данную функцию на VLAN, необходимо предварительно включить ее глобально.

Пример:

```
console(config)# ip igmp snooping querier
```

14.10. Команда ip igmp snooping vlan querier

Команда **ip igmp snooping vlan querier** предназначена для включения IGMP Snooping querier на заданной VLAN. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip igmp snooping vlan *vlan-id* querier

no ip igmp snooping vlan *vlan-id* querier

Параметры:

- *vlan-id* – идентификатор vlan.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Данную функцию можно включить на VLAN только в том случае, если на этой VLAN включен режим IGMP Snooping.

Пример:

```
console(config)# ip igmp snooping vlan 2 querier
```

14.11. Команда ip igmp snooping vlan querier address

Команда **ip igmp snooping vlan querier address** предназначена для указания IP адреса который используется для функции IGMP Snooping querier. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

ip igmp snooping vlan *vlan-id* querier address *ip-address*

no ip igmp snooping vlan *vlan-id* querier address

Параметры:

- *vlan-id* – идентификатор VLAN;
- *ip-address* – IP-адрес источника.

Состояние по умолчанию:

Если IP адрес сконфигурирован для VLAN, он используется как адрес источника IPGM Snooping querier. Если IP адресов несколько, то используется минимальный IP адрес заданный в VLAN.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Если IP адрес не задан этой командой, а на VLAN не сконфигурирован ни один IP адрес, то данная функция отключена.

Пример:

```
console(config)# ip igmp snooping vlan 2 querier address  
172.16.0.23
```

14.12. Команда `ip igmp snooping vlan querier election`

Команда **`ip igmp snooping vlan querier election`** предназначена для включения механизма выбора IGMP Querier для IGMP Snooping на заданной VLAN. Использование префикса «**no**» выключает этот механизм.

Синтаксис:

`ip igmp snooping vlan vlan-id querier election`

`no ip igmp snooping vlan vlan-id querier election`

Параметры:

- *vlan-id* – идентификатор VLAN.

Состояние по умолчанию:

Включено.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Если включен механизм выбора IGMP Querier, запрос IGMP Snooping поддерживает стандартный механизм выборов IGMP Querier, указанный в RFC2236 и RFC3376.
2. Если механизм выборов IGMP Querier отключен, IGMP Snooping Querier задерживает отправку сообщений общего запроса в течение 60 секунд с момента его включения. В течение этого времени, если коммутатор не получил запрос IGMP от другого Querier, он начинает отправлять сообщения общего запроса. Когда коммутатор действует как Querier, он прекратит отправку сообщений общего запроса, если он обнаружит другой Querier в VLAN. В этом случае коммутатор возобновит отправку сообщений общего запроса, если он примет другой запрос Querier for Query Passive, равный $\langle \text{Robustness} \rangle * \langle \text{Query Interval} \rangle + 0.5 * \langle \text{Query Response Interval} \rangle$.
3. Конфигурирование этих параметров описано в командах **`ip igmp robustness`**, **`ip igmp query-interval`**, и **`ip igmp query-max-response-time`**.
4. Рекомендуется отключить механизм IGMP Querier, если в сети VLAN есть многоадресный маршрутизатор PIM.

Пример:

```
console(config)# no ip igmp snooping vlan 2 querier election
```

14.13. Команда `ip igmp snooping vlan querier version`

Команда **`ip igmp snooping vlan querier version`** предназначена для указания версии IGMP в IGMP Snooping querier в заданной VLAN. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

ip igmp snooping vlan *vlan-id* querier version { 2 | 3 }

no ip igmp snooping vlan *vlan-id* querier version

Параметры:

- *vlan-id* – идентификатор VLAN;
- **version** – указание используемой версии IGMP (2 или 3).

Состояние по умолчанию:

Используется версия IGMP 2

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip igmp snooping vlan 2 querier version 3
```

14.14. Команда ip igmp snooping vlan immediate-leave

Команда **ip igmp snooping vlan immediate-leave** предназначена для включения функции мгновенного отключения IGMP Snooping на заданной VLAN. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

ip igmp snooping vlan *vlan-id* immediate-leave

no ip igmp snooping vlan *vlan-id* immediate-leave

Параметры:

- *vlan-id* – идентификатор VLAN.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Перед выполнением команды предварительно создать необходимо VLAN.

Пример:

```
console(config)# ip igmp snooping vlan 2 immediate-leave
```


14.15. Команда show ip igmp snooping cpe vlans

Команда **show ip igmp snooping cpe vlans** предназначена для отображения информации CPE VLAN ассоциированного с многоадресной TV VLAN.

Синтаксис:

show ip igmp snooping cpe vlans [vlan *vlan-id*]

Параметры:

- *vlan-id* – идентификатор VLAN

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip igmp snooping cpe vlans

  CPE VLAN      multicast TV VLAN
-----
          2              31
```

14.16. Команда show ip igmp snooping groups

Команда **show ip igmp snooping groups** предназначена для отображения на экране информации о группах многоадресной рассылки непосредственно подключенные к устройству и обнаруженные с помощью IGMP.

Синтаксис:

show ip igmp snooping groups [vlan *vlan-id*] [address *ip-multicast-address*] [source *ip-address*]

Параметры:

- *vlan-id* – идентификатор VLAN ;
- *ip-multicast-address* – заданный адрес многоадресной рассылки;
- *ip-address* – заданный адрес источника.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Для отображения всех групп многоадресной рассылки обнаруженных с помощью IGMP необходимо использовать команду без параметров.
2. Для просмотра полной таблицы адресов многоадресной рассылки (включая статические адреса) применяется команда **show bridge multicast address-table**.

Пример:

```
console# show ip igmp snooping groups

Vlan   Group          Source          Include Ports   Exclude Ports
Comp.
      Address      Address
Mode
-----
2      239.255.255.250 *          tel1/0/1
v2

IGMP Reporters that are forbidden statically:

Vlan   Group          Source          Ports
      Address      Address
-----
```

14.17. Команда show ip igmp snooping interface

Команда **show ip igmp snooping interface** предназначена для отображения информации о конфигурации IGMP Snooping на указанной VLAN.

Синтаксис:

show ip igmp snooping interface *vlan-id*

Параметры:

- *vlan-id* – идентификатор VLAN.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip igmp snooping interface 2

IGMP Snooping is globally enabled
IGMP Snooping Querier is globally enabled
VLAN 2
  IGMP Snooping is enabled
  IGMP snooping last immediate leave: enable
  Automatic learning of Multicast router ports is enabled
  IGMP Snooping Querier is enabled
  IGMP Snooping Querier operation state: is not running
  IGMP Snooping Querier version: 3
  IGMP Snooping Querier election is disabled
  IGMP Snooping Querier address : 172.16.0.23
  IGMP snooping robustness: admin 2 oper 2
  IGMP snooping query interval: admin 125 sec oper 125 sec
  IGMP snooping query maximum response: admin 10 sec oper 10 sec
```

```
IGMP snooping last member query counter: admin 2 (default) oper 2
IGMP snooping last member query interval: admin 1000 msec oper
1000 msec

Groups that are in IGMP version 2 compatibility mode:
Groups that are in IGMP version 1 compatibility mode:
```

14.18. Команда show ip igmp snooping mrouter

Команда **show ip igmp snooping mrouter** предназначена для отображения на экране информации о динамически изученных интерфейсах маршрутизатора многоадресной передачи для всех VLAN или указанной.

Синтаксис:

show ip igmp snooping mrouter [interface *vlan-id*]

Параметры:

- *vlan-id* – идентификатор VLAN.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip igmp snooping mrouter

Vlan      Dynamic                Static                Forbidden
-----
-
  2    tel1/0/1                tel1/0/2
```

14.19. Команда show ip igmp snooping multicast-tv

Команда **show ip igmp snooping multicast-tv** предназначена для отображения IP-адресов ассоциированных с многоадресными TV VLAN.

Синтаксис:

show ip igmp snooping multicast-tv [vlan *vlan-id*]

Параметры:

- *vlan-id* – идентификатор VLAN.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip igmp snooping multicast-tv
```

VLAN	IP Address
2	239.2.2.2
2	239.2.2.3
2	239.2.2.4

15. КОМАНДЫ IP АДРЕСАЦИИ (IP АДРЕСАЦИЯ И ИНТЕРФЕЙСЫ ВТОРОГО УРОВНЯ)

IP адреса могут быть настроены на следующих интерфейсах второго уровня:

- Ethernet port
- Port Channel
- VLAN
- Loopback port
- OOB port.

15.1. Команда ip address

Команда **ip address** предназначена для назначения IP адреса на интерфейсе. Использование префикса «**no**» удаляет адрес.

Синтаксис:

Для порта OOB:

```
ip address ip-address { mask | !prefix-length } [ default-gateway-ip-address ]
```

```
no ip address
```

Для остальных интерфейсов:

```
ip address ip-address { mask | !prefix-length }
```

```
no ip address [ ip-address ]
```

Параметры:

- *ip-address* – IP адрес назначаемый на интерфейс;
- *mask* – маска подсети для заданного адреса;
- *prefix-length* – префикс IP адреса. Задается после косой черты (/). Диапазон: 8 – 30;
- *default-gateway-ip-address* – шлюз по умолчанию для указанного IP адреса. Маршрут получит метрику 2 для OOB интерфейса и 6 для всех остальных.

Состояние по умолчанию:

IP адреса не назначены.

Режим ИКС:

Режим конфигурации интерфейса

Примечание:

Команда используется для назначения статических IP адресов на интерфейсе.

Встроенные интерфейсы:

1. Имеется поддержка нескольких IP адресов на одном интерфейсе. Задание нового IP адреса добавляет его на интерфейс.

2. Задание статического IP адреса останавливает работу клиента DHCP на интерфейсе и удаляет IP-адрес назначенный DHCP.
3. Если заданный IP-адрес дублирует существующий на другом интерфейсе, то будет выдано предупреждение. Для изменения существующего IP-адреса необходимо удалить существующий и задать новый.

ООВ интерфейс:

1. Поддерживается только один IP-адрес. Новый IP-адрес заданный на порту ООВ переопределяет старый.
2. Задание статического IP адреса останавливает работу клиента DHCP на интерфейсе и удаляет IP-адрес назначенный DHCP.

Пример:

```
console(config)# interface vlan 2  
console(config-if)# ip address 172.21.0.23 /24
```

15.2. Команда ip address dhcp

Команда **ip address dhcp** предназначена для включения DHCP клиента. Использование префикса «**no**» отключает клиент и освобождает IP адрес.

Синтаксис:

ip address dhcp

no ip address dhcp

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Режим конфигурации интерфейса

Примечания:

1. Данная команда включает DHCP-клиент на интерфейсе.
2. Выполнение команды удаляет все статические IP-адреса настроенные на интерфейсе ранее.
3. Маршруту по умолчанию (Default Gateway), принятому от DHCP в Option 3 присваивается метрика 8 для внутренних интерфейсов и 4 для ООВ порта.

Пример:

```
console(config)# interface vlan 1  
console(config-if)# ip address dhcp
```

15.3. Команда `renew dhcp`

Команда **renew dhcp** предназначена для обновления IP-адреса на заданном интерфейсе, полученного от DHCP сервера.

Синтаксис:

renew dhcp *interface-id* [**force-autoconfig**]

Параметры:

- *interface-id* – идентификатор интерфейса;
- **force-autoconfig** – если DHCP-сервер для назначенного IP-адреса содержит Option 67, то конфигурация устройства перезаписывается.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Данная команда не включает DHCP клиент на интерфейсе и если клиент не включен, то будет возвращена ошибка.

Пример:

```
console# renew dhcp vlan 1
```

15.4. Команда `ip default-gateway`

Команда **ip default-gateway** предназначена для задания шлюза по умолчанию для устройства. Использование префикса `no` устанавливает значение по умолчанию.

Синтаксис:

ip default-gateway *ip-address*

no ip default-gateway [*ip-address*]

Параметры:

- *ip-address* – IP адрес шлюза.

Состояние по умолчанию:

Шлюз не задан.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Для шлюза подключенного к внутреннему интерфейсу маршрут добавляется с метрикой 6 и для шлюза подключенного к ООБ с метрикой 2.
2. Использование команды **no ip default-gateway** без указания IP-адреса шлюза удаляет все заданные шлюзы на коммутаторе.

Пример:

```
console(config)# ip default-gateway 172.18.39.1
```

15.5. Команда show ip interface

Команда **show ip interface** предназначена для отображения на экране статуса настроенных IP интерфейсов.

Синтаксис:

show ip interface [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса.

Состояние по умолчанию:

Отображаются все IP адреса настроенные на интерфейсах

Режим ИКС:

Пользовательский режим управления.

Пример:

```
console# show ip interface

      IP Address      I/F    I/F Status  Type  Directed  Prec
Redirect Status
-----
admin/oper          Broadcast
-----
-----
192.168.2.137/24    vlan 1  UP/UP       DHCP  disable   No
enable Valid
172.18.0.23/24     vlan 2  UP/DOWN     Static disable   No
enable Valid
```

15.6. Команда arp

Команда **arp** предназначена для добавления статической записи в ARP кэш. Использование префикса «**no**» удаляет запись.

Синтаксис:

arp ip-address mac-address [*interface-id*]

no arp ip-address

Параметры:

- *ip-address* – IP-адрес сопоставляемый с MAC-адресом;
- *mac-address* – MAC-адрес для указанного IP-адреса;

- *interface-id* – идентификатор интерфейса.

Состояние по умолчанию:

Статические записи отсутствуют.

Если идентификатор интерфейса опущен, то адресная пара применяется для всех интерфейсов.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Программное обеспечение коммутатора использует записи ARP кэша для трансляции 32-битных IP-адресов в 48-битные аппаратные (MAC) адреса. Поскольку большинство узлов поддерживает динамическую трансляцию адресов, статические записи ARP кэша обычно указывать не требуется.

Пример:

```
console(config)# arp 192.168.0.123 00:00:0c:40:0f:bc vlan 2
```

15.7. Команда `arp timeout` (Global)

Команда **arp timeout** (Global) предназначена для задания временного интервала, в течение которого запись остается в ARP кэше. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

arp timeout *seconds*

no arp timeout

Параметры:

- *seconds* – временной интервал (в секундах). Диапазон: 1 – 40000000.

Состояние по умолчанию:

По умолчанию временной интервал составляет 60000 секунд, если маршрутизация разрешена и 300 секунд, если маршрутизация отключена.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# arp timeout 12000
```

15.8. Команда ip arp proxy disable

Команда **ip arp proxy disable** предназначена для отключения прокси ARP на устройстве. Использование префикса «**no**» разрешает использование прокси.

Синтаксис:

ip arp proxy disable

no ip arp proxy disable

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Прокси ARP разрешен.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Выполнение команды отключает возможность использования прокси ARP на интерфейсе.
2. Команда поддерживается только когда разрешена IP маршрутизация.

Пример:

```
console(config)# ip arp proxy disable
```

15.9. Команда ip proxy-arp

Команда **ip proxy-arp** предназначена для включения прокси ARP на заданном интерфейсе. Использование префикса «**no**» отключает интерфейс.

Синтаксис:

ip proxy-arp

no ip proxy-arp

Состояние по умолчанию:

Прокси ARP выключен на интерфейсах.

Режим ИКС:

Режим конфигурации интерфейса

Примечание:

Конфигурация может быть применена только когда на интерфейсе задан хотя бы один IP-адрес.

Пример:

```
console(config)# interface gil/0/23  
console(config-if)# ip proxy-arp
```

15.10. Команда clear arp-cache

Команда **clear arp-cache** предназначена для удаления всех динамических записей в ARP кэше.

