ViPNet Coordinator HW 5

Справочник команд и конфигурационных файлов

Версия продукта: 5.3.2

ViPNet Coordinator HW50
ViPNet Coordinator HW100
ViPNet Coordinator HW1000
ViPNet Coordinator HW2000
ViPNet Coordinator HW5000
ViPNet Coordinator VA

infotecs

ФРКЕ.465614.003ИС3

Версия продукта 5.3.2

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение **19**
О документе 20
Соглашения документа 21
Обратная связь 23

Глава 1. Справочник команд **24**
Команды группы admin 25
admin certificate create 25
admin certificate delete 25
admin clear-auth-warning 26
admin escape 27
admin passwd 28
admin remove keys 28
admin show check integrity status 29
admin ssh reset-key 30
admin ssh reset-key local 30
admin ssh show-key 32
admin upgrade software 33
Команды группы alg 35
alg module direct-media 35
alg module h323 direct-h245 36
alg module process off 37
alg module process on 37
alg show 38
Команды группы failover 40
failover config edit 40
failover config mode 40
failover show active-mac-address 41
failover show config 42
failover show info 43
failover show sync-connections 45
failover start 45
failover stop 46
failover view 46

Команды группы firewall 48
firewall add 48
firewall add name 54
firewall change append 55
firewall delete 56
firewall move rule 58
firewall object delete 59
firewall object show 59
firewall rules log-blocked 60
firewall rules show 61
firewall settings 64
firewall settings show 66
firewall show 67
Команды группы inet 70
inet bgp 70
inet bgp as-path-filter add 70
inet bgp as-path-filter clear seq 71
inet bgp as-path-filter delete 72
inet bgp AS-path-filter seq 72
inet bgp clear 74
inet bgp community-list add 75
inet bgp community-list clear seq 75
inet bgp community-list delete 76
inet bgp community-list seq 76
inet bgp neighbor add 78
inet bgp neighbor delete 78
inet bgp neighbor remove advertise-map 79
inet bgp neighbor remove AS-path-filter 80
inet bgp neighbor remove password 80
inet bgp neighbor remove prefix-list 81
inet bgp neighbor remove route-map 81
inet bgp neighbor set advertise-map 82
inet bgp neighbor set AS-path-filter 83
inet bgp neighbor set default-originate 84
inet bgp neighbor set ebgp-multihop 84
inet bgp neighbor set next-hop-self 85
inet bgp neighbor set password 86
inet bgp neighbor set port 86
inet bgp neighbor set prefix-list 87

inet bgp neighbor set remote-as 88
inet bgp neighbor set route-map 88
inet bgp neighbor set ttl-security 89
inet bgp network add 90
inet bgp network delete 90
inet bgp network redistribute 91
inet bgp network redistribute route-map 92
inet bgp router as 92
inet bgp router bestpath AS-path-relax 93
inet bgp router bestpath bandwith 94
inet bgp router conditional-advertisement-timer 94
inet bgp router id 95
inet bgp router reset 96
inet bgp route-reflector client add 96
inet bgp route-reflector client delete 97
inet bgp route-reflector cluster-id 97
inet bgp route-reflector outbound-policy 98
inet bgp show 99
inet bgp show AS-path-filter 101
inet bgp show bestpath 102
inet bgp show community-list 102
inet bgp show neighbors 103
inet bgp show neighbors filters 108
inet bgp show neighbors list 110
inet bgp show network 111
inet bgp show route-reflector 112
inet bgp show summary 112
inet bonding add mode slaves 113
inet bonding delete 116
inet clear mac-address-table 116
inet dgd configuration default 117
inet dgd configuration interval-time 118
inet dgd configuration response-time 118
inet dgd configuration retries-count 119
inet dgd configuration syslog-level 120
inet dgd next-hop add 121
inet dgd next-hop delete 122
inet dgd mode 123
inet dgd rule add action-priority 123