Синтаксис:

clear arp-cache

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear arp-cache
```

15.11. Команда show arp

Команда **show arp** предназначена для отображения на экране всех записей ARP таблицы.

Синтаксис:

show arp [ip-address ip-address] [mac-address mac-address] [interface-id]

Параметры:

- *ip-address* – IP-адрес в ARP таблице;
- *mac-address* – MAC-адрес в ARP таблице;
- *interface-id* – идентификатор интерфейса.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Поскольку связанный с интерфейсом MAC-адрес может устареть и быть удаленным из FDB таблицы, то идентификатор интерфейса может быть пустым.
2. Если ARP-запись связана с интерфейсом определенным как Ethernet-интерфейс или port channel, то идентификатор VLAN может быть пустым.

Пример:

```
console# show arp  
  
Total number of entries: 1  
  
      VLAN      Interface      IP address      HW address  
status
```

vlan 1	gi1/0/23	10.7.23.1	04:62:73:6d:43:4c	dynamic

15.12. Команда show arp configuration

Команда **show arp configuration** предназначена для отображения на экране информации о конфигурации ARP протокола.

Синтаксис:

show arp configuration

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show arp configuration

Global configuration:
    ARP Proxy:    disabled
    ARP timeout:  12000 Seconds

Interface configuration:
VLAN 1:
    ARP Proxy:    enabled
    ARP timeout:  12000 Seconds (Global)
VLAN 2:
    ARP Proxy:    enabled
    ARP timeout:  12000 Seconds (Global)
```

15.13. Команда interface ip

Команда **interface ip** предназначена для перехода в режим конфигурации IP интерфейса.

Синтаксис:

interface ip *ip-address*

Параметры:

- *ip-address* – один из IP адресов устройства.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# interface ip 172.23.14.25
```

15.14. Команда `ip helper-address`

Команда **ip helper-address** предназначена для включения пересылки широковещательных UDP пакетов, полученных интерфейсе, на заданный (*helper*) адрес. Использование префикса «**no**» отключает пересылку.

Синтаксис:

ip helper-address { *ip-interface* | **all** } *address* [*udp-port-list*]

no ip helper-address { *ip-interface* | **all** } *address*

Параметры:

- *ip-interface* – заданный IP интерфейс;
- **all** – все интерфейсы;
- *address* – широковещательный адрес назначения или адрес узла-приемника UDP пакетов. Значение 0.0.0.0 указывает на то, что пересылка UDP пакетов не производится;
- *udp-port-list* – номер UDP порта для пересылки широковещательных пакетов. Диапазон: 1 – 65535. Может быть задан список портов, разделенных пробелами.

Состояние по умолчанию:

Пересылка широковещательных UDP пакетов не происходит.

Если параметр *udp-port-list* не задан, пакеты для сервисов по умолчанию пересылаются на указанный адрес (*helper*).

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Широковещательные пакеты перенаправляются с одного интерфейса на другой, на указанные UDP порты. По умолчанию, если номер UDP порта не указан, то устройство передает пакеты для следующих сервисов:
 - IEN-116 Name Service (порт 42);
 - DNS (порт 53);
 - NetBIOS Name Server (порт 137);
 - NetBIOS Datagram Server (порт 138);
 - TACACS Server (порт 49);
 - Time Service (порт 37).
2. Может быть определено несколько вспомогательных (*helper*) адресов, однако общее количество пар адрес-порт ограничено 128 на устройство.
3. Установка *helper* адреса для определенного интерфейса имеет приоритет над установкой одного адреса для всех интерфейсов. Пересылка BOOTP/DHCP (порты 67, 68) не может быть включена с помощью этой команды. Для включения пересылки BOOTP/DHCP служит команда **ip dhcp relay**.
4. Аргумент *ip-interface* не может быть применен к ООВ порту.

Пример:

```
console(config)# ip helper-address all 172.16.9.9 49 53 1 2
```

15.15. Команда show ip helper-address

Команда **show ip helper-address** предназначена для отображения на экране конфигурации вспомогательных (helper) IP-адресов.

Синтаксис:

show ip helper-address

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show ip helper-address

  Interface      Helper Address      Udp port
-----
All             172.16.9.9         1,2,49,53
```

15.16. Команда show ip dhcp client interface

Команда **show ip dhcp client interface** предназначена для отображения на экране информации об интерфейсе клиента DHCP.

Синтаксис:

show ip dhcp client interface [interface-id]

Параметры:

- *interface-id* – идентификатор интерфейса.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Если при задании команды идентификатор интерфейса опущен, то отображается информация обо всех интерфейсах, на которых включен DHCP-клиент.

Пример:

```
console# show ip dhcp client interface
vlan 1 is in client mode
Address: 10.38.112.137 Mask: 255.255.255.0 T1 900, T2 1575
Default Gateway: 10.38.112.1
DNS Servers: 10.0.0.12, 10.0.0.11
Host Name: console.domain.com
DNS Domain Name: domain.com
Configuration Server Addresses: 255.255.255.255
```

16. КОМАНДЫ IP МАРШРУТИЗАЦИИ НЕ ПРИВЯЗАННЫЕ К ПРОТОКОЛУ

16.1. Команда accept-lifetime

Команда **accept-lifetime** предназначена для установки временного периода, в течение которого ключ аутентификации, используемый для проверки подлинности принимаемых маршрутов, в цепочке ключей считается действительным. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

accept-lifetime *start-time* { **infinite** | *end-time* | **duration** *seconds* }

no accept-lifetime

Параметры:

- *start-time* – начало периода. Допускаются следующие варианты синтаксиса:
 - *hh:mm:ss month date year*;
 - *hh:mm:ss date month year*;
 - *hh* – часы (0-23);
 - *mm* – минуты (0-59);
 - *ss* – секунды (0-59);
 - *month* – первые три буквы названия месяца. Возможные значения: **Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec**;
 - *date* – дата (1-31);
 - *year* – год (2000-2037);

По умолчанию начало периода принимается за 1 января 2000 г.

- **infinite** – ключ действителен со времени старта и до бесконечности;
- *end-time* – окончание периода. Синтаксис аналогичный параметра *start-time*. По умолчанию параметр имеет значение **infinite**;
- **duration** *seconds* – продолжительность (в секундах) времени приема ключа. Диапазон: 1 – 2147483646.

Состояние по умолчанию:

По умолчанию период времени, в течение которого ключ аутентификации действителен установлен в Forever.

Определение Forever: начало периода - 1 января 2000 года, окончание периода – бесконечно.

Режим ИКС:

Режим конфигурации ключа в цепочке ключей

Примечания:

1. Коммутатор перепроверяет значение *start-time* независимо от того установлено ли системное время вручную или при помощи SNTP. По умолчанию значение Time-of-Date всегда является прошедшим временем.

2. Если проверка значения аргумента *start-time* была пройдена и аргумент окончания периода установлен в бесконечность (**infinite**), то ключ считается валидным, не зависимо от того задано ли время вручную или SNTP.
3. Если системное время не задано с вручную или SNTP, а аргумент окончания периода установлен с точным значением, отличного от бесконечного, то ключ считается истекшим.
4. Если срок действия ключа истек, то аутентификация будет завершена с ошибкой.

Пример:

```
console(config-keychain-key)# accept-lifetime 22:12:00 jul 10 2017
infinite
```

16.2. Команда directed-broadcast

Команда **directed-broadcast** предназначена для включения трансляции широковещательных пакетов на физический сегмент адресуемой сети. Использование префикса «**no**» отключает функцию.

Синтаксис:

directed-broadcast

no directed-broadcast

Состояние по умолчанию:

Трансляция широковещательных пакетов запрещена.

Все широковещательные передачи отбрасываются.

Режим ИКС:

Режим конфигурации интерфейса IP

Пример:

```
console(config)# interface ip 172.18.0.23
console(config-ip)# directed-broadcast
```

16.3. Команда ip redirects

Команда **ip redirects** предназначена для разрешения отправки сообщений ICMP-редиректа через тот же интерфейс, на который был получен пакет. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip redirects

no ip redirects

Состояние по умолчанию:

Отправка разрешена.

Режим ИКС:

Режим конфигурации интерфейса IP

Пример:

```
console(config)# interface ip 172.18.0.23  
console(config-ip)# no ip redirects
```

16.4. Команда ip route

Команда **ip route** предназначена для добавления статического маршрута в таблицу маршрутизации. Использование префикса «**no**» удаляет маршрут из таблицы.

Синтаксис:

ip route *prefix* { *mask* | *lprefix-length* } { *ip-address* [**metric** *value*] | **reject-route** }

no ip route *prefix* { *mask* | *lprefix-length* } [*ip-address*]

Параметры:

- *prefix* – подсеть назначения;
- *mask* – сетевая маска подсети назначения;
- *lprefix-length* – префикс подсети назначения. Диапазон: 0 – 32;
- *ip-address* – IP-адрес следующего перехода, который можно использовать для доступа к этой подсети;
- **metric value** – метрика маршрута. По умолчанию для внутренних интерфейсов применяется метрика 6, для ООВ порта – метрика 2. Диапазон: 1 – 255;
- **reject-route** – запрещает маршрутизацию в целевую подсеть через все шлюзы.

Состояние по умолчанию:

Статические маршруты не заданы.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# ip route 172.18.0.0 /24 172.18.1.1
```

16.5. Команда ip routing

Команда **ip routing** предназначена для включения функции маршрутизации на коммутаторе. Использование префикса «**no**» отключает функцию.

Синтаксис:

ip routing

no ip routing

Состояние по умолчанию:

Маршрутизация отключена.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Коммутатор поддерживает один IPv4 стек на внутренних портах и ООВ порту.
2. IP-стек всегда работает на ООВ порту, независимо от того включена IP-маршрутизация или нет.
3. Коммутатор блокирует маршрутизацию между внутренними портами и портом ООВ.
4. В случае, когда есть два равнозначных маршрута – один через внутренний интерфейс и один через порт ООВ, коммутатор будет использовать маршрут через ООВ интерфейс.
5. DHCP Relay и IP Helper не могут быть включены на ООВ порту.
6. Протоколы маршрутизации не могут быть активированы на ООВ порту.
7. IP-подсеть заданная на порту ООВ не перераспределяется на протоколы маршрутизации работающие на внутренних интерфейсах.

Пример:

```
console(config)# ip routing
```

16.6. Команда key-string

Команда **key-string** предназначена для задания строки аутентификации для ключа. Использование префикса «**no**» удаляет строку.

Синтаксис:

key-string *text*

no key-string

Параметры:

- *text* – строка аутентификации. Длина: 1 – 16 символов.

Состояние по умолчанию:

Ключи не заданы.

Режим ИКС:

Режим конфигурации ключа в цепочке ключей

Пример:

```
console(config)# key chain chain1
console(config-keychain)# key 1
console(config-keychain-key)# key-string keyOne
console(config-keychain-key)# accept-lifetime 12:30:00 jun 1 2018
duration 7200
```

```
console(config-keychain-key)# send-lifetime 14:00:00 jun 1 2018
duration 3600
```

16.7. Команда `key` (`key-chain`)

Команда **key** (`key-chain`) предназначена для идентификации ключа в цепочке ключей. Использование префикса **no** удаляет ключ из цепочки.

Синтаксис:

key *key-id*

no key *key-id*

Параметры:

- *key-id* – идентификационный номер ключа аутентификации в цепочке ключей. Диапазон: 1 – 255. Идентификационные номера ключей не обязательно должны быть последовательными. Идентификационный номер действует только в рамках цепочки ключей, где ключ определен.

Состояние по умолчанию:

Ключи не заданы в цепочке ключей.

Режим ИКС:

Режим конфигурации цепочки ключей

Примечания:

1. Рекомендуется иметь несколько ключей в цепочке ключей. В этом случае ПО коммутатора может использовать их последовательно, поскольку некоторые из ключей могут стать не действительными по окончании времени заданного командами **accept-lifetime** и **send-lifetime**.
2. Каждый ключ имеет собственный идентификатор, который хранится локально. Сочетание идентификатора ключа и номера интерфейса уникальным образом идентифицируют алгоритм аутентификации и используемый ключ. Не зависимо от количества действительных ключей, посылается только один пакет аутентификации. ПО коммутатора перебирает ключи начиная с самого низкого номера и использует первый действительный ключ.
3. Если действие ключа закончилось, то аутентификация будет завершена с ошибкой.
4. Для удаления всех ключей в цепочке применяется команда **no key chain** без параметров.

Пример:

```
console(config)# key chain chain1
console(config-keychain)# key 1
console(config-keychain-key)# key-string keyOne
console(config-keychain-key)# accept-lifetime 12:30:00 jun 1 2018
duration 7200
console(config-keychain-key)# send-lifetime 14:00:00 jun 1 2018
duration 3600
```

```
console(config-keychain-key)# exit
console(config-keychain)# key 2
console(config-keychain-key)# key-string keyTwo
console(config-keychain-key)# accept-lifetime 12:30:00 sep 1 2018
duration 6800
console(config-keychain-key)# send-lifetime 13:00:00 sep 1 2018
duration 3600
```

16.8. Команда key chain

Команда **key chain** предназначена для включения режима аутентификации для протоколов маршрутизации и задает цепочку ключей. Использование префикса «**no**» удаляет цепочку.

Синтаксис:

key chain *name-of-chain*

no key chain *name-of-chain*

Параметры:

- *name-of-chain* – имя цепочки ключей. Диапазон: 1 – 32 символа. Одна цепочка может содержать до 256 ключей.

Состояние по умолчанию:

Цепочка ключей не задана.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Для включения аутентификации необходимо предварительно настроить цепочку ключей.
2. Хотя имеется возможность настроить несколько цепочек ключей рекомендуется использовать одну цепочку на один протокол маршрутизации.
3. После выполнения данной команды, коммутатор переходит в режим конфигурации цепочки ключей.

Пример:

```
console(config)# key chain chain1
console(config-keychain)# key 1
console(config-keychain-key)# key-string keyOne
console(config-keychain-key)# accept-lifetime 12:30:00 jun 1 2018
duration 7200
console(config-keychain-key)# send-lifetime 14:00:00 jun 1 2018
duration 3600
console(config-keychain-key)# exit
console(config-keychain)# key 2
console(config-keychain-key)# key-string keyTwo
console(config-keychain-key)# accept-lifetime 12:30:00 sep 1 2018
duration 6800
```

```
console(config-keychain-key)# send-lifetime 13:00:00 sep 1 2018
duration 3600
console(config-keychain-key)# exit
console(config-keychain)# exit
console(config)# interface ip 172.18.0.23
console(config-ip)# rip
console(config-ip)# rip authentication md5 chain1
```

16.9. Команда send-lifetime

Команда **send-lifetime** предназначена для установки временного периода, в течение которого ключ аутентификации действителен для отправки. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

send-lifetime *start-time* { **infinite** | *end-time* | **duration** *seconds* }

no send-lifetime

Параметры:

- *start-time* – начало периода. Допускаются следующие варианты синтаксиса:
 - *hh:mm:ss month date year*;
 - *hh:mm:ss date month year*;
 - *hh* – часы (0-23);
 - *mm* – минуты (0-59);
 - *ss* – секунды (0-59);
 - *month* – первые три буквы названия месяца. Возможные значения: **Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec**;
 - *date* – дата (1-31);
 - *year* – год (2000-2037);

По умолчанию начало периода принимается за 1 января 2000 г.

- **infinite** – ключ действителен со времени старта и до бесконечности;
- *end-time* – окончание периода. Синтаксис аналогичный параметра *start-time*. По умолчанию параметр имеет значение **infinite**;
- **duration** *seconds* – продолжительность (в секундах) времени приема ключа. Диапазон: 1 – 2147483646.

Состояние по умолчанию:

По умолчанию время действия ключа не ограничено.

Действие ключа начинается с 1 января 2000 года.

Режим ИКС:

Режим конфигурации ключа в цепочке ключей

Примечания:

1. Необходимо указать время старта периода и одно из конечных значений: **infinite**, *end-time* или **duration**.

2. Если системное время не установлено вручную или с помощью SNTP, то ключ считается не действительным.
3. По истечении срока действия ключа аутентификация будет завершаться с ошибкой.

Пример:

```
console(config)# key chain chain1
console(config-keychain)# key 1
console(config-keychain-key)# key-string keyOne
console(config-keychain-key)# accept-lifetime 12:30:00 jun 1 2018
duration 7200
console(config-keychain-key)# send-lifetime 14:00:00 jun 1 2018
duration 3600
console(config-keychain-key)# exit
```

16.10. Команда show ip protocols

Команда **show ip protocols** предназначена для отображения на экране статус и параметры протоколов маршрутизации IP.

Синтаксис:

show ip protocols

Режим ИКС:

Привилегированный режим управления.

Примечание:

Информация отображаемая данной командой полезна при отладке маршрутизации.

Пример:

```
console# show ip protocols

Routing Protocol is "rip"
Sending updates every 30 seconds
Invalid after 180 seconds, hold down 120, flushed after 300
Redistributing: RIP
Default version control: send version 1, receive version 1
Interfaces:
  Interface          Send      Receive   Key-chain
-----
Routing Information Sources:
  Gateway            Last Update
-----

Preference: 120

Routing Protocol is "ospf"
Redistributing: OSPF
```

```
Interfaces:

  Interface      Metric      Key-chain
  -----
Routing Information Sources:

  Gateway      State
  -----

External Preference: 110
Internal Preference: 110

Routing Protocol is "BGP"
BGP process is deactivated
No BGP router is currently configured
Neighbor(s):
Peer          AS          RID
Announced network(s):
```

16.11. Команда show ip route

Команда **show ip route** предназначена для отображения на экране текущей таблицы маршрутизации.

Синтаксис:

```
show ip route [ ip-address mask [ longer-prefixes ] ] [ rip | ospf [ process-id ] | static | rejected | icmp | connected | summary ]
```

Параметры:

- *ip-address* – IP-адрес о котором должна быть отображена информация о маршрутизации;
- *mask* – маска подсети данного адреса;
- **longer-prefixes** – отображаются маршруты на префиксы, покрываемые указанным префиксом
- **rip** – отображаются маршруты добавленные протоколом RIP;
- **ospf** – Маршруты добавленные протоколом OSPF. *process-id* идентифицирует процесс OSPF;
- **connected** – прямые маршруты;
- **icmp** – маршруты добавленные ICMP Direct;
- **rejected** – отклоненные маршруты;
- **summary** – выводит текущее содержимое таблицы маршрутизации в кратком формате.

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1. Вывод команды **show ip route** при отключенной маршрутизации.

```
console# show ip route
Maximum Parallel Paths: 4 (4 after reset)
IP Forwarding: disabled
Codes: > - best, C - connected, S - static,
       R - RIP,
       O - OSPF intra-area, OIA - OSPF inter-area,
       OE1 - OSPF external 1, OE2 - OSPF external 2,
       B - BGP

S 10.10.0.0/16 [1/2] via 10.119.254.244, 00:02:22, vlan2
S 10.10.0.0/16 [1/1] via 10.120.254.244, 00:02:22, vlan3
S 10.16.2.0/24 [1/1] via 10.119.254.244, 00:02:22, vlan2
C 10.119.0.0/16 is directly connected, vlan2
C 10.120.0.0/16 is directly connected, vlan3
```

Пример 2. Вывод команды **show ip route** при включенной маршрутизации.

```
console# show ip route
Maximum Parallel Paths: 4 (4 after reset)
IP Forwarding: enabled
Codes: > - best, C - connected, S - static,
       R - RIP,
       O - OSPF intra-area, OIA - OSPF inter-area,
       OE1 - OSPF external 1, OE2 - OSPF external 2,
       B - BGP

R 10.7.10.0/24 [120/5] via 10.119.254.244, 00:02:22, vlan2
O 10.10.0.0/16 [10/128] via 10.119.254.244, 00:02:22, vlan2
O 10.10.0.0/16 [10/128] via 10.120.254.244, 00:02:22, vlan3
O 10.16.2.0/24 [110/128] via 10.119.254.244, 00:02:22, vlan2
O 10.16.2.64/26 [110/128] via 10.119.254.244, 00:02:22, vlan2
O 10.16.2.64/26 [110/130] via 10.119.254.244, 00:02:22, vlan3
O 10.16.2.128/26 [110/128] via 10.119.254.244, 00:02:22, vlan2
O 10.16.208.0/24 [110/128] via 10.120.254.244, 00:02:22, vlan2
O 10.16.223.0/24 [110/128] via 10.119.254.244, 00:02:22, vlan2
O 10.16.236.0/24 [110/129] via 10.119.254.240, 00:02:23, vlan2
OE2 10.68.132.0/24 [110/5] via 10.119.254.6, 00:00:59, vlan2
O 10.75.139.0/24 [110/129] via 10.119.254.240, 00:02:23, vlan2
O 10.84.148.0/24 [110/129] via 10.119.254.240, 00:02:23, vlan2
OE2 10.110.0.0/24 [110/128] via 10.119.254.6, 00:01:00, vlan1
O 10.128.0.0/16 [110/128] via 10.119.254.244, 00:02:22, vlan2
O 10.129.0.0/16 [110/129] via 10.119.254.240, 00:02:02, vlan2
O 10.140.0.0/16 [110/129] via 10.119.254.240, 00:02:23, vlan2
O 10.141.0.0/16 [110/129] via 10.119.254.240, 00:02:22, vlan2
S 10.175.0.0/16 [1/1] via 10.119.254.240, 00:02:22, vlan2
S 10.180.0.0/16 [1/1] via 10.119.254.240, 00:02:42, vlan3
C 10.119.0.0/16 is directly connected, vlan2
C 10.120.0.0/16 is directly connected, vlan3
```


Пример 3. Вывод команды **show ip route** с параметром **longer-prefixes**.

```
console# show ip route 10.16.0.0 255.255.0.0 longer-prefixes
Maximum Parallel Paths: 4 (4 after reset)
IP Forwarding: enabled
Codes: > - best, C - connected, S - static,
       R - RIP,
       O - OSPF intra-area, OIA - OSPF inter-area,
       OE1 - OSPF external 1, OE2 - OSPF external 2,
       B - BGP

S 10.16.2.0/24 [1/1] via 10.119.254.244, 00:02:22, vlan2
S 10.16.2.64/26 [1/1] via 100.1.14.244, 00:02:22, vlan1
S 10.16.2.128/26 [1/1] via 110.9.2.2, 00:02:22, vlan3
S 10.16.208.0/24 [1/1] via 120.120.5.44, 00:02:22, vlan2
S 10.16.223.0/24 [1/1] via 20.1.2.24, 00:02:22, vlan5
S 10.16.236.0/24 [1/1] via 30.19.54.240, 00:02:23, vlan6
```

Пример 4. Вывод команды **show ip route** с параметром **summary**.

```
console# show ip route summary

IP Routing Table Summary - 2 entries
1 connected, 1 static
Number of prefixes:
/0: 1, /24: 1
```

16.12. Команда show key chain

Команда **show key chain** предназначена для отображения на экране информации о цепочке ключей аутентификации.

Синтаксис:

show key chain [*name-of-chain*]

Параметры:

- *name-of-chain* – имя цепочки ключей.

Состояние по умолчанию:

Отображается информация обо всех цепочках ключей.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show key chain
Current Time of Day is 15:36:51 May 30 2018
Key-chain 1:
  key 1 -- text  "SeYvuSa1PaICtOPGY/qI8myhhnKh2rogae5QbgGgf+k="
                accept lifetime (22:12:00 Jul 10 2017) - (forever)
```

```
send lifetime (always valid) - (always valid) [valid now]

Key-chain chain1:
  key 1 -- text (Encrypted) "OUNOvth-
jOqvuSYKeqP5mV4LYNFCEZgM59BnIiQnjBrk="
    accept lifetime (12:30:00 Jun 1 2018) - (14:30:00 Jun 1
2018)
      send lifetime (14:00:00 Jun 1 2018) - (15:00:00 Jun 1 2018)
    key 2 -- text (Encrypted)
"50mwZ/ENPfautWwkyBFPI569NzjHEp5wOSrfSnNveY4="
    accept lifetime (12:30:00 Sep 1 2018) - (14:23:20 Sep 1
2018)
      send lifetime (13:00:00 Sep 1 2018) - (14:00:00 Sep 1 2018)
```

17. КОМАНДЫ МНОГОАДРЕСНОЙ МАРШРУТИЗАЦИИ IPV4

17.1. Команда ip multicast-routing

Команда **ip multicast-routing** предназначена для включения многоадресной маршрутизации IPv4 на всех IP-интерфейсах и многоадресной переадресации. Использование префикса «**no**» отключает маршрутизацию и переадресацию.

Синтаксис:

ip multicast-routing [{ pim | igmp-proxy }]

no ip multicast-routing

Параметры:

- **pim** – многоадресная маршрутизация с использованием протокола PIM;
- **igmp-proxy** – многоадресная маршрутизация с использованием IGMP прокси.

Состояние по умолчанию:

Многоадресная маршрутизация запрещена.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Необходимо использование команды с параметром, чтобы указать необходимый IP протокол многоадресной маршрутизации.
2. Использование команды без параметра включает режим PIM.
3. Для переадресации многоадресных пакетов IPv4 на интерфейсе необходимо включить многоадресную маршрутизацию глобально, а на интерфейсе должен быть включен протокол маршрутизации PIMv4.

Пример:

```
console(config)# ip multicast-routing igmp-proxy
```

17.2. Команда ip multicast ttl-threshold

Команда **ip multicast ttl-threshold** предназначена для настройки порогового времени жизни (TTL) пакетов, отправляемых через интерфейс. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold

Параметры:

- *ttl-value* – пороговое время жизни, в промежуточных узлах. Диапазон: 0 – 256.

Состояние по умолчанию:

По умолчанию значение TTL равно 0.

Режим ИКС:

Режим конфигурации интерфейса

Примечания:

1. Многоадресные пакеты со значением TTL меньше установленного порогового значения не будут передаваться на интерфейс.
2. Значение по умолчанию (0) означает что все пакеты многоадресной передачи будут передаваться на интерфейс.
3. Значение 256 означает что многоадресные пакеты не будут передаваться на интерфейс.
4. Порог TTL необходимо настроить только на пограничных маршрутизаторах. И наоборот – маршрутизаторы на которых настраивается пороговое значение TTL автоматически становятся пограничными.

Пример:

```
console(config)# interface vlan 2
console(config-if)# ip multicast ttl-threshold 200
```

17.3. Команда show ip mroute

Команда **show ip mroute** предназначена для отображения на экране содержимого многоадресной таблицы маршрутизации (mroute).

Синтаксис:

show ip mroute [*group-address* [*source-address*]] [**summary**]

Параметры:

- *group-address* – многоадресный IP-адрес назначения;
- *source-address* – многоадресный IP-адрес источника;
- **summary** – отображает однострочное сокращенное резюме каждой записи в таблице.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Коммутатор заполняет таблицу маршрутизации многоадресной передачи, создавая записи (S, G) из записей (*, G). Звездочка (*) относится ко всем исходным адресам, «S» относится к одному исходному адресу, а «G» - это адрес целевой группы многоадресной рассылки. При создании (S, G) записей коммутатор использует наилучший путь к этой целевой группе, найденной в таблице маршрутизации Unicast (то есть путем перенаправления обратного пути [RPF])

Примеры:

Описание значимых полей в приведенных ниже примерах.

- **Флаг:**
 - **C** – Connected. Член группы многоадресной передачи присутствует на интерфейсе с прямым подключением.
 - **L** – Local. Данный маршрутизатор является членом группы многоадресной передачи.
 - **S** – Sparse. Маршрут находится в sparse режиме.
 - **s** – SSM Group. Указывает, что группа многоадресной рассылки находится в диапазоне IP-адресов SSM. Этот флаг сбрасывается, если диапазон SSM изменяется.
 - **R** – RP-bit set. Запись (S, G) указывает на RP. Этот флаг обычно указывает состояние «обрезки» вдоль общего дерева для определенного источника.
 - **F** – Register flag. Программное обеспечение регистрируется для источника многоадресной рассылки.
 - **T** – SPT-bit set. Указывает, что пакеты получены по кратчайшему пути.
 - **J** – Join SPT. Для записей (*, G) указывает, что скорость трафика, идущего вниз по общему дереву, превышает пороговое значение SPT-Threshold для группы. (Значение по умолчанию SPT-Threshold - 0 kbps.) Когда установлен флаг **J**-Join shortest tree (SPT), следующий (S, G) пакет, принятый по общему дереву, запускает соединение (S, G) в направлении источника, тем самым заставляя маршрутизатор присоединиться к исходному дереву. Для записей (S, G) указывает, что запись была создана, потому что превышен порог SPT для группы. Когда флаг **J**-Join SPT установлен для записей (S, G), маршрутизатор контролирует скорость трафика в дереве источников и пытается вернуться к общему дереву для этого источника, если скорость трафика в исходном дереве падает ниже SPT-Порог группы более 1 минуты.

Примечание. Маршрутизатор измеряет скорость трафика на общем дереве и сравнивает измеренную скорость с SPT-порогом группы раз в секунду. Если скорость трафика превышает порог SPT, флаг **J**-Join SPT устанавливается в записи (*, G) до следующего измерения скорости трафика. Флаг очищается, когда следующий пакет поступает на общее дерево, и начинается новый интервал измерения. Если для группы используется значение SPT-Threshold по умолчанию 0 Кбит/с, флаг **J**-Join SPT всегда устанавливается в (*, G) и никогда не очищается. Когда используется значение SPT-Threshold по умолчанию, маршрутизатор немедленно переключается на дерево кратчайшего пути при получении трафика из нового источника.

- **I** - Received Source Specific Host Report. Указывает, что запись (S, G) была создана в отчете (S, G). Этот (S, G) отчет мог быть создан протоколом IGMPv3, URD или IGMPv3lite. Этот флаг устанавливается только на назначенный маршрутизатор (DR).
- **Timers:Uptime/Expires** - Uptime указывает для каждого интерфейса, как долго (в часах, минутах и секундах) запись была в таблице маршрутизации IP-

многоадресной рассылки. Expires указывает для каждого интерфейса, как долго (в часах, минутах и секундах), как долго запись не будет удалена из таблицы маршрутизации многоадресной передачи IP.

- **(*, 224.0.255.1)** и **(192.168.37.100/32, 224.0.255.1)** - Запись состоит из IP-адреса исходного маршрутизатора, за которым следует IP-адрес группы многоадресной рассылки. Звездочка (*) вместо исходного маршрутизатора указывает все источники. Записи в первом формате называются (*, G) или «звездочка запятая G». Записи во втором формате называются (S, G) или «S запятая G». (*, G) используются для построения (S, G) записей.
- **Incoming interface:** - Предполагаемый интерфейс для пакета многоадресной передачи из источника. Если пакет не получен на этом интерфейсе, он отбрасывается.
- **RPF neighbor** или **RPF nbr** - IP-адрес восходящего маршрутизатора к источнику. Туннелирование указывает, что этот маршрутизатор отправляет данные в RP, инкапсулированные в пакеты регистров. Шестнадцатеричное число в круглых скобках указывает, в каком RP он регистрируется. Каждый бит указывает на другой RP, если используется несколько RP для каждой группы. Если после IP-адреса в этом поле появляется звездочка (*), сосед RPF узнается через assert.
- **Outgoing Interface List (OIF):** - интерфейсы через которые будут отправляться пакеты.