inet dgd rule add match-next-hop 124
inet dgd rule clear 125
inet dgd rule delete action-priority 126
inet dgd rule delete match-next-hop 127
inet dhcp client route-default-metric 127
inet dhcp client route-distance 128
inet dhcp relay add backup-interface 129
inet dhcp relay add external-interface 129
inet dhcp relay add listen-interface 130
inet dhcp relay delete backup-interface 131
inet dhcp relay delete external-interface 132
inet dhcp relay delete listen-interface 133
inet dhcp relay mode 134
inet dhcp relay reset 135
inet dhcp relay start 135
inet dhcp relay stop 136
inet dhcp server add default-lease-time 137
inet dhcp server add dns 138
inet dhcp server add domain 139
inet dhcp server add host 140
inet dhcp server add interface 141
inet dhcp server add max-lease-time 141
inet dhcp server add ntp 142
inet dhcp server add option 143
inet dhcp server add range 144
inet dhcp server add relay-interface 145
inet dhcp server add router 146
inet dhcp server add subnet-mask 147
inet dhcp server add tftp 148
inet dhcp server add voip 149
inet dhcp server add wins 150
inet dhcp server delete default-lease-time 151
inet dhcp server delete dns 152
inet dhcp server delete domain 153
inet dhcp server delete host 153
inet dhcp server delete interface 154
inet dhcp server delete max-lease-time 155
inet dhcp server delete ntp 156
inet dhcp server delete option 157

inet dhcp server delete range 158
inet dhcp server delete relay-interface 159
inet dhcp server delete router 159
inet dhcp server delete subnet-mask 160
inet dhcp server delete tftp 161
inet dhcp server delete voip 162
inet dhcp server delete wins 163
inet dhcp server mode 163
inet dhcp server reset 164
inet dhcp server start 165
inet dhcp server stop 165
inet dns clients add 166
inet dns clients delete 166
inet dns clients list 167
inet dns forwarders add 168
inet dns forwarders delete 169
inet dns forwarders list 169
inet dns mode 170
inet dns querylog 171
inet dns querylog show 172
inet dns querylog size 172
inet dns start 173
inet dns stop 174
inet ifconfig address 174
inet ifconfig address add 175
inet ifconfig address delete 176
inet ifconfig bonding add 177
inet ifconfig bonding ad-select 178
inet ifconfig bonding delete 179
inet ifconfig bonding lacp-rate 179
inet ifconfig bonding miimon 180
inet ifconfig bonding primary 181
inet ifconfig bonding xmit-hash-policy 181
inet ifconfig class 182
inet ifconfig disable 183
inet ifconfig dhcp 184
inet ifconfig dhcp route-metric 185
inet ifconfig down 186
inet ifconfig enable 187

inet ifconfig mtu 187
inet ifconfig reset 188
inet ifconfig speed 190
inet ifconfig speed auto 191
inet ifconfig up 192
inet ifconfig vlan add 192
inet ifconfig vlan delete 193
inet ntp add 194
inet ntp delete 194
inet ntp list 195
inet ntp mode 196
inet ntp orphan 197
inet ntp start 197
inet ntp stop 198
inet ospf area auth 198
inet ospf interface keys add 199
inet ospf interface keys remove 200
inet ospf interface password 200
inet ospf mode 201
inet ospf network add 202
inet ospf network delete 203
inet ospf redistribute add 203
inet ospf redistribute delete 204
inet ospf priority 205
inet ospf router-id 206
inet ospf show configuration 206
inet ospf show database 208
inet ospf show neighbour 209
inet ping 209
inet policy active 211
inet policy rule add match 211
inet policy rule add 213
inet policy rule clear 214
inet policy rule delete match 215
inet policy rule delete 216
inet prefix-list add 217
inet prefix-list clear seq 217
inet prefix-list delete 218
inet prefix-list seq 219

inet prefix-list show 220
inet route add 221
inet route clear 222
inet route delete 223
inet route-map add 224
inet route-map clear 225
inet route-map delete 226
inet route-map match as-path 226
inet route-map match community 227
inet route-map match prefix-list 228
inet route-map on-match 228
inet route-map seq 229
inet route-map set as-path-prepend 230
inet route-map set community 231
inet route-map set local-preference 232
inet route-map set metric 232
inet route-map set next-hop 233
inet route-map set weight 234
inet route-map show 234
inet show dgd configuration 236
inet show dgd next-hop 236
inet show dgd rule 238
inet show dhcp client 239
inet show dhcp server 240
inet show dhcp server lease 240
inet show dhcp relay 242
inet show dns 242
inet show interface 243
inet show interface state 246
inet show mac-address-table 247
inet show ntp 249
inet show policy rule 250
inet show routing 251
inet show traffic 253
inet show usb-modem 254
inet show usb-modem chatscript 255
inet show usb-modem config 257
inet show usb-modem providers 257
inet show vlan 258

inet show wifi 259
inet snmp autostart 259
inet snmp cluster node community 260
inet snmp cluster node context 261
inet snmp cluster show 262
inet snmp cluster v2 263
inet snmp community add 263
inet snmp community change 264
inet snmp community delete 265
inet snmp community list 265
inet snmp logging 266
inet snmp port 267
inet snmp reset-engineid 268
inet snmp show 268
inet snmp start 269
inet snmp stop 270
inet snmp system contact 270
inet snmp system location 271
inet snmp system name 272
inet snmp trapsink add 273
inet snmp trapsink delete 274
inet snmp trapsink list 275
inet snmp user add 276
inet snmp user delete 277
inet snmp user list 277
inet snmp user set key 279
inet snmp user set name 280
inet snmp user set passwd 281
inet snmp user set read 282
inet snmp user set trapsess 282
inet snmp user set trapsess add 283
inet snmp user set trapsess delete 284
inet snmp v2 285
inet snmp v3 286
inet ssh 287
inet usb-modem add provider 288
inet usb-modem delete provider 288
inet usb-modem mode 289
inet usb-modem modify chatscript 289

inet usb-modem modify config ... 290
inet usb-modem reset pin ... 290
inet usb-modem set connection address ... 291
inet usb-modem set dns ... 291
inet usb-modem set password ... 292
inet usb-modem set phone ... 292
inet usb-modem set pin ... 293
inet usb-modem set provider ... 293
inet usb-modem set route ... 294
inet usb-modem set route-metric ... 295
inet usb-modem set user ... 295
inet vlan comment add ... 296
inet vlan comment delete ... 296
inet wifi access-point channel ... 297
inet wifi access-point hwmode ... 298
inet wifi access-point show ... 298
inet wifi authentication ... 299
inet wifi mode ... 300
inet wifi role ... 301
inet wifi scan ... 302
Команды группы iplir ... 303
iplir adapter add ... 303
iplir adapter delete ... 304
iplir adapter traffic ... 304
iplir config ... 305
iplir info ... 306
iplir option be-default-gateway ... 307
iplir option connection-server ... 308
iplir option interface-timeout ... 309
iplir option ip-forwarding ... 309
iplir option keepalive-timeout ... 310
iplir option maxtimediff ... 310
iplir option mode ... 311
iplir option mss-decrease ... 312
iplir option ping-timeout ... 313
iplir option show ... 313
iplir option sync-time ... 315
iplir option syslog-level ... 316
iplir option udp-ports-count ... 317

iplir ping 317
iplir set l2overip interface 318
iplir set l2overip local-port 319
iplir set l2overip mac-ttl 319
iplir set l2overip mode 320
iplir set l2overip remote-port 321
iplir set l2overip remote-port delete 321
iplir set l2overip unsolicited-frames 322
iplir node access-point 323
iplir node blockforward 324
iplir node domain-name 324
iplir node list 325
iplir node show 327
iplir node show domain-names 329
iplir node update domain-name cache 330
iplir set performance-mode 330
iplir show adapter 331
iplir show adapters 332
iplir show adapters groups 333
iplir show authentication-type 333
iplir show ciphertype 333
iplir show config 334
iplir show exchange-keys 335
iplir show firewall status 336
iplir show key-info 337
iplir show l2overip 339
iplir show performance-mode 340
iplir show tcptunnel-info 340
iplir start 341
iplir stop 342
iplir warning-threshold 342
iplir tcptunnel server 343
Команды группы machine 344
machine backup 344
machine backup export 345
machine backup schedule 346
machine config export usb 347
machine config import 348
machine halt 350