Пример 1. Вывод команды **show ip mroute** с параметром **summary**.

```
console# show ip mroute summary

Timers: Uptime/Expires

IP Multicast Routing Table
(172.16.160.67/32, 224.2.127.254), 00:02:46/00:00:12, OIF count:2
(172.16.244.217/32, 224.2.127.254), 00:02:15/00:00:40, OIF count:
(172.16.8.33/32, 224.2.127.254), 00:00:25/00:02:32, OIF count:2
(172.16.2.62/32, 224.2.127.254), 00:00:51/00:02:03, OIF count:2
(172.16.8.3/32, 224.2.127.254), 00:00:26/00:02:33, OIF count:2
(172.16.60.189/32, 224.2.127.254), 00:03:47/00:00:46, OIF count:2
```

Пример 2. Вывод команды **show ip mroute** при включенном IGMP Proxy.

```
console# show ip mroute

Timers: Uptime/Expires

IP Multicast Routing Table
(*, 224.0.255.3), 5:29:15/00:03:01
  Incoming interface: vlan2
  Outgoing interface list:
    vlan100, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), 05:29:15/00:02:59
  Incoming interface: vlan2
  Outgoing interface list:
```

```
vlan5, 05:29:15/00:02:57
```

Пример 3. Вывод команды `show ip mroute` при включенном PIM.

```
console# show ip mroute

Flags: C - Connected, L - Local,
       S - Sparse, s - SSM Group, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
Timers: Uptime/Expires

IP Multicast Routing Table
(*, 224.0.255.3), 05:29:15/00:03:23, RP is 192.168.37.2, flags: SC
  Incoming interface: vlan2, RPF neighbor 10.3.35.1
  Outgoing interface list:
    vlan100, 05:29:15/00:02:57
(192.168.46.0/24, 224.0.255.3), 05:29:15/00:02:59, flags: C
  Incoming interface: vlan2, RPF neighbor 10.3.35.1
  Outgoing interface list:
    vlan5, 05:29:15/00:02:57
```

Пример 3. Вывод команды `show ip mroute` с фильтром по групповому адресу 232.6.6.6 при включенном PIM.

```
console# show ip mroute 232.6.6.6

Flags: C - Connected, L - Local,
       S - Sparse, s - SSM Group, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
Timers: Uptime/Expires

IP Multicast Routing Table
(*, 232.6.6.6), 00:01:20/00:02:59, RP 224.0.0.0, flags: sSJP
  Incoming interface: Null, RPF nbr 224.0.0.0
  Outgoing interface list: Null
(10.2.2.2, 232.6.6.6), 00:01:20/00:02:59, flags: CTI
  Incoming interface: vlan33, RPF nbr 224.0.0.0
  Outgoing interface list:
    vlan30, 00:00:36/00:02:35
```

Пример 4. Вывод команды `show ip mroute` с параметром `summary` при включенном PIM.

```
console# show ip mroute summary

Flags: C - Connected, L - Local,
       S - Sparse, s - SSM Group, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
```

```
Timers: Uptime/Expires

IP Multicast Routing Table
(*, 224.255.255.255), 2d16h/00:02:30, RP 172.16.10.13, OIF count:1,
flags: SJ
(*, 224.2.127.253), 00:58:18/00:02:00, RP 172.16.10.13, OIF
count:2, flags: SJC
(*, 224.1.127.255), 00:58:21/00:02:03, RP 172.16.10.13, OIF
count:2, flags: SJ
(*, 224.2.127.254), 2d16h/00:00:00, RP 172.16.10.13, OIF count:2,
flags: SJCL
(172.16.160.67/32, 224.2.127.254), 00:02:46/00:00:12, OIF
count:2, flags: CLJT
(172.16.244.217/32, 224.2.127.254), 00:02:15/00:00:40, OIF
count:2, flags: CLJT
(172.16.8.33/32, 224.2.127.254), 00:00:25/00:02:32, OIF count:2,
flags: CLJT
(172.16.2.62/32, 224.2.127.254), 00:00:51/00:02:03, OIF count:2,
flags: CLJT
(172.16.8.3/32, 224.2.127.254), 00:00:26/00:02:33, OIF count:2,
flags: CLJT
(172.16.60.189/32, 224.2.127.254), 00:03:47/00:00:46, OIF
count:2, flags: CLJT
```

17.4. Команда show ip multicast

Команда **show ip multicast** предназначена для отображения на экране информации о конфигурации многоадресной рассылки IP.

Синтаксис:

show ip multicast [interface *interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса на котором настроена многоадресная передача.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Выполнение команды без параметров отображает общую информацию о состоянии многоадресной рассылки IP на маршрутизаторе.

Пример:

Пример 1. Вывод команды **show ip multicast** при выключенной многоадресной маршрутизации.

```
console# show ip multicast
IP Unicast Forwarding: enabled
IP Multicast Protocol: No
```


Пример 2. Вывод команды **show ip multicast** при включенном IGMP Proxy.

```
console# show ip multicast
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
```

Пример 3. Вывод команды **show ip multicast** с указанием интерфейса. На интерфейсе включен IGMP Proxy и он является восходящим интерфейсом.

```
console# show ip multicast interface vlan 200
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
vlan 200
  TTL-threshold: 0
  IGMP Protocol: IGMPv3
  PIM: disabled
  IGMP Proxy: Upstream
```

Пример 4. Вывод команды **show ip multicast** с указанием интерфейса. На интерфейсе включен IGMP Proxy и он является нисходящим интерфейсом.

```
console# show ip multicast interface vlan 100
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
vlan 200
  TTL-threshold: 0
  IGMP Protocol: IGMPv3
  PIM: disabled
  IGMP Proxy: DownStream (Upstream: vlan 200)
```

Пример 5. Вывод команды **show ip multicast** с указанием интерфейса. На интерфейсе выключен IGMP Proxy.

```
console# show ip multicast interface vlan 100
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
vlan 200
  IP Status: enabled
  hop-threshold: 100
  IGMP Protocol: IGMPv3
  PIM: disabled
  IGMP Proxy: disabled
```

Пример 6. Вывод команды **show ip multicast** с указанием интерфейса. На интерфейсе включен PIM.

```
console# show ip multicast interface vlan 100
IP Unicast Forwarding: enabled
IP Multicast Protocol: PIM
```

```
vlan 200
  IP Status: enabled
  hop-threshold: 100
  IGMP Protocol: IGMPv3
  IGMP Proxy: DownStream (Upstream: vlan 200)
```

18. СИСТЕМНЫЕ КОМАНДЫ УПРАВЛЕНИЯ IP

18.1. Команда `ping`

Команда **ping** предназначена для отправки ICMP echo-request пакетов на другой узел в сети.

Синтаксис:

```
ping [ ip ] { ipv4-address | hostname } [ size packet_size ] [ count packet_count ] [ timeout timeout ] [ source source-address ]
```

Параметры:

- **ip** – используется IPv4 для проверки соединения;
- *ipv4-address* – адрес в формате IPv4;
- *hostname* – сетевое имя узла. Длина: 1 – 160 символов. Максимальная длина части имени до точки – 58 символов;
- *packet_size* – Количество байт в пакете не считая тег VLAN. По умолчанию: 64 Б. Диапазон: IPv4: 64 – 1518;
- *packet_count* – количество пакетов для отправки. Диапазон: 1 – 65535. По умолчанию – 4 пакета. Если введено значение 0, то команда завершит работу после отправки 65535 пакетов;
- *timeout* – временной интервал (в миллисекундах) ожидания ответа. Диапазон: 50 – 65535. По умолчанию: 2000 миллисекунд;
- *source-address* – IP-адрес источника от которого отправляются пакеты.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Для остановки пинга необходимо нажать Esc. Ниже приведены примеры результатов выполнения команды:
 - **Destination does not respond** – удаленный узел не отвечает. Сообщение выводится, если в течение 10 секунд результат работы команды по `answer from host`.
 - **Destination unreachable** – ответ шлюза между отправителем и получателем запросов. Указывает на то, что заданный узел недоступен.
 - **Network or host unreachable** – коммутатор не нашел соответствующей записи о данном узле или сети в своей таблице.

Пример:

```
console# ping 10.3.2.1
Pinging 10.3.2.1 with 18 bytes of data:

18 bytes from 10.3.2.1: icmp_seq=1. time=10 ms
18 bytes from 10.3.2.1: icmp_seq=2. time=0 ms
18 bytes from 10.3.2.1: icmp_seq=3. time=10 ms
```

```
18 bytes from 10.3.2.1: icmp_seq=4. time=0 ms

----10.3.2.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/5/10
```

18.2. Команда `ssh`

Команда `ssh` предназначена для создания защищенного соединения с удаленным сетевым устройством.

Синтаксис:

```
ssh { ip-address | hostname } [ port ] [ keyword...]
```

Параметры:

- *ip-address* – IP-адрес назначения (IPv4 или IPv6);
- *hostname* – сетевое имя узла назначения. Длина: 1 – 160 символов. Максимальная длина части имени до точки – 58 символов;
- *port* – удаленный TCP-порт. По умолчанию порт используемый протоколом SSH – 22;
- *keyword* – одно или несколько ключевых слов. Ключевые слова перечислены в таблице ниже.

Таблица ключевых слов:

Ключевое слово	Описание
<code>/password password</code>	Задает пароль, используемый при входе в систему на удаленном сетевом устройстве, на котором запущен ssh-сервер. Если параметр не указан, то используется пароль, заданный командой <code>ip ssh-client password</code> . При задании данного параметра необходимо указать ключевое слово <code>/user</code> .
<code>/source-interface interface-id</code>	Задает исходящий интерфейс, в котором минимальный IP адрес будет использоваться в качестве исходящего адреса. Если параметр не задан, используется исходящий IP-адрес, настроенный командой <code>ip ssh-client source-interface</code> .
<code>/user user-name</code>	Задает имя пользователя, используемое при входе в систему на удаленном сетевом устройстве с SSH-сервером. Если параметр не указан, то используется имя пользователя, заданное командой <code>ip ssh-client username</code> . Если используется данный параметр, необходимо также указать параметр <code>/password</code> .

Состояние по умолчанию:

Используется порт 22.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Команда **ssh** позволяет коммутатору создать безопасное, зашифрованное соединение с другим сетевым устройством, на котором запущен SSH-сервер. Такое соединение обеспечивает функциональность аналогичную подключению Telnet, за исключением того, что соединение зашифровано. Благодаря аутентификации и шифрованию, клиент SSH обеспечивает безопасную связь по небезопасной сети. Одновременно может быть активировано только одно соединение SSH.

Пример:

```
console# ssh 172.28.20.123 /user admin /password QwErTy port 1022
```

18.3. Команда telnet

Команда предназначена для создания соединения по протоколу Telnet с удаленным сетевым устройством.

Синтаксис:

telnet { *ip-address* | *hostname* } [*port*] [*keyword* ...]

Параметры:

- *ip-address* – IP-адрес назначения (IPv4 или IPv6);
- *hostname* – сетевое имя узла назначения. Длина: 1 – 160 символов. Максимальная длина части имени до точки – 58 символов;
- *port* – удаленный TCP-порт. Задаёт номер порта или ключевое слово, перечисленные в таблице ниже;
- *keyword* – одно или несколько ключевых слов. Ключевые слова перечислены в таблице ниже.

Состояние по умолчанию:

По умолчанию используется 23 порт.

Режим ИКС:

Привилегированный режим управления.

Примечание:

ПО коммутатора поддерживает специальные команды Telnet в виде последовательностей символов, которые отображают общие функции управления терминалом для функций, зависящих от операционной системы. Для ввода последовательностей необходимо нажать клавиши escape-последовательности (Ctrl-Shift-6), а затем символ команды Telnet. Специальные последовательности Telnet приведены в таблице ниже.

Специальные последовательности Telnet

Telnet	Назначение
--------	------------

последовательность	
Ctrl-shift-6-b	Break
Ctrl-shift-6-c	Interrupt Process (IP)
Ctrl-shift-6-h	Erase Character (EC)
Ctrl-shift-6-o	Abort Output (AO)
Ctrl-shift-6-t	Are You There? (AYT)
Ctrl-shift-6-u	Erase Line (EL)

В любой момент, во время активного сеанса Telnet доступные команды можно просмотреть набрав в системном приглашении **?/help**.

Пример вывода справки в сеансе:

```

console> ?/help
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
?/help suspends the session (return to system command prompt)

```

Допускается открытие нескольких параллельных сеансов Telnet, позволяющих переключаться между сеансами. Для открытия следующего сеанса, текущее соединение необходимо приостановить, выполнив escape-последовательность (Ctrl-Shift-6) и “x”, для возврата в системную командную строку. После этого можно открыть новое соединение командой **telnet**.

Переключение между сессиями осуществляется с помощью цифровых клавиш (1,2,3...). Ключевые слова приведены в таблице.

Таблица ключевых слов:

Ключевое слово	Описание
/echo	Включает локальное эхо.
/quiet	Предотвращает отображение на экране всех сообщений ПО.
/source-interface	Задаёт исходящий интерфейс.
/stream	Включает поточную обработку, которая обеспечивает необработанный поток TCP без управляющих последовательностей Telnet. Соединение по потоку не обрабатывает параметры Telnet и может использоваться для соединения с портами, использующими протокол UUCP, а также другие протоколы, отличные от Telnet.
Ctrl-shift-6 x	Выход в системную командную строку.

Параметры и номера портов приведены в таблице.

Таблица портов

Параметр	Описание	Номер порта
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Пример:

```
console# telnet 172.18.20.110
```

18.4. Команда traceroute

Команда **traceroute** предназначена для отображения маршрута прохождения пакетов до узла назначения.

Синтаксис:

```
traceroute [ ip ] { ipv4-address | hostname } [ size packet_size ] [ ttl max-ttl ] [ count packet_count ] [ timeout time_out ] [ source ip-address ]
```

Параметры:

- **ip** – используется IPv4;
- *ipv4-address* – IPv4 адрес назначения;
- *hostname* – сетевое имя узла назначения. Длина: 1 – 160 символов. Максимальная часть имени до точки – 58 символов;
- *packet_size* – Размер пакета в байтах, не включая тэг VLAN. По умолчанию 64 Б. IPv4: 54 – 1518);
- *max-ttl* – максимальное значение TTL которое можно использовать. По умолчанию: 30. Команда завершит работу, когда будет достигнута цель или когда наступит заданное значение TTL. Диапазон: 1 – 255;
- *packet_count* – количество попыток отправки пакетов на каждом уровне TTL. По умолчанию: 3. Диапазон: 1 – 10;
- *time_out* – количество секунд ожидания ответа на отправленный пакет. По умолчанию: 3. Диапазон: 1 – 10;
- *ip-address* – один из IP-адресов устройства, настроенных на интерфейсах. Используется в качестве адреса источника. По умолчанию, коммутатор выбирает оптимальный адрес.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Для определения маршрута прохождения пакета, команда отправляет целевому узлу серию пакетов, с каждым шагом увеличивая значение TTL на 1. Первая серия пакетов имеет TTL равный 1, поэтому первый маршрутизатор возвращает обратно сообщение об ошибке «time exceeded». Команда фиксирует адрес маршрутизатора, время между отправкой пакета и получением ответа (эти значения отображаются на экране терминала).
2. Далее команда повторяет серию, но значение TTL установлено равным 2. Первый маршрутизатор уменьшает значение на 1 и отправляет пакет дальше, второй маршрутизатор получив серию пакетов с TTL равным 1 также формирует сообщение об ошибке. Адрес второго маршрутизатора также фиксируется и отображается на экране.
3. Алгоритм повторяется до тех пор, пока не будет получен ответ от узла назначения. В этом случае работа команды считается завершенной.
4. Сообщение об ошибке **Destination unreachable** указывает, что промежуточный маршрутизатор получил пакет и отбросил его, поскольку не смог доставить его получателю. В этом случае очередной узел помечается звездочкой (*).
5. Команда завершает свою работу, когда узел назначения присылает ответ, когда превышен максимальный TTL или когда пользователь прерывает работу команды клавишей Esc.

Пример:

```
console# traceroute ip umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
 0 1 i2-gateway.stanford.edu (192.68.191.83) 0 msec 0 msec 0 msec
```



```

2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162) 1 msec 1 msec 1
msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103) 33 msec 35 msec 35
msec
6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80) 47 msec 45 msec 45
msec
7 so-0-2-0x1.aa1.mich.net (192.122.183.9) 56 msec 53 msec 54 msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82) 56 msec 56 msec 57
msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu(141.211.5.22)58 msec 58msec
58
msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64) 62 msec 63 msec 63
msec
Trace completed

```

В таблице ниже приведены символы, которые могут отображаться в выводе команды traceroute.

Поле	Описание
*	Превышено время ожидания.
?	Неизвестный тип пакета.
A	Административно недоступен. Обычно это указывает на то, что список доступа блокирует трафик.
F	Требуется фрагментация и установлен флаг DF.
H	Узел недоступен.
N	Сеть недоступна.
P	Протокол недоступен.
Q	Подавление источника.
R	Превышено время сборки фрагментов.
S	Исходный маршрут неверен.
U	Порт недоступен.