machine hosts add 351
machine hosts remove 351
machine hosts show 352
machine logs clear dns 353
machine logs export usb 353
machine logs export-and-clear usb 355
machine logs export network-traffic usb 356
machine logs settings 357
machine logs settings cef 358
machine logs settings cef event-type 358
machine logs settings network-traffic maxsize 359
machine logs settings network-traffic omit-client-port 360
machine logs settings network-traffic register 361
machine logs settings network-traffic timediff 362
machine logs settings show 362
machine logs show crypto-audit 364
machine logs show mftp 366
machine logs show network-traffic 367
machine logs show syslog 368
machine logs show user-audit 369
machine reboot 371
machine reboot-schedule 372
machine reboot-schedule show 372
machine reboot-schedule time 373
machine self-test 374
machine session-inactivity-timeout set 375
machine session-inactivity-timeout show 376
machine set date 376
machine set hostname 377
machine set loghost 378
machine set log invalid-packet 379
machine set log queue 379
machine set timezone 380
machine show backup 381
machine show date 382
machine show hostname 382
machine show loghost 383
machine show log invalid-packet 383
machine show log queue 384

machine show memory ... 384
machine show timezone ... 386
machine show uptime ... 386
machine update-queue ... 387
Команды группы mftp ... 389
mftp config ... 389
mftp info ... 390
mftp show config ... 391
mftp start ... 391
mftp stop ... 392
Команды группы service ... 393
service cert delete ... 393
service cert import ... 394
service cert list ... 395
service cert request create ... 396
service cert request delete ... 398
service cert request export ... 399
service cert request list ... 399
service cert request show ... 400
service cert show cert ... 400
service cert show crl ... 401
service dpi mode ... 402
service dpi show status ... 403
service dpi start ... 404
service dpi stop ... 404
service dpi update usb ... 405
service http-proxy antivirus bypass ... 406
service http-proxy antivirus mode ... 406
service http-proxy antivirus server-url add ... 407
service http-proxy antivirus server-url delete ... 408
service http-proxy antivirus server-url list ... 409
service http-proxy antivirus show-status ... 409
service http-proxy cache ... 410
service http-proxy content-filter add ... 410
service http-proxy content-filter change num ... 412
service http-proxy content-filter default-reply-action ... 414
service http-proxy content-filter default-request-action ... 415
service http-proxy content-filter delete ... 415
service http-proxy content-filter list ... 416

service http-proxy content-filter mode 417
service http-proxy content-filter move 417
service http-proxy content-filter show-status 418
service http-proxy external-address set 419
service http-proxy external-address show 419
service http-proxy fw-rules apply 420
service http-proxy fw-rules delete 420
service http-proxy fw-rules show 421
service http-proxy listen-address add 422
service http-proxy listen-address delete 422
service http-proxy listen-address list 423
service http-proxy mode 424
service http-proxy reset 424
service http-proxy show 425
service http-proxy start 425
service http-proxy stop 426
service http-proxy transparent-mode 426
service ips start 427
service ips stop 428
service ips mode 428
service ips rule restore-default 429
service ips rule update 430
service ips rule update fetch 430
service ips rule update server proxy address 431
service ips rule update server proxy port 432
service ips rule update schedule 432
service ips rule update server address 433
service ips rule update server login 434
service ips rule update server password 434
service ips rule update usb 435
service ips show status 436
service ips show update-settings 437
service ips syslog-level 438
service user-control 440
service user-control active-users 440
service user-control ad reset 441
service user-control ad show 442
service user-control ad set controller 443
service user-control ad set connection-timeout 444

service user-control ad set sync-delay ... 445
service user-control cp reset ... 445
service user-control cp set connection-secure ... 446
service user-control cp set connection-timeout ... 447
service user-control cp set custom-login-form ... 447
service user-control cp set hostcert ... 448
service user-control cp set idle-timeout ... 449
service user-control cp set ldap ... 449
service user-control cp set ldap cacert ... 450
service user-control cp show ... 451
service user-control fw-rules apply ... 452
service user-control fw-rules delete ... 452
service user-control fw-rules show ... 453
service user-control mode ... 453
service user-control show ... 454
service user-control syslog-level ... 455
service vpn mode ... 455
service vpn show status ... 456
service vpn start ... 457
service vpn stop ... 457
Команды группы ups ... 459
ups set driver ... 459
ups set mode ... 459
ups set monitoring ... 460
ups show config ... 461
ups show status ... 461
ups start ... 462
ups stop ... 463
Команды группы vpn ... 464
vpn config delete ... 464
vpn config list ... 464
vpn config load ... 465
vpn config save ... 466
vpn start ... 467
vpn stop ... 467
Команды группы webui ... 469
webui https-cert ... 469
webui info ... 469
webui port ... 470

webui protocol ... 471
webui recreate-cert ... 472
webui restart ... 473
Прочие команды ... 474
debug off ... 474
debug on ... 475
enable ... 476
exit ... 476
license ... 477
serial ... 478
user certificate create ... 478
user certificate delete ... 479
user passwd ... 480
user reset passwd ... 481
version ... 481
version features list ... 483
who ... 483

Глава 2. Справочник конфигурационных файлов ... 485
Файл iplir.conf ... 486
Секция [adapter] ... 486
Секция [debug] ... 487
Секция [dynamic] ... 488
Секция [id] ... 488
Секция [misc] ... 494
Секция [servers] ... 496
Секция [virtualip] ... 496
Секция [visibility] ... 497
Файл iplir.conf-<интерфейс или группа интерфейсов> ... 499
Секция [db] ... 499
Секция [cef] ... 501
Файл failover.ini ... 502
Секция [channel] ... 502
Секция [debug] ... 504
Секция [misc] ... 505
Секция [network] ... 506
Секция [sendconfig] ... 508
Файл mftp.conf ... 510
Секция [channel] ... 510

Секция [debug] ... 511
Секция [journal] ... 512
Секция [misc] ... 513
Секция [reserv] ... 515
Секция [transport] ... 516
Секция [upgrade] ... 516

Приложение A. Список служб ПО ViPNet Coordinator HW ... 518

Приложение B. События системного журнала и журнала аудита ... 520
События Linux ... 520
События, инициированные пользователями ... 521
События запуска и остановки служб ... 528
События системы защиты от сбоев ... 530
События обмена служебной информацией между узлами ViPNet ... 531
События об ошибках ДСЧ и шифратора ... 532
События антивирусной проверки и контент-фильтрации ... 533

Приложение C. Термины и сокращения ... 534

Введение

О документе 20

Соглашения документа 21

Обратная связь 23

О документе

Документ содержит описание команд, доступных для выполнения в командном интерпретаторе многофункционального шлюза безопасности ViPNet Coordinator HW. В описании команды приводятся: назначение, синтаксис, параметры и ключевые слова, режим и особенности использования, а также примеры. Команды сгруппированы по первому ключевому слову, список групп и список команд внутри каждой группы упорядочены по алфавиту.

Также в документе приведено описание параметров конфигурационных файлов:

- `iplir.conf` — конфигурационный файл управляющей службы;
- `iplir.conf-<интерфейс или группа интерфейсов>` — конфигурационные файлы сетевых интерфейсов;
- `failover.ini` — конфигурационный файл системы защиты от сбоев;
- `mftp.conf` — конфигурационный файл транспортного сервера MFTP.

Нередактируемые параметры конфигурационных файлов задаются автоматически и носят информационный характер. Такие описаны в специальных подразделах. Изменять их значения вручную не следует.

Справочно приведены список служб ПО ViPNet Coordinator HW и описание событий системного журнала и журнала аудита.

Соглашения документа

Внимание! Все сценарии работы с ViPNet Coordinator HW приведены для локального администратора `admin` в режимах просмотра или настройки.