19. КОМАНДЫ LACP

19.1. Команда `lacp port`

Команда **lacp port** предназначена для установки приоритета физического порта. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

lacp port-priority *value*

no lacp port-priority

Параметры:

- *value* – приоритет порта. Диапазон: 1 – 65535.

Состояние по умолчанию:

По умолчанию приоритет порта равен 1.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Пример:

```
console(config)# interface gil/0/10
console(config-if)# lacp port-priority 1000
```

19.2. Команда `lacp system-priority`

Команда **lacp system-priority** предназначена для установки системного приоритета. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lacp system-priority *value*

no lacp system-priority

Параметры:

- *value* – значение системного приоритета. Диапазон: 1 – 65535.

Состояние по умолчанию:

По умолчанию приоритет порта равен 1.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# lacp system-priority 120
```

19.3. Команда lacp timeout

Команда **lacp timeout** предназначена для установки административного времени ожидания LACP на интерфейсе. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lacp timeout { long | short }

no lacp timeout

Параметры:

- **long** – задает длинное время ожидания;
- **short** – задает короткое время ожидания.

Состояние по умолчанию:

По умолчанию на порту задан длинное время ожидания.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Пример:

```
console(config)# interface gil/0/10
console(config-if)# lacp timeout short
```

19.4. Команда show lacp

Команда **show lacp** предназначена для отображения на экране информации LACP для указанного интерфейса.

Синтаксис:

show lacp interface-id [parameters | statistics | protocol-state]

Параметры:

- *interface-id* – идентификатор интерфейса;
- **parameters** – отображает только параметры;
- **statistics** – отображает только статистику;
- **protocol-state** – отображает состояние протокола.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show lacp gil/0/10
gil/0/10 LACP parameters:
    Actor
    system priority:          120
```

```
system mac addr:      00:19:0f:29:1e:be
port Admin key:      1000
port Oper key:       1000
port Oper number:    10
port Admin priority: 1000
port Oper priority:  1000
port Admin timeout:  SHORT
port Oper timeout:   SHORT
LACP Activity:       ACTIVE
Aggregation:         AGGREGATABLE
synchronization:     FALSE
collecting:          FALSE
distributing:        FALSE
expired:             FALSE

Partner
system priority:     0
system mac addr:     00:00:00:00:00:00
port Admin key:      0
port Oper key:       0
port Oper number:    0
port Admin priority: 0
port Oper priority:  0
port Oper timeout:   LONG
LACP Activity:       PASSIVE
Aggregation:         AGGREGATABLE
synchronization:     FALSE
collecting:          FALSE
distributing:        FALSE
expired:             FALSE

gil/0/10 LACP statistics:
  LACP Pdus sent:    0
  LACP Pdus received: 0
gil/0/10 LACP Protocol State:
  LACP State Machines:
    Receive FSM:      Port Disabled State
    Mux FSM:          Detached State
    Periodic Tx FSM:  No Periodic State

Control Variables:
  BEGIN:              FALSE
  LACP_Enabled:       TRUE
  Ready_N:            FALSE
  Selected:           UNSELECTED
  Port_moved:         FALSE
  NNT:                FALSE
  Port_enabled:       FALSE

Timer counters:
  periodic tx timer:  0
  current while timer: 0
  wait while timer:   0
```

19.5. Команда show lacp port-channel

Команда **show lacp port-channel** предназначена для отображения на экране информации LACP для интерфейса агрегированного канала.

Синтаксис:

show lacp port-channel [*port_channel_number*]

Параметры:

- *port_channel_number* – номер агрегированного канала.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show lacp Port-Channel 1
Port-Channel Po1
  Port Type Gigabit Ethernet
  Attached Lag id:
  Actor
    System Priority:120
    MAC Address:    00:19:0f:29:1e:be
    Admin Key:      1000
    Oper Key:       1000
  Partner
    System Priority:0
    MAC Address:    00:00:00:00:00:00
    Oper Key:       0
```

20. КОМАНДЫ LLDP

20.1. Команда clear lldp table

Команда **clear lldp table** предназначена для очистки таблицы соседей, полученных со всех портов или с указанного.

Синтаксис:

clear lldp table [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса.

Состояние по умолчанию:

Если идентификатор интерфейса не указан, то очищается таблица для всех портов.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# clear lldp table
```

20.2. Команда lldp chassis-id

Команда **lldp chassis-id** предназначена для задания ID шасси на порту. Использование префикса «**no**» устанавливает номер шасси по умолчанию.

Синтаксис:

lldp chassis-id { **mac-address** | **host-name** }

no lldp chassis-id

Параметры:

- **mac-address** – в качестве ID шасси используется MAC-адрес устройства;
- **host-name** – в качестве ID шасси используется заданное сетевое имя устройства.

Состояние по умолчанию:

В качестве ID используется MAC-адрес.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Сетевое имя устройства должно быть уникальным.

2. Если ID шасси, сконфигурировано для использования в LLDP-пакетах и не задано, то LLDP использует ID по умолчанию.

Пример:

```
console(config)# lldp chassis-id host-name
```

20.3. Команда lldp hold-multiplier

Команда **lldp hold-multiplier** предназначена для задания времени, как долго коммутатор удерживает пакет LLDP до его удаления. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

lldp hold-multiplier *number*

no lldp hold-multiplier

Параметры:

- *number* – задает временной интервал удержания пакета LLDP, как кратное значению таймера LLDP. Диапазон: 2 – 10).

Состояние по умолчанию:

Коэффициент удержания по умолчанию равен 4.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Фактическое значение TTL (Time-To-Live) для пакетов LLDP рассчитывается по формуле:

$$TTL = \min(65535, LLDP\text{-Timer} * LLDP\text{-hold-multiplier})$$

Например, если значение таймера LLDP составляет 30 с, а значение hold-multiplier 4, то в поле TTL заголовка пакета LLDP копируется результат – 120.

Пример:

```
console(config)# lldp timer 50  
console(config)# lldp hold-multiplier 5
```

20.4. Команда lldp lldpdu

Команда **lldp lldpdu** предназначена для установки режима обработки пакетов LLDP, когда функция LLDP глобально отключена. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

lldp lldpdu { **filtering** | **flooding** }

no lldp lldpdu

Параметры:

- **filtering** – LLDP пакеты отфильтровываются (удаляются);
- **flooding** – LLDP пакеты пропускаются (перенаправляются на все интерфейсы).

Состояние по умолчанию:

При отключенной функции LLDP все LLDP-пакеты удаляются.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Если на коммутаторе установлен режим MSTP, то режим обработки LLDP пакетов не может быть настроен на перенаправление и наоборот.
2. Если LLDP отключен глобально, а режим обработки LLDP пакетов настроен на перенаправление, то пакеты LLDP обрабатываются как пакеты данных, со следующими исключениями:
 - Правила обработки входящих пакетов VLAN не применяются к LLDP-пакетам. Пакеты LLDP блокируются на всех портах, для которых состояние STP является Forwarding.
 - Правило deny-all по умолчанию не применяется для LLDP пакетов.
 - Правила исходящих пакетов VLAN не применяются к LLDP пакетам. Все LLDP пакеты перенаправляются на интерфейсы, на которых установлено состояние STP Forwarding.
 - Пакеты LLDP отправляются не тегированными.

Пример:

```
console(config)# lldp lldpdu flooding
```

20.5. Команда lldp management-address

Команда **lldp management-address** предназначена для объявления адреса управления, заданного на интерфейсе. Использование префикса «no» прекращает объявление.

Синтаксис:

lldp management-address {*ip-address* | **none** | **automatic** [*interface-id*]}

no lldp management-address

Параметры:

- *ip-address* – указывает статический адрес для объявления;
- **none** – ни один адрес не объявляется;
- **automatic** – ПО коммутатора автоматически выбирает адрес управления для анонсирования из всех IP-адресов устройства. В случае нескольких IP-адресов выбирается самый меньший среди динамических адресов. Если динамических

адресов нет, программное обеспечение выбирает самый меньший адрес из статических;

- **automatic interface-id** - ПО коммутатора автоматически выбирает адрес управления для анонсирования из IP-адресов, которые настроены на интерфейсе. В случае нескольких адресов, выбирается самый меньший IP-адрес. Идентификатор интерфейса может быть одним из следующих типов: Ethernet, Port Channel или VLAN.

Примечание: Если порт или агрегированный канал являются членами VLAN которому присвоен IP-адрес, то данный адрес не используется, так как привязан к VLAN.

Состояние по умолчанию:

IP-адрес для анонсирования не задан.

Выбор анонсирования по умолчанию: **automatic**.

Режим ИКС:

Режим конфигурации интерфейса

Примечание:

Один порт может анонсировать только один IP-адрес.

Пример:

```
console(config)# interface gil/0/23
console(config-if)# lldp management-address automatic
```

20.6. Команда lldp med

Команда **lldp med** предназначена для включения/отключения режима LLDP MED (Media Endpoint Discovery) на интерфейсе. Использование префикса **no** устанавливает значение по умолчанию.

Синтаксис:

lldp med { enable [tlv ... tlv4] | disable }

no lldp med

Параметры:

- **enable** – разрешает LLDP MED.
- **tlv** – указывает какие TLV (Type, Value, Length) должны быть включены в пакет. Доступны следующие TLV: **Network-policy**, **Location**, **POE-PSE**, **Inventory**. TLV всегда включается, когда включен LLDP MED. Всего может быть задано до 4 TLV.
- **disable** – отключает LLDP MED на порту.

Состояние по умолчанию:

Разрешен, включая TLV **Network-Policy**

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Пример:

```
console(config)# interface gi1/0/23
console(config-if)# lldp med enable
```

20.7. Команда lldp med notification topology-change

Команда **lldp med notification topology-change** предназначена для включения уведомлений LLDP MED при изменениях в топологии на порт. Использование префикса «no» устанавливает значения по умолчанию.

Синтаксис:

lldp med notifications topology-change { enable | disable }

no lldp med notifications topology-change

Параметры:

- **enable** – включает отправку сообщений;
- **disable** – отключает отправку сообщений.

Состояние по умолчанию:

Отправка сообщений отключена.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Пример:

```
console(config)# interface gi1/0/10
console(config-if)# lldp med notifications topology-change enable
```

20.8. Команда lldp med fast-start repeat-count

Когда порт переходит в состояние «ifOperStatus UP», LLDP может отправлять пакеты быстрее, чем обычно, используя свой механизм быстрого запуска.

Команда **lldp med fast-start repeat-count** предназначена для указания количества пакетов, отправляемых по время активации механизма быстрого запуска. Использование префикса «no» устанавливает значение по умолчанию.

Синтаксис:

lldp med fast-start repeat-count *number*

no lldp med fast-start repeat-count

Параметры:

- *number* – количество отправляемых пакетов LLDPDU при активации быстрого запуска (диапазон: 1 – 10).

Состояние по умолчанию:

3

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# lldp med fast-start repeat-count 8
```

20.9. Команда lldp med location

Команда **lldp med location** предназначена для настройки информации о местоположении, для обнаружения конечных точек LLDP MED (Media Endpoint Discovery). Использование префикса «**no**» удаляет данные о местоположении.

Синтаксис:

lldp med location { coordinate data | civic-address data | ecs-elin data }

no lldp med location { coordinate | civic-address | ecs-elin }

Параметры:

- **coordinate** – данные о местоположении в виде координат, в шестнадцатеричном формате;
- **civic-address** – адрес местоположения в шестнадцатеричном формате;
- **ecs-elin** – данные о местоположении для использования вызова экстренной помощи ECS ELIN (Emergency Call Service Emergency Location Identification Number);
- *data* – данные о местоположении в формате определенном в ANSI/TIA 1057. Каждый байт в шестнадцатеричной строке состоит из двух шестнадцатеричных цифр. Байты разделены точкой или двоеточием. Длина: **coordinate** – 16 Б, **civic-address** – 6 – 160 Б, **ecs-elin** – 10 – 25 Б.

Состояние по умолчанию:

Местоположение не задано.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Пример:

```
console(config)# interface gil/0/10  
console(config-if)# lldp med location civic-address 616263646566
```

20.10. Команда `lldp med network-policy` (Global)

Команда **lldp med network-policy** (Global) предназначена для задания сетевых политик для LLDP MED. Для голосовых приложений применяется команда **lldp med network-policy voice auto**. Использование префикса «no» удаляет политики.

Созданные данной командой политики далее можно применить на интерфейсе с помощью команды **lldp med network-policy** (interface).

Синтаксис:

```
lldp med network-policy number application [ vlan vlan-id ] [ vlan-type { tagged | untagged } ] [ up priority ] [ dscp value ]
```

```
no lldp med network-policy number
```

Параметры:

- *number* – номер сетевой политики, диапазон: 1 – 32;
- *application* – имя или номер основной функции приложения, определенного для этой сетевой политики. Доступны следующие имена приложений:
 - **voice**;
 - **voice-signaling**;
 - **quest-voice**;
 - **quest-voice-signaling**;
 - **softphone-voice**;
 - **video-conferencing**;
 - **streaming-video**;
 - **video-signaling**;
- *vlan-id* – идентификатор VLAN используемый приложением.
- **vlan-type** – указывает использует ли приложение тегированный или не тегированный VLAN.
- *priority* – пользовательский приоритет (приоритет 2 уровня OSI) используемый заданным приложением;
- *value* – значение DSCP используемое заданным приложением.

Состояние по умолчанию:

Сетевые политики не заданы.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# lldp med network-policy 1 voice-signaling vlan 1
vlan-type untagged up 1 dscp 2
console(config)# interface gil1/0/10
console(config-if)# lldp med network-policy add 1
```

20.11. Команда `lldp med network-policy` (Interface)

Команда **lldp med network-policy** (Interface) предназначена для назначения или удаления сетевой политики на порт. Использование префикса «**no**» удаляет сетевую политику с порта.

Сетевые политики создаются командой **lldp med network-policy** (Global).

Синтаксис:

lldp med network-policy { **add** | **remove** } *number*

no lldp med network-policy *number*

Параметры:

- **add/remove** – назначает или удаляет заданную сетевую политику на порту;
- *number* – номер сетевой политики. Диапазон: 1 – 32.

Состояние по умолчанию:

Сетевые политики на портах не назначены.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечание:

Для каждого интерфейса может быть применена только одна сетевая политика на приложение.

Пример:

```
console(config)# lldp med network-policy 1 voice-signaling vlan 1
vlan-type untagged up 1 dscp 2
console(config)# interface gil0/0/10
console(config-if)# lldp med network-policy add 1
```

20.12. Команда `lldp med network-policy voice auto`

Сетевая политика для голосовых пакетов LLDP может быть создана с использованием команды **lldp med network-policy** (Global).

Команда **lldp med network-policy voice auto** предназначена для автоматического создания сетевой политики на основе конфигурации голосовых приложений.

Команда генерирует сетевую политику LLDP MED для голосовых приложений, если режим голосовой VLAN – `auto voice VLAN`. В политике используется голосовая VLAN, приоритет 802.1p и DSCP для голосовой VLAN.

Использование префикса «**no**» отключает режим.

Созданная сетевая политика автоматически применяется к голосовой VLAN.

Синтаксис:

lldp med network-policy voice auto

no lldp med network-policy voice auto

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Политики не определены.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. В автоматическом режиме функция определяет голосовую VLAN, на каких интерфейсах анонсируется TLV и используется голосовое приложение, а также контролирует этот TLV.
2. Для включения автоматической генерации сетевой политике на голосовой VLAN, в голосовом приложении не должно быть предварительно настроенных сетевых политик. В автоматическом режиме нельзя вручную задать сетевую политику для голосовой VLAN.

Пример:

```
console(config)# lldp med network-policy voice auto
```

20.13. Команда lldp notifications

Команда **lldp notifications** предназначена для включения/отключения отправки LLDP уведомлений на интерфейсе. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

lldp notifications { enable | disable }

no lldp notifications

Параметры:

- **enable** – включает отправку уведомлений;
- **disable** – отключает отправку уведомлений.