Обозначение	Описание
	**Внимание!** Содержит критически важную информацию
	**Примечание.** Содержит рекомендательную информацию
	**Совет.** Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, службы, интерфейса, путь или команда

Описание команд:

- Приглашение команд, которые могут быть выполнены аудитором или администратором в режиме просмотра, заканчивается символом `>`:

  ```
  hostname> firewall local show
  ```

- Приглашение команд, которые могут быть выполнены администратором в режиме настройки, заканчивается символом `#`:

  ```
  hostname# admin upgrade software
  ```

- Параметры, которые должны быть заданы аудитором или администратором, заключены в угловые скобки `<>`:

  ```
  inet bonding delete <номер>
  ```

  При вводе в командный интерпретатор параметры вводятся без угловых скобок:

  ```
  hostname# inet bonding delete 1
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки `[]`:

  ```
  firewall <тип> add name @<имя> <состав> [exclude <исключения>]
  ```

  При вводе в командный интерпретатор необязательные параметры или ключевые слова вводятся без квадратных скобок:

  ```
  hostname# firewall ip-object add name @IP_group_1 110.35.14.0/24 exclude
  110.35.14.3,110.35.14.13
  ```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки `{}` и разделены вертикальной чертой `|`:

  ```
  inet ntp mode {on | off}
  ```

  При вводе в командный интерпретатор выбранные варианты параметров вводятся без фигурных скобок:

  ```
  hostname# inet ntp mode off
  ```

- Идентификатор сетевого узла ViPNet указывается в шестнадцатеричном формате с префиксом `0x`:

  ```
  hostname# iplir ping 0x270e000a
  ```

Обратная связь

Контактная информация

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телеграм-канал поддержки: t.me/vhd21

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- О продуктах ViPNet.
- О решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется политикой ответственного разглашения.

1

Справочник команд

Команды группы admin 25

Команды группы alg 35

Команды группы failover 40

Команды группы firewall 48

Команды группы inet 70

Команды группы iplir 303

Команды группы machine 344

Команды группы mftp 389

Команды группы service 393

Команды группы ups 459

Команды группы vpn 464

Команды группы webui 469

Прочие команды 474

Команды группы admin

Управление доступом локального администратора и SSH-ключами, обновление ПО и другие административные задачи.

admin certificate create

Издать или перевыпустить сертификат локального администратора `admin`.

Синтаксис

```
admin certificate create
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда может быть выполнена от имени локального (`admin`) или централизованного администратора.
- При выполнении команды введите ПИН администратора USB-токена, затем введите и подтвердите ПИН пользователя (требования к ним см. в документации на USB-токен).

Пример использования

```
hostname# admin certificate create
Insert token and press Enter
Upon executing the command, you will lost all current token data. Continue? [Yes/No]: y
Enter admin-token pincode: ********
Enter new user-token pincode: ********
Confirm new user-token pincode: ********
Certificate has been successfully created.
```

admin certificate delete

Удалить сертификат локального администратора `admin`.

Синтаксис

```
admin certificate delete
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда может быть выполнена от имени локального (`admin`) или централизованного администратора.
- После выполнения команды локальное подключение администратора `admin` к ViPNet Coordinator HW с помощью консоли будет заблокировано. При этом остается доступным удаленное подключение по SSH и HTTP/HTTPS.

Пример использования

```
hostname# admin certificate delete

Upon executing the command, you will not be able to log on with user account. Continue?
[Yes/No]: y

Certificate has been successfully deleted.
```

admin clear-auth-warning

Сбросить счётчик попыток подбора пароля.

Синтаксис

```
admin clear-auth-warning
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Значение счётчика не изменяется при следующих операциях с ViPNet Coordinator HW:
  - перезагрузка;
  - обновление ПО;
  - проверка целостности ПО;
  - восстановление конфигурации.
- В кластере команда выполняется на активном узле.

Пример использования

```
hostname# admin clear-auth-warning

Password guessing counter was cleared.
```

admin escape

Выйти в системную командную оболочку shell.

Внимание! Команда предназначена для использования опытными администраторами в целях отладки. ИнфоТеКС не гарантирует нормальную работу ViPNet Coordinator HW в случае некорректных действий администратора в системной командной оболочке.

Синтаксис

```
admin escape
```

Режимы командного интерпретатора

- Режим настройки.

Особенности использования

- При вводе команды автозаполнение не работает.
- При выполнении команды требуется указать пароль локального администратора `admin`.
- Команда устанавливает глобальную блокировку управляющих запросов. В других сессиях пользователя, выполнившего команду, доступен только просмотр параметров. Сессии всех остальных пользователей завершаются.
- Для выхода из системной командной оболочки необходимо выполнить команду `exit`.

Пример использования

```
hostname# admin escape
This command is intended only for debugging.
It should be used only by InfoTeCS support team or people who
 were explicitly advised by InfoTeCS support team to use it.
InfoTeCS does not guarantee normal operation of Platform: HW
 in case of incorrect user actions in the system shell.
Are you sure you want to exit to the Linux system shell?
Continue? [Yes/No]: Yes
Type the administrator password:
sh-4.4#
```

admin passwd

Изменить пароль локального администратора `admin`.

Синтаксис

```
admin passwd
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Требования к паролю:
  - Длина пароля: 6–31 символ.
  - Допустимые символы:
    - Прописные и строчные буквы латинского алфавита: `A–Z`, `a–z`.
    - Арабские цифры: `0–9`.
    - Специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- При вводе пароля вводимые символы не отображаются.
- В кластере команда выполняется только на активном узле.

Пример использования

```
hostname# admin passwd
Enter new admin password:
Confirm new admin password:
```

admin remove keys

Удалить ключи и справочники ViPNet Coordinator HW.

Синтаксис

```
admin remove keys
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда недоступна в удаленной SSH-сессии.
- Если на ViPNet Coordinator HW запущен DHCP-сервер, то его работа будет автоматически завершена.
- Команда устанавливает глобальную блокировку управляющих запросов; сессии всех пользователей завершаются.

Пример использования

```
hostname# admin remove keys
This command deletes all VPN keys and cannot be reverted.
You will need to deploy keys anew after executing this command.
Are you sure you want to execute this command?
Continue? [Yes/No]: Yes
DHCP server is already off. Command ignored.
DNS server is already off. Command ignored.
NTP server is already off. Command ignored.
Stopping all VPN services
...
server login:
```

admin show check integrity status

Просмотреть информацию о последней проверке целостности файлов:

- время последней проверки;
- результаты проверки.

Синтаксис

```
admin show check integrity status
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname# admin show check integrity status
Sat Feb 13 02:18:31 YEKT 2024
Total:
1 PRG files checked, 1 checks passed, 0 checks failed
188 files checked, 188 checks passed, 0 files corrupted, 0 checks failed
Check file bzImage successfully
Check file initramfs-va successfully
```

```
Check file fs_main.tgz successfully
Check file sysimg.dat successfully
Check file vpnimg.dat successfully
Sat Feb 13 02:21:12 Periodic control passed successfully
```

admin ssh reset-key

Удалить отпечатки SSH-ключей, хранящиеся локально на ViPNet Coordinator HW.

Синтаксис

```
admin ssh reset-key {host <адрес> | id <идентификатор>}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сервера, чей отпечаток SSH-ключа необходимо удалить.
- `<идентификатор>` — идентификатор сервера, чей отпечаток SSH-ключа необходимо удалить.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Для параметра `id` при двойном нажатии **Tab** выводится подсказка со списком всех идентификаторов серверов, с которыми есть связи.

Пример использования

Чтобы удалить отпечаток SSH-ключа для сервера `ssh.domain.com`:

```
hostname# admin ssh reset-key host ssh.domain.com
```

admin ssh reset-key local

Перевыпустить ключи локального SSH-сервера ViPNet Coordinator HW.

Синтаксис

```
admin ssh reset-key local
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# admin ssh reset-key local

command: admin ssh remove key local

Reseting DSA-Hostkey...

Generating public/private dsa key pair.

Your identification has been saved in /mnt/main/etc/ssh/ssh_host_dsa_key.

Your public key has been saved in /mnt/main/etc/ssh/ssh_host_dsa_key.pub.

The key fingerprint is:

SHA256:TvsHXJ9ybY3Rmoy2L8Pfut5JN0TpdLNuOkp3nuXaisw root@hostname

The key's randomart image is:

+---[DSA 1024]----+

|                 |

|                .|

|               *.|

|             . = =|

|        S. . + @.|

|       o .o + @ +|

|        o  = = Bo|

|         ..oBo*=*|

|          .oEBXO=|

+----[SHA256]-----+

Reseting RSA-Hostkey...