Состояние по умолчанию:

Отключено.

Режим ИКС:

Режим конфигурации интерфейса

Пример:

```
console(config)# interface gil/0/10
```

```
console(config-if)# lldp notifications enable
```

20.14. Команда lldp notifications interval

Команда **lldp notifications interval** предназначена для задания максимальной скорости передачи LLDP уведомлений. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lldp notifications interval *seconds*

no lldp notifications interval

Параметры:

- *seconds* – временной интервал между отправками уведомлений. Диапазон: 5 – 3600.

Состояние по умолчанию:

5 секунд.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# lldp notifications interval 60
```

20.15. Команда lldp optional-tlv

Команда **lldp optional-tlv** предназначена для указания передачи дополнительно TLV (Type, Length, Value). Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lldp optional-tlv { *tlv* [*tlv2* ... *tlv5*] | **none** }

no lldp optional-tlv

Параметры:

- *tlv* – определяет какие дополнительные TLV включаются в пакет. Доступные опции: **port-desc**, **sys-name**, **sys-desc**, **sys-cap**, **802.3-mac-phy**, **802.3-lag**, **802.3-max-frame-size**. Может быть задано до 5 опций.
- **none** – отменяет отправку всех дополнительных TLV на интерфейсе.

Дополнительная опция 802.1 описывается в команде **lldp optional-tlv 802.1**.

Состояние по умолчанию:

Передаются следующие TLV:

sys-name

sys-cap

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Пример:

```
console(config)# interface gi1/0/10
console(config-if)# lldp optional-tlv port-desc
```

20.16. Команда lldp optional-tlv 802.1

Команда **lldp optional-tlv 802.1** предназначена для настройки передачи уведомлений TLV, для протокола 802.1. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lldp optional-tlv 802.1 pvid { enable | disable } - PVID объявляется или нет.

no lldp optional-tlv 802.1 pvid - объявление PVID устанавливается в состояние по умолчанию.

lldp optional-tlv 802.1 ppvid add ppvid – Объявление протокола Port VLAN ID (PPVID). PPVID - это PVID, который используется в зависимости от протокола пакета.

lldp optional-tlv 802.1 ppvid remove ppvid - PPVID не объявляется.

lldp optional-tlv 802.1 vlan add vlan-id – Объявляется идентификатор vlan-id.

lldp optional-tlv 802.1 vlan remove vlan-id – Идентификатор vlan-id удаляется из объявления.

lldp optional-tlv 802.1 protocol add { stp | rstp | mstp | pause | 802.1x | lacp | gvrp } – Объявляются выбранные протоколы.

lldp optional-tlv 802.1 protocol remove { stp | rstp | mstp | pause | 802.1x | lacp | gvrp } – Выбранные протоколы удаляются из объявления.

Параметры:

- **lldp optional-tlv 802.1 pvid { enable | disable }** – объявляет или прекращает объявления PVID порта;
- **lldp optional-tlv 802.1 ppvid add/remove ppvid** – добавляет или удаляет PVID в объявлении. Диапазон: 0 – 4094. PVID = 0 указывает на то, что порт не способен поддерживать порты и протоколы VLAN и/или порт не включен ни в один из протоколов VLAN;
- **add/remove vlan-id** – добавляет/удаляет VLAN в/из объявления. Диапазон: 0 – 4094;
- **add/remove {stp | rstp | mstp | pause | 802.1x | lacp | gvrp}** – **add** указывает на то что необходимо объявлять указанный протокол, **remove** – не следует объявлять указанные протоколы.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Пример:

```
console(config)# interface gi1/0/10  
console(config-if)# lldp optional-tlv 802.1 protocol add 802.1x
```

20.17. Команда **lldp run**

Команда **lldp run** предназначена для включения протокола LLDP на коммутаторе. Использование префикса «**no**» отключает протокол.

Синтаксис:

lldp run

no lldp run

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Включено.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# lldp run
```

20.18. Команда **lldp receive**

Команда **lldp receive** предназначена для включения получения LLDP уведомлений на интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

lldp receive

no lldp receive

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Включено.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. LLDP управляет LAG-портами индивидуально. Данные LLDP полученные через порты LAG сохраняются отдельно для каждого порта.
2. Операции LLDP на порту не зависят от состояния STP на порту. Кадры LLDP принимаются и на заблокированных портах.
3. Если на порту настроен 802.1x LLDP работает только в том случае, если порт авторизован.

Пример:

```
console(config)# interface gil/0/10  
console(config-if)# lldp receive
```

20.19. Команда lldp reinit

Команда **lldp reinit** предназначена для задания минимального времени ожидания LLDP порта перед повторной инициализации передачи LLDP пакетов. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lldp reinit *seconds*

no lldp reinit

Параметры:

- *seconds* – время ожидания повторной инициализации в секундах. Диапазон: 1 – 10.

Состояние по умолчанию:

Время ожидания повторной инициализации 2 секунды

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# lldp reinit 5
```

20.20. Команда lldp timer

Команда **lldp timer** предназначена для задания времени частоты отправки обновлений LLDP. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lldp timer *seconds*

no lldp timer

Параметры:

- *seconds* – интервал в секундах между отправками обновлений. Диапазон: 5 – 32768.

Состояние по умолчанию:

Интервал между отправками обновлений 30 секунд.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# lldp timer 120
```

20.21. Команда lldp transmit

Команда **lldp transmit** предназначена для включения передачи LLDP пакетов на интерфейсе. Использование префикса «**no**» отключает передачу.

Синтаксис:

lldp transmit

no lldp transmit

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Включено.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet)

Примечания:

1. LLDP управляет LAG-портами индивидуально. Данные LLDP полученные через порты LAG сохраняются отдельно для каждого порта.
2. Операции LLDP на порту не зависят от состояния STP на порту. Т.е. кадры LLDP принимаются и на заблокированных портах.
3. Если на порту настроен 802.1x LLDP работает только в том случае, если порт авторизован.

Пример:

```
console(config)# interface gil/0/10  
console(config-if)# lldp transmit
```

20.22. Команда lldp tx-delay

Команда **lldp tx-delay** предназначена для установки времени задержки между последовательными передачами кадров LLDP, инициированных изменениями значения статуса в локальной системе LLDP MIB. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

lldp tx-delay *seconds*

no lldp tx-delay

Параметры:

- *seconds* – время задержки (в секундах). Диапазон: 1 – 8192.

Состояние по умолчанию:

Время задержки – 2 с.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# lldp tx-delay 120
```

20.23. Команда show lldp configuration

Команда **show lldp configuration** предназначена для вывода на экран конфигурации LLDP для всех портов или заданного.

Синтаксис:

show lldp configuration [{ *interface-id* | **detailed** }]

Параметры:

- *interface-id* – идентификатор интерфейса;
- **detailed** – отображает информацию о неучтенных портах в дополнение к текущим.

Состояние по умолчанию:

Отображает информацию обо всех портах. Если параметр **detailed** не используется, отображаются только текущие порты коммутатора.

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1:

```
console# show lldp configuration

LLDP state: Enabled
Timer: 120 Seconds
Hold multiplier: 4
Reinit delay: 5 Seconds
Tx delay: 120 Seconds
Notifications Interval: 60 Seconds
LLDP packets handling: Filtering
```

Chassis ID: mac-address				
Port	State	Optional TLVs	Address	
Notifica-tions				

gil/0/1	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/2	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/3	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/4	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/5	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/6	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/7	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/8	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/9	Rx and Tx	SN, SC	None	
Disa-bled				
gil/0/10	Rx and Tx		None	
Enabled				
gil/0/11	Rx and Tx	SN, SC	None	
Disa-bled				

Пример 2:

```

console# show lldp configuration gil/0/10

LLDP state: Enabled
Timer: 120 Seconds
Hold multiplier: 4
Reinit delay: 5 Seconds
Tx delay: 120 Seconds
Notifications Interval: 60 Seconds
LLDP packets handling: Filtering
Chassis ID: mac-address

    Port      State      Optional TLVs      Address
Notifica-tions
-----
gil/0/10    Rx and Tx
Enabled

802.3 optional TLVs: 802.3-mac-phy

802.1 optional TLVs
PVID: Enabled

```

PPVIDs: VLANs: Protocols:

Описание полей:

Поле	Описание
Timer	Временной интервал между обновлениями LLDP.
Hold multiplier	Количество времени (кратное таймеру), которое принимающее устройство удерживает LLDP пакет перед отбрасыванием.
Reinit timer	Минимальное количество времени, которое ожидает порт LLDP перед повторной инициализацией передачи LLDP.
Tx delay	Задержка между последовательными передачами кадров LLDP, инициированных изменением значения/состояния в локальной системе LLDP MIB.
Port	Номер порта
State	LLDP статус порта.
Optional TLVs	Дополнительные TLV, которые объявляются. Возможные значения: <ul style="list-style-type: none"> • PD - Port description; • SN - System name; • SD - System description; • SC - System capabilities; • 4W - 4 wire spare pair capability.
Address	Адрес управления, который объявляется.
Notifications	Показывает включены или отключены уведомления LLDP
PVID	Объявляемый порт VLAN ID.
PPVID	Объявляемый протокол порта VLAN ID.
Protocols	Объявляемые протоколы.

20.24. Команда show lldp local

Команда **show lldp local** предназначена для отображения на экране LLDP информацию, объявляемую через указанный порт.

Синтаксис:

show lldp local *interface-id*

Параметры:

- *interface-id* – идентификатор интерфейса.

Режим ИКС:

Привилегированный режим управления.

Пример:

<pre>console# show lldp local gi1/0/10 Device ID: 00:19:0f:29:1e:be</pre>
--

```
Port ID: gil/0/10

802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Disabled
Auto-negotiation Advertised Capabilities: other or unknown
Operational MAU type: Unknown

802.1 PVID: 1
802.1 PPVID:
802.1 VLAN:
802.1 Protocol:
```

20.25. Команда show lldp local tlvs-overloading

Когда пакет LLDP содержит слишком много информации для одного пакета, это называется перегрузкой.

Команда **show lldp local tlvs-overloading** предназначена для отображения на экране информации о перегрузке пакета LLDP опциями TLV, для всех портов или заданного.

Синтаксис:

show lldp local tlvs-overloading [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса.

Состояние по умолчанию:

Если идентификатор не задан, выводится информация для всех портов.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Команда вычисляет статус перегрузки текущей конфигурации LLDP, а не по последнему отправленному пакету.

Пример:

```
console# show lldp local tlvs-overloading gil/0/10

      TLVs Group           Bytes           Status
-----
Mandatory                   26           Transmitted
802.3                       11           Transmitted
802.1                        8           Transmitted

Total: 45 bytes
```

```
Left: 0 bytes
console#show lldp local tlvs-overloading
No LLDP TLV overloading.
```

20.26. Команда show lldp med configuration

Команда **show lldp med configuration** предназначена для отображения на экране конфигурации LLDP MED (Media Endpoint Discovery), для всех портов или для заданного.

Синтаксис:

show lldp med configuration [{ interface-id | detailed }]

Параметры:

- *interface-id* – идентификатор интерфейса.
- **detailed** – отображает информацию о неучтенных портах в дополнение к текущим.

Состояние по умолчанию:

Отображает информацию обо всех портах. Если параметр **detailed** не используется, отображаются только текущие порты коммутатора.

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1:

```
console# show lldp med configuration

Fast Start Repeat Count: 8.
LLDP MED network-policy voice: auto

Network policy 1
-----
Application type: voiceSignaling
VLAN ID: 1 untagged
Layer 2 priority: 1
DSCP: 2

      Port      Capabilities  Network  Location  Notifications
Inventory
              policy
-----
---
gil/0/1        Yes          Yes      No        Disabled   No
gil/0/2        Yes          Yes      No        Disabled   No
gil/0/3        Yes          Yes      No        Disabled   No
gil/0/4        Yes          Yes      No        Disabled   No
gil/0/5        Yes          Yes      No        Disabled   No
gil/0/6        Yes          Yes      No        Disabled   No
gil/0/7        Yes          Yes      No        Disabled   No
```


gil/0/8	Yes	Yes	No	Disabled	No
gil/0/9	Yes	Yes	No	Disabled	No
gil/0/10	Yes	Yes	No	Enabled	No
gil/0/11	Yes	Yes	No	Disabled	No
gil/0/12	Yes	Yes	No	Disabled	No
gil/0/13	Yes	Yes	No	Disabled	No
gil/0/14	Yes	Yes	No	Disabled	No
gil/0/15	Yes	Yes	No	Disabled	No
gil/0/16	Yes	Yes	No	Disabled	No
gil/0/17	Yes	Yes	No	Disabled	No
gil/0/18	Yes	Yes	No	Disabled	No
gil/0/19	Yes	Yes	No	Disabled	No
gil/0/20	Yes	Yes	No	Disabled	No
gil/0/21	Yes	Yes	No	Disabled	No
gil/0/22	Yes	Yes	No	Disabled	No
gil/0/23	Yes	Yes	No	Disabled	No
gil/0/24	Yes	Yes	No	Disabled	No
tel/0/1	Yes	Yes	No	Disabled	No
tel/0/2	Yes	Yes	No	Disabled	No
oob	Yes	Yes	No	Disabled	No

Пример 2:

```

console# show lldp med configuration gil/0/10

      Port      Capabilities  Network  Location  Notifications
Inventory
-----
policy
-----
---
gil/0/10      Yes          Yes       No        Enabled    No

Network policies: 1
Location:
Civic-address: 61:62:63:64:65:66

```

20.27. Команда show lldp neighbors

Команда **show lldp neighbors** предназначена для отображения на экране информации о соседних устройствах, обнаруженных с помощью LLDP, для всех портов или заданного.

Синтаксис:

show lldp neighbors [*interface-id*]

Параметры:

- *interface-id* – идентификатор интерфейса.

Состояние по умолчанию:

Если идентификатор порта не указан, то выводится информация по всем портам.

Режим ИКС:

Привилегированный режим управления.

Примечание:

Опции TLV, которые не могут быть отображены в виде ASCII-строки отображаются в шестнадцатеричном виде.

Примеры:

Пример 1:

```
console# show lldp neighbors

System capability legend:
B - Bridge; R - Router; W - Wlan Access Point; T - telephone;
D - DOCSIS Cable Device; H - Host; r - Repeater;
TP - Two Ports MAC Relay; S - S-VLAN; C - C-VLAN; O - Other

   Port          Device ID          Port ID          System Name
Capabilities  TTL
-----
-----
   gil/0/23     2c:23:3a:76:0e:56 2c:23:3a:76:0   HP 1920G Switch   B, R
102
                                     e:79
   gil/0/23     d0:50:99:97:17:2d d0:50:99:97:1   O
2902
                                     7:2d
```

Пример 2:

```
console# show lldp neighbors gil/0/23

Device ID: 2c:23:3a:76:0e:56
Port ID: 2c:23:3a:76:0e:79
Capabilities: Bridge, Router
System Name: HP 1920G Switch
System description: 1920-48G Switch Software Version 5.20.99,
Release 1111
Copyright(c)2010-2016 Hewlett-Packard Development Company, L.P.
Port description: GigabitEthernet1/0/34 Interface
Management Address: 10.3.2.2
Time To Live: 105

802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities:
Operational MAU type: 1000BaseTFD

802.3 Power via MDI:
MDI Power support Port Class: PD
```

PSE MDI Power Support: Not supported
PSE MDI Power State: Not enabled
Power Type: Type 1 PD
Power Source: PSE and Local Power Source
Power Priority: high
PD Requested Power Value: 230.4

802.3 Link Aggregation

Aggregation capability: Capable of being aggregated
Aggregation status: Currently not in aggregation

802.3 Maximum Frame Size: 9600

802.1 PVID: 1

802.1 PPVID: 0 not supported, not enabled

802.1 VLAN: 1 (VLAN 0001)

802.1 Protocol:

LLDP-MED capabilities: Capabilities, Network Policy, Location,
Inventory

LLDP-MED Device Type: Network Connectivity

Hardware revision: REV.A

Firmware revision: 115

Software revision: Release 1111

Serial number: CN50GP74CK

Manufacturer name: HP

Model name: HP 1920-48G Switch JG927A

Asset ID: Unknown

Device ID: d0:50:99:97:17:2d

Port ID: d0:50:99:97:17:2d

Capabilities: Other

System Name:

System description:

Port description:

Time To Live: 2844

802.3 MAC/PHY Configuration/Status

Auto-negotiation support: Supported

Auto-negotiation status: Enabled

Auto-negotiation Advertised Capabilities: 1000BASE-T full duplex

Operational MAU type: Unknown

802.1 PVID: None

802.1 PPVID:

802.1 VLAN:

802.1 Protocol:
LLDP-MED capabilities: Capabilities
LLDP-MED Device Type: Endpoint Class1

Таблица полей LLDP:

Поле	Описание
Port	Идентификатор порта.
Device ID	Идентификатор соседнего устройства (имя) или MAC-адрес.
Port ID	Идентификатор порта соседнего устройства.
System name	Административно назначенное имя соседнего устройства.
Capabilities	Роль соседнего устройства. Возможны следующие значения: <ul style="list-style-type: none"> • B – Bridge • R – Router • W - WLAN Access Point • T – Telephone • D - DOCSIS cable device • H – Host • r – Repeater • O - Other
System description	Системное описание соседнего устройства.
Port description	Описание порта соседнего устройства.
Management address	Адрес управления соседнего устройства.
Auto-negotiation support	Статус режима автосогласования порта (включено/выключено)
Auto-negotiation status	Текущий статус режима автосогласования порта.
Auto-negotiation Advertised Capabilities	Возможности автосогласования объявляемые на порту (speed/duplex/flow-control).
Operational MAU type	Тип порта MAU.
LLDP MED Capabilities	Отправляемые опции LLDP-MED.
Device type	Тип устройства. Указывает является ли отправитель подключенным к сети устройством или конечным устройством в сети. И если устройство является конечным, то к какому классу оно принадлежит.
LLDP MED - Network Policy Application type	Основная функция приложения, определенного в данной сетевой политике.
Flags	Флаги. Возможные значения: <ul style="list-style-type: none"> • Unknown policy: Политика требуется устройством, но в настоящее время неизвестна. • Tagged VLAN: указанное приложение использует тегированную VLAN. • Untagged VLAN: указанное приложение

	использует не тегированную VLAN.
VLAN ID	Идентификатор VLAN используемый приложением.
Layer 2 priority	Приоритет 2 уровня OSI используемый приложением.
DSCP	Значение DSCP используемое приложением.

20.28. Команда show lldp statistics

Команда **show lldp statistics** предназначена для отображения на экране статистики LLDP для всех портов или заданного.

Синтаксис:

show lldp statistics [{ *interface-id* | **detailed** }]

Параметры:

- *interface-id* – идентификатор интерфейса.
- **detailed** – отображает информацию о неучтенных портах в дополнение к текущим.

Состояние по умолчанию:

Отображает информацию обо всех портах. Если параметр **detailed** не используется, отображаются только текущие порты коммутатора.

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1:

```

console# show lldp statistics

Tables Last Change Time: 04-Jun-2018 14:24:58
Tables Inserts: 2
Tables Deletes: 0
Tables Dropped: 0
Tables Ageouts: 0

          TX Frames          RX Frames          RX TLVs
RX Ageouts
  Port      Total      Total  Discarded Errors Discarded Unrecognized
Total
-----
0  gi1/0/1      0        0        0        0        0        0
0  gi1/0/2      0        0        0        0        0        0
0  gi1/0/3      0        0        0        0        0        0
0  gi1/0/4      0        0        0        0        0        0
0

```

0	gil/0/5	0	0	0	0	0	0
0	gil/0/6	0	0	0	0	0	0
0	gil/0/7	0	0	0	0	0	0
0	gil/0/8	0	0	0	0	0	0
0	gil/0/9	0	0	0	0	0	0
0	gil/0/10	0	0	0	0	0	0
0	gil/0/11	0	0	0	0	0	0
0	gil/0/12	0	0	0	0	0	0
0	gil/0/13	0	0	0	0	0	0
0	gil/0/14	0	0	0	0	0	0
0	gil/0/15	0	0	0	0	0	0
0	gil/0/16	0	0	0	0	0	0
0	gil/0/17	0	0	0	0	0	0
0	gil/0/18	0	0	0	0	0	0
0	gil/0/19	0	0	0	0	0	0
0	gil/0/20	0	0	0	0	0	0
0	gil/0/21	0	0	0	0	0	0
0	gil/0/22	0	0	0	0	0	0
0	gil/0/23	3186	3507	0	3399	3399	0
0	gil/0/24	0	0	0	0	0	0
0	tel/0/1	0	0	0	0	0	0
0	tel/0/2	0	0	0	0	0	0
0	oob	0	0	0	0	0	0

Пример 2:

```
console# show lldp statistics gil/0/23  
  
Tables Last Change Time: 04-Jun-2018 14:25:08  
Tables Inserts: 2
```

Tables Deletes: 0						
Tables Dropped: 0						
Tables Ageouts: 0						
	TX Frames		RX Frames		RX TLVs	
RX Ageouts						
Port	Total	Total	Discarded	Errors	Discarded	Unrecognized
Total						

gil/0/23	3188	3516	0	3408	3408	0
0						

21. КОМАНДЫ НАСТРОЙКИ ЛИНИИ

21.1. Команда autobaud

Команда **autobaud** предназначена для включения функции автоматического определения скорости передачи в бодах. Использование префикса «**no**» отключает функцию.

Синтаксис:

autobaud

no autobaud

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Автоматическое определение скорости включено.

Режим ИКС:

Режим конфигурации линии (Console)

Примечания:

1. Данная команда доступна только в режиме настройки линии консоли.
2. Если функция включена, то активируется она следующим образом: подключить консольный кабель к устройству и дважды нажать клавишу Enter. Устройство автоматически определит скорость передачи в бодах. Если нажимать кнопки отличные от Enter, то скорость может быть определена неправильно.

Пример:

```
console(config)# line console
console(config-line)# autobaud
Console baud-rate auto detection is enabled, press Enter twice to
complete the detection process
console(config-line)#
Detected speed: 115200
```

21.2. Команда exec-timeout

Команда **exec-timeout** задает временной интервал ожидания неактивности текущей сессии терминала, по истечении которого происходит автоматический выход из сессии. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

exec-timeout *minutes* [*seconds*]

no exec-timeout

Параметры:

- *minutes* – количество минут в интервале. Диапазон: 0 – 65535;
- *seconds* – количество секунд в интервале. Диапазон: 0 – 59.

Состояние по умолчанию:

Временной интервал – 10 минут.

Режим ИКС:

Режим конфигурации линии

Примечание:

Установка параметров в 0 предотвращает автоматическое закрытие сессии.

Пример:

```
console(config)# line telnet
console(config-line)# exec-timeout 20 10
```

21.3. Команда line

Команда **line** предназначена для задания конкретной линии и перехода в режим конфигурации линии.

Синтаксис:

line { console | telnet | ssh }

Параметры:

- **console** – переход в режим конфигурирования линии консольного доступа.
- **telnet** – переход в режим конфигурирования линии для виртуального терминала удаленной сессии (telnet).
- **ssh** – переход в режим конфигурирования линии для виртуального терминала защищенной удаленной сессии.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# line telnet
```

21.4. Команда speed

Команда предназначена для установки скорости передачи, в bps. Использование префикса «**no**» устанавливает значение по умолчанию.

Синтаксис:

speed bps

no speed

Параметры:

- *bps* – задает скорость передачи в bps (bits per second). Возможные значения: 4800, 9600, 19200, 38400, 57600 и 115200.

Состояние по умолчанию:

По умолчанию скорость передачи – 115200.

Режим ИКС:

Режим конфигурации линии (console)

Примечание:

Команда применяется только тогда, когда отключен режим **autobaud**. Новые настройки скорости применяются только к текущему сеансу.

Пример:

```
console(config-line)# speed 57600
```

21.5. Команда show line

Команда **show line** предназначена для отображения на экране текущих параметров настройки линий.

Синтаксис:

show line [{ console | telnet | ssh }]

Параметры:

- **console** – отображает конфигурацию линии console;
- **telnet** – отображает конфигурацию линии telnet;
- **ssh** – отображает конфигурацию линии ssh.

Состояние по умолчанию:

Если тип линии не задан, выводится информация по всем линиям.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show line
Console configuration:
Interactive timeout: Disabled
History: 10
Baudrate: autobaud
Databits: 8
Parity: none
Stopbits: 1
```

```
Telnet configuration:  
Telnet is disabled.  
Interactive timeout: 20 minute(s) 10 second(s)  
History: 10
```

```
SSH configuration:  
Interactive timeout: 10 minute(s)  
History: 10
```

22. КОМАНДЫ ОБНАРУЖЕНИЯ ОБРАТНОЙ ПЕТЛИ (LOOPBACK)

22.1. Команда loopback-detection enable (Global)

Команда **loopback-detection enable** (Global) предназначена для включения функции Loopback Detection (LBD) глобально. Использование префикса «**no**» отключает функцию.

Синтаксис:

loopback-detection enable

no loopback-detection enable

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Функция отключена.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Данная команда разрешает использование функции глобально. Для включения функции на интерфейсе используется команда **loopback-detection enable** в режиме конфигурирования интерфейса.

Пример:

```
console(config)# loopback-detection enable
```

22.2. Команда loopback-detection enable (Interface)

Команда **loopback-detection enable** (Interface) предназначена для включения функции Loopback Detection (LBD) на интерфейсе. Использование префикса «**no**» отключает функцию.

Синтаксис:

loopback-detection enable

no loopback-detection enable

Параметры:

Дополнительные параметры отсутствуют.

Состояние по умолчанию:

Функция включена.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Пример:

```
console(config)# interface gi1/0/23
console(config-if)# loopback-detection enable
```

22.3. Команда loopback-detection interval

Команда **loopback-detection interval** предназначена для установки временного интервала между пакетами LBD. Использование префикса «**no**» устанавливает значения по умолчанию.

Синтаксис:

loopback-detection interval *seconds*

no loopback-detection interval

Параметры:

- *seconds* – временной интервал, в секундах. Диапазон: 10 – 60.

Состояние по умолчанию:

Временной интервал составляет 30 с.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# loopback-detection interval 60
```

22.4. Команда show loopback-detection

Команда **show loopback-detection** предназначена для отображения на экране информации о функции LBD.

Синтаксис:

show loopback-detection [{ *interface-id* | **detailed** }]

Параметры:

- *interface-id* – идентификатор интерфейса;
- **detailed** - отображает информацию о неучтенных портах в дополнение к текущим портам.

Состояние по умолчанию:

Отображает информацию по всем портам. Если параметр **detailed** не указан, то выводится информация только по текущим портам.

Режим ИКС:

Привилегированный режим управления.

Примечания:

1. Операционный статус **Active** указывает на соответствие следующим условиям:
 - функция LBD включена глобально;
 - функция LBD включена на интерфейсе;
 - операционный статус интерфейса – UP;
 - статус STP на интерфейсе: Forwarding или STP отключено.
2. Операционный статус **LoopDetected** указывает на то, что интерфейс перевелся в состояние **errDisabled** (см. **set interface active** или **errdisable recovery cause** для дополнительной информации).
3. Операционный статус **Inactive** указывает на то, что функция LBD не определяет наличие петли, т.е. условия состояния **Active** не выполняются.

Пример:

```
console# show loopback-detection gi1/0/23

Loopback detection: Enabled
Loopback detection interval : 60

Interface Loopback Detection Loopback Detection
           Admin State       Operational State
-----
gi1/0/23      enabled         active
```

23. КОМАНДЫ НАСТРОЙКИ ACL УПРАВЛЕНИЯ УСТРОЙСТВОМ

23.1. команда allow

Команда **allow** режима конфигурации интерфейса предназначена для разрешения доступа на управление устройством через клиентские порты по определенным протоколам.

Синтаксис:

allow { http | https | telnet | ssh | snmp | ftp }

Параметры:

- **http** – разрешает доступ по протоколу HTTP.
- **https** – разрешает доступ по протоколу HTTPS.
- **telnet** – разрешает доступ по протоколу TELNET.
- **ssh** – разрешает доступ по протоколу SSH.
- **snmp** – разрешает доступ по протоколу SNMP.
- **ftp** – разрешает доступ по протоколу FTP.

Состояние по умолчанию:

Доступ через порты Ethernet отключен.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port-Channel).

Примечание:

Изначально удаленный доступ к устройству разрешен только через порт OOB. Данная команда применяется в тех случаях, когда необходимо предоставить доступ к устройству через клиентский порт.

Пример:

```
console(config)# interface GigabitEthernet 1/0/10
console(config-if)# allow ssh
```

23.2. Команда deny (Management)

Команда **deny** (Management) предназначена для задания запрещающих правил в списке доступа к управлению устройством.

Синтаксис:

deny [interface-id] [service service]

deny ip-source ipv4-address [mask { mask | prefix-length }] [interface-id] [service service]

Параметры:

- *interface-id* – идентификатор интерфейса. Допустимые типы: Ethernet, Port Channel или VLAN;

- *service* – задает тип сервиса. Доступные значения: Telnet, SSH, HTTP, HTTPS и SNMP;
- *ipv4-address* – IPv4 адрес источника;
- **mask** *mask* – маска сети для IPv4 адреса;
- **mask** *prefix-length* – префикс для IPv4 адреса. Диапазон: 0 – 32;

Состояние по умолчанию:

Списки доступа отсутствуют.

Режим ИКС:

Режим конфигурации списка доступа управления

Примечание:

Правила с идентификаторами Ethernet, VLAN или Port Channel действительны только в том случае, если на соответствующих интерфейсах задан IP-адрес.

Пример:

```
console(config)# management access-list One
console(config-macl)# deny vlan 1 service telnet
```

23.3. Команда permit (Management)

Команда **permit** (Management) предназначена для задания разрешающих правил в списке доступа к управлению устройством.

Синтаксис:

permit [*interface-id*] [**service** *service*]

permit ip-source *ipv4-address* [**mask** { *mask* | *prefix-length* }] [*interface-id*] [**service** *service*]

Параметры:

- *interface-id* – идентификатор интерфейса, допустимые типы: Ethernet, Port Channel или VLAN;
- *service* – задает тип сервиса, доступные значения: Telnet, SSH, HTTP, HTTPS и SNMP;
- *ipv4-address* – IPv4 адрес источника;
- **mask** *mask* – маска сети для IPv4 адреса;
- **mask** *prefix-length* – префикс для IPv4 адреса. Диапазон: 0 – 32.

Состояние по умолчанию:

Списки доступа отсутствуют.

Режим ИКС:

Режим конфигурации списка доступа управления

Примечание:

Правила с идентификаторами Ethernet, VLAN или Port Channel действительны только в том случае, если на соответствующих интерфейсах задан IP-адрес.

Пример:

```
console(config)# management access-list One
console(config-macl)# permit service ssh
```

23.4. Команда management access-list

Команда **management access-list** предназначена для создания списка доступа к управлению устройством и перехода в режим конфигурации списка доступа управления. Использование префикса «**no**» удаляет список.

Синтаксис:

management access-list *name*

no management access-list *name*

Параметры:

- *name* – имя списка доступа. Диапазон: 1 – 32 символа.

Состояние по умолчанию:

Списки доступа отсутствуют.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Если правила не определены, то по умолчанию для списка принимается **deny**.
2. При повторном входе в контекст списка доступа новые правила вводятся в конце списка.
3. Для активации созданного списка используется команда **management access-class**.
4. Активный список доступа не может быть удален или изменен.
5. Для управления трафиком IPv6 инкапсулированного в IPv4, правило применяется сначала во внешнем заголовке IPv4 (правила с полем обслуживания игнорируются), а затем во внутреннем заголовке IPv6.

Пример:

```
console(config)# management access-list One
console(config-macl)# deny vlan 1 service telnet
console(config-macl)# permit service ssh
```

23.5. Команда management access-class

Команда **management access-class** предназначена для активизации выбранного списка доступа к управлению устройством. Использование префикса «**no**» отключает список.

Синтаксис:

management access-class { console-only | *name* }

no management access-class

Параметры:

- **console-only** – для управления устройством используется только консольный порт;
- *name* – имя списка доступа.

Состояние по умолчанию:

По умолчанию никаких ограничений доступа к управлению нет.

Режим ИКС:

Режим глобальной конфигурации

Пример:

```
console(config)# management access-class One
```

23.6. Команда show management access-list

Команда **show management access-list** предназначена для отображения на экране списка доступа к управлению.

Синтаксис:

show management access-list [*name*]

Параметры:

- *name* – имя списка доступа.

Состояние по умолчанию:

Использование команды без параметров отображает все доступные списки доступа к управлению.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show management access-list

One
---
permit vlan 1 service ssh
permit ip-source 172.20.21.33 mask 255.255.255.0
! (Note: all other access implicitly denied)

console-only
-----
deny
```

! (Note: all other access implicitly denied)

23.7. Команда show management access-class

Команда **show management access-class** предназначена для отображения на экране активного списка доступа к управлению.

Синтаксис:

show management access-class

Параметры:

Дополнительные параметры отсутствуют.

Режим ИКС:

Привилегированный режим управления.

Пример:

```
console# show management access-class
Management access-class is enabled, using access-list One
```

24. КОМАНДЫ МАКРОСОВ

24.1. Команда `macro name`

Команда **macro name** предназначена для создания макросов.

Существует два типа макросов:

1. Глобальные макросы. Группа команд ИКС, которые можно запускать в любое время.
2. Макросы типа Smartport. Для каждого макроса данного типа должен быть определен анти-макрос (макрос имя которого объединено с префиксом «**no**»). Анти-макрос отменяет действие макроса.

Если макрос с таким именем уже существует, он переопределяет ранее определенный.

Использование префикса «**no**» удаляет созданный макрос.

Синтаксис:

macro name *macro-name*

no macro name [*macro-name*]

Параметры:

- *macro-name* – имя создаваемого макроса, имена макросов чувствительны к регистру.

Режим ИКС:

Режим глобальной конфигурации

Примечание:

Макрос – это скрипт, содержащий команды ИКС и которому присвоено имя. Скрипт может содержать до 3000 символов и 200 строк.

Ключевые слова.

Макросы могут содержать ключевые слова (параметры):

- макрос может содержать до трех ключевых слов;
- все совпадающие вхождения ключевого слова заменяются соответствующим значением, указанным в команде **macro**;
- ключевые слова чувствительны к регистру;
- применение макроса с ключевыми словами не изменяет состояние исходного определения макроса.

Обратная связь.

Поведение макроса, требующего обратной связи с пользователем такое же, как если бы команда была введена с терминала: она отправляет запрос на терминал и принимает ответ пользователя.

Создание макроса.

При создании макроса следует придерживаться следующих рекомендаций:

- использовать одну команду ИКС на строку;
- для завершения макроса используется символ @;
- для ввода комментариев в теле макроса используется символ # в начале строки. Кроме того, данный символ используется для идентификации некоторых команд препроцессора, которые могут использовать только в макросе. Возможны две команды препроцессора:
- **#macro key description** – каждый макрос может быть настроен с тремя парами параметр/описание. Параметры и описания отображаются при отображении макроса в GUI.

Синтаксис данной команды следующий:

#macro key description \$keyword1 description1 \$keyword2 description2 #keyword3 description3

Параметр должен иметь префикс \$.

- **#macro keyword** – эта команда позволяет устройству отображать ключевые слова как часть справки ИКС. Допускается до трех ключевых слов. Команда создает строку справки ИКС для макроса с ключевыми словами. Строка справки будет работать, если запрос выполнен из команд **macro** или **macro global**. GUI также использует параметры указанные в команде, как имена параметров макроса. В примерах 2 и 3 показано как используется эта команда.

Синтаксис данной команды следующий:

#macro keywords \$keyword1 \$keyword2 \$keyword3

Редактирование макроса.

Макросы нельзя редактировать. Необходимо создать новый макрос с таким же именем с соответствующими изменениями. Новый макрос перезапишет старый.

Область действия макроса.

Важно учитывать область действия макроса. Из-за потенциальной опасности непреднамеренных изменений конфигурации не рекомендуется изменять режимы конфигурации внутри макроса, используя такие команды как **exit**, **end** или **interface-id**. За некоторыми исключениями существуют другие способы выполнения макросов в различных режимах конфигурации.

Макросы могут выполняться в привилегированном режиме управления, режиме глобальной конфигурации и режиме конфигурации интерфейса (кроме интерфейса VLAN).

Примеры:

Пример 1:

В примере показано, как создать макрос, который настраивает дуплексный режим порта.

```
console(config)# macro name dup
Enter macro commands one per line. End with the character '@'.
#macro description duplex
duplex full
@
console(config)#
```

Пример 2:

В примере показано, как создать макрос с параметрами DUPLEX и SPEED. При выполнении макроса значения DUPLEX и SPEED вводятся пользователем.

```
console(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex $DUPLEX
speed $SPEED
#macro keywords $DUPLEX $SPEED
@
console(config)#
```

Пример 3:

В примере показано, как вывести ключевые слова с помощью символа «?» (которые определены командой #macro keywords в предыдущем примере), а затем выполнить макрос в режиме конфигурации порта.

```
console(config)# interface gil/0/10
WORD<1-32> Keyword to replace with a value e.g.
$DUPLEX, $SPEED
<CR>
console(config-if)# macro apply duplex $DUPLEX full $SPEED 100
```

24.2. Команда macro

Команда **macro** предназначена для выполнения макроса.

Синтаксис:

macro { apply | trace } macro-name [parameter-name1 value] [parameter-name2 value] [parameter-name3 value]

Параметры:

- **apply** – выполнить макрос;
- **trace** – выполнить с отображением выполнения команд;
- *macro-name* – имя выполняемого макроса;
- *parameter-name value* – для каждого параметра, заданного в макросе, необходимо указать его имя и значение. Можно ввести до трех пар параметр/значение. Ключевое слово параметра чувствительно к регистру. Все совпадающие вхождения имени параметра в макросе заменяются заданными значениями.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel).

Примечания:

1. Команда **macro apply** скрывает ход выполнения команд, заданных в макросе.
2. Команда **macro trace** отображает выполнение команд, вместе с любыми генерируемыми ошибками. Данный режим используется для отладки макроса, поиска синтаксических ошибок или ошибок конфигурации.
3. Если после запуска макроса одна из заданных в нем команд завершается с ошибкой, то макрос продолжает выполнять оставшиеся команды.
4. Если выполняется макрос, содержащий параметры в командах, то команда завершается с ошибкой, если необходимые значения не были указаны. Для отображения справки используется команда **macro apply macro-name ?** (если они определены с помощью команды препроцессора **#macro keywords**).
5. Параметр (ключевое слово) чувствителен к регистру. Все совпадающие вхождения параметра заменяются введенным значением.
6. Когда макрос применяется к интерфейсу, коммутатор автоматически генерирует команду описания макроса, включающую его имя. В результате имя макроса добавляется к истории выполненных макросов на интерфейсе. Команда **show parser macro** отображает историю макросов на интерфейсе.
7. Макрос, применяемый к диапазону интерфейсов ведет себя так же, как макрос примененный к одному интерфейсу. Когда макрос применяется к диапазону интерфейсов, он применяется последовательно к каждому интерфейсу в пределах диапазона. Если команда завершает работу с ошибкой на одном интерфейсе, то на остальных будет продолжена попытка ее выполнения, не зависимо от результатов ее выполнения.

Примеры:

Пример 1:

```
console(config)# interface gil/0/10
console(config-if)# macro trace duplex $DUPLEX full $SPEED 100
Applying command...'duplex full'
Applying command...'speed 100'
console(config-if)#
```

Пример 2:

```
console(config)# interface gil/0/10
console(config-if)# macro apply duplex $DUPLEX full $SPEED 100
console(config-if)#
```

24.3. Команда macro description

Команда **macro description** предназначена для добавления описания к макросу, например используемое в истории макросов. Использование префикса «**no**» очищает историю макросов на интерфейсе.

Когда макрос применяется на интерфейсе, коммутатор автоматически генерирует команду описания макроса с именем макроса. В результате имя макроса добавляется к истории макросов интерфейса.

Синтаксис:

macro description *text*

no macro description

Параметры:

- *text* – строка описания. Строка может содержать до 160 символов. Если строка содержит несколько слов, то она должна быть заключена в кавычки.

Состояние по умолчанию:

Команда не имеет настройки по умолчанию.

Режим ИКС:

Режим конфигурации интерфейса (Ethernet, Port Channel)

Примечания:

1. Если на интерфейсе применяется несколько макросов, текст описания представляет собой конкатенацию текстов из ранее примененных макросов.
2. Для проверки настроек, произведенных с помощью данной команды, необходимо выполнить команду **show parser macro**.

Пример:

```
console(config)# interface gil/0/9
console(config-if)# macro apply duplex $DUPLEX full $SPEED 100
console(config-if)# macro description duplex
console(config-if)# end
console# show parser macro description
Global Macro(s):
Interface Macro Description(s)
-----
gil/0/9    duplex
gil/0/10  duplex
-----
```

24.4. Команда macro global

Команда **macro global** предназначена для применения макроса глобально ко всему коммутатору.

Синтаксис:

macro global { **apply** | **trace** } *macro-name* [*parameter-name1 value*] [*parameter-name2 value*] [*parameter-name3 value*]

Параметры:

- **apply** – выполнить макрос;
- **trace** – выполнить с отображением выполнения команд;
- *macro-name* – имя выполняемого макроса;
- *parameter-name value* – Для каждого параметра, заданного в макросе, необходимо указать его имя и значение. Можно ввести до трех пар параметр/значение. Ключевое слово параметра чувствительно к регистру. Все совпадающие вхождения имени параметра в макросе заменяются заданными значениями.

Состояние по умолчанию:

Команда не имеет настройки по умолчанию.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Если команда завершает работу с ошибкой, макрос продолжит выполнение оставшихся команд.
2. Параметр (ключевое слово) чувствителен к регистру. Все совпадающие вхождения параметра заменяются введенным значением.
3. Если применяется макрос, содержащий ключевые слова в своих командах, то при пропуске значения для параметра команды завершит работу с ошибкой. Для отображения параметров до выполнения макроса необходимо использовать данную команду с добавлением «?». Определить параметры в строке справки можно используя ключевые слова **#macro keyword** в теле макроса.
4. Команда макрос применяется в режиме глобальной конфигурации, коммутатор автоматически генерирует описание с именем макроса. В результате имя макроса добавляется к глобальной истории макросов. Для отображения истории макросов используется команда **show parser macro**.

Пример:

```
console(config)# macro name console-timeout
Enter macro commands one per line. End with the character '@'.
line console
exec-timeout $TIME
@
console(config)# macro global trace console-timeout $TIME 0
Applying command...'line console'
Applying command...'exec-timeout 0'
console(config)#
```

24.5. Команда macro global description

Команда **macro global description** предназначена для добавления описания к макросу, используемое для указания того, какие макросы были применены к коммутатору.

Синтаксис:

macro global description *text*

no macro global description

Параметры:

- *text* – строка описания. Строка может содержать до 160 символов. Если строка содержит несколько слов, то она должна быть заключена в кавычки.

Состояние по умолчанию:

Команда не имеет настройки по умолчанию.

Режим ИКС:

Режим глобальной конфигурации

Примечания:

1. Если на интерфейсе применяется несколько макросов, текст описания представляет собой конкатенацию текстов из ранее примененных макросов.
2. Для проверки настроек, произведенных с помощью данной команды, необходимо выполнить команду **show parser macro**.

Пример:

```
console(config)# macro global description "set console timeout interval"
```

24.6. Команда show parser macro

Команда **show parser macro** предназначена для отображения на экране всех сконфигурированных макросов на устройстве.

Синтаксис:

```
show parser macro [ { brief | description [interface interface-id ] | name macro-name } ]
```

Параметры:

- **brief** – отображает только имена макросов;
- **description [interface *interface-id*]** – отображает описание для всех макросов или для заданного интерфейса;
- **name *macro-name*** – отображает информацию о макросе с заданным именем.

Состояние по умолчанию:

Отображает все макросы, существующие на устройстве.

Режим ИКС:

Привилегированный режим управления.

Примеры:

Пример 1:

```
console# show parser macro  
Total number of macros = 25  
-----
```

```
Macro name : ap
Macro type : default interface
 1.
 2. #macro description ap
 3. #macro keywords $native_vlan
 4. #
 5. #macro key description:  $native_vlan: The untag VLAN which
will be configured on the port
 6. #
 7. #Default Values are
 8. # $native_vlan = Default VLAN
 9. #
10. switchport trunk allowed vlan all
11. switchport trunk native vlan $native_vlan
12. switchport mode trunk
13. #
14. spanning-tree link-type point-to-point
-----

Macro name : no_ap
Macro type : default interface
 1.
 2. #macro description No ap
 3. #
 4. no switchport mode
 5. no switchport trunk allowed vlan
 6. no switchport trunk native vlan
 7. #
 8. no spanning-tree link-type
-----
```

Пример 2:

```
console# show parser macro name duplex
Macro name : duplex
Macro type : customizable
 1. duplex $DUPLEX
 2. speed $SPEED
 3. #macro keywords $DUPLEX $SPEED
 4.
```

Пример 3:

```
console# show parser macro brief
default interface : ap, no_ap
default interface : desktop, no_desktop
default interface : guest, no_guest
default interface : host, no_host
default interface : ip_camera, no_ip_camera
default interface : ip_phone, no_ip_phone
default interface : ip_phone_desktop, no_ip_phone_desktop
default interface : printer, no_printer
default interface : router, no_router
```

```
default interface : server, no_server  
default interface : switch, no_switch  
customizable      : console-timeout  
customizable      : duplex
```

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Определение
ЛВС	Локальная сеть;
ЛИНК	Нормальное состояние соединения сетевых интерфейсов;
ПЗУ	Постоянное запоминающее устройство;
ПК	Персональный компьютер;
ПО	Программное обеспечение;
ХОСТ	Любое сетевое устройство (коммутатор, маршрутизатор, сервер);
ЦПУ	Центральное процессорное устройство;
ACE	Англ. Access Control Element – правила доступа, входящие в список ACL;
ACL	Англ. Access Control List – список контроля доступа к интерфейсу устройства;
CIDR	Англ. Classless Inter-Domain Routing – бесклассовая адресация, метод IP-адресации;
DHCP	Англ. Dynamic Host Configuration Protocol – протокол динамической конфигурации узла;
GBIC	Англ. GigaBit Interface Converter – стандарт для передатчиков;
GUI	Англ. Graphical User Interface - графический пользовательский интерфейс;
HTTPS	Англ. HyperText Transfer Protocol Secure – расширение протокола HTTP, поддерживающее шифрование;
IP	Англ. Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP;
LACP	Англ. Link Aggregation Control Protocol – протокол, предназначенный для объединения нескольких физических каналов в один логический;
MAC	Англ. Media Access Control – управление доступом к среде;
RFC	Англ. Request for Comments – документ из серии пронумерованных информационных документов Интернета, охватывающих технические спецификации и Стандарты;
SFP/ SFP+	Англ. Small Form-factor Pluggable – промышленный стандарт модульных компактных приемопередатчиков;
SNTP	Англ. Simple Network Time Protocol – протокол синхронизации времени;
SSH	Англ. Secure Shell – сетевой протокол прикладного уровня;
TCAM	Англ. Ternary Content Addressable Memory - троичная ассоциативная

	память;
TFTP	Англ. Trivial File Transfer Protocol – простой протокол передачи файлов;
TTL	Англ. Time to Live – время жизни пакета данных в протоколе IP;
QoS	Англ. Quality of Service – качество обслуживания;
VLAN	Англ. Virtual Local Area Network - виртуальная локальная сеть.