Generating public/private rsa key pair.

Your identification has been saved in /mnt/main/etc/ssh/ssh_host_rsa_key.

Your public key has been saved in /mnt/main/etc/ssh/ssh_host_rsa_key.pub.

The key fingerprint is:

SHA256:Q6PlZVt8y5eEh+lnC3yuP5CS6u2P8H4CTkA3xyOFOEY root@hostname

The key's randomart image is:

+---[RSA 2048]----+

|      .E. +.     |

|       = = =  +  |

|      o * * ++.o |

|       * + oooo..|

|      . S . .++=.|
```

```
|          + o o*..|
|         o.o . .o |
|          o+..... |
|         ..o*+o...|
+----[SHA256]-----+
```

admin ssh show-key

Просмотреть информацию об SSH-ключах, хранящихся локально на ViPNet Coordinator HW.

Синтаксис

```
admin ssh show-key {host <адрес> | id <идентификатор> | local}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сервера, чей отпечаток SSH-ключа необходимо просмотреть.
- `<идентификатор>` — идентификатор сервера, чей отпечаток SSH-ключа необходимо просмотреть.
- `local` — просмотр информации о ключах локального SSH-сервера.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Для параметра `id` при двойном нажатии **Tab** выводится подсказка со списком всех идентификаторов серверов, с которыми есть связи.
- В результате выполнения команды выводится:
  - `Key type` — тип ключа:
    - `ssh-dsa(ssh2)` — SSH-ключ, сгенерированный с использованием алгоритма dsa;
    - `ssh-rsa(ssh2)` — SSH-ключ, сгенерированный с использованием алгоритма rsa;
  - `Fingerprint` — отпечаток SSH-ключа;
  - `Public key` — открытый SSH-ключ.

Пример использования

Чтобы просмотреть информацию о ключах локального SSH-сервера:

```
hostname# admin ssh show-key local

command: admin ssh show key local

Local host ssh public keys:

============================================================

Key type: ssh-dsa(ssh2)

Fingerprint: SHA256:Q5/e7nofhVTre1K72AWf0V0K1FxqUysfVxMQP0PnIuw

Public key:
AAAAB3NzaC1kc3MAAACBAOiitldq9nRVKx72gOR4nVVPotoAdjJvgJRbYs9mLvJdmypb4Y+JvG8GLQZvODJCnI
KzWLJ2eUJi5/iVTOfBwHt9oXo+W+K4JaVwUaQq0uEHj6YbhPk6mIlV+TIBfCbSP5r9quQCFdnn4IKcVng7rVKu
dl8geMKW0GQGrOtZl9pRAAAAFQC2iqrroLE+zS6qmAkM2x/iOCzeiQAAAIEAxBbdKDITOtJDNykwYuCPnCgWZu
jXz0oUUxAOsp+dVYcsnevRN6IiM51gTAUDRR5AKPkY7M5ma3EOXAZTrdKj+Y7NePt4smEQQat93L+nKgoNDjf+
oUnQFh07XkK0eydX3/xCO0M+pn/VvICDjXP6DdpDmXr01Gy389wakaqHZX4AAACBAJYC9XgjKgnLRcKjmSVLuA
/yZ/YFk3P0LJUmSRe4yzV16v2uLlRH8rEfTGVllMWuDX47ZmRhpemoM3QbvkFAFMBkmbqZzrn8nFARLAoP1syS
2CO3gaEFkmeQ/d7rL7HRq05tH2e4gUX2ZxWJQHNYgprj8r5gKPWyN6zBCRJ0GF8U

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

Key type: ssh-rsa(ssh2)

Fingerprint: SHA256:Txn8IloRmfAbD+l/F6/UWah4DfwGu2cKXDGiDE5VXQk

Public key:
AAAAB3NzaC1yc2EAAAADAQABAAABAQDgRfTwzDnmxg3GCofsWFqOlh96opUuTz1zkPA1c70ncnyNtkW6kmaeXx
MU3EM7r/yf3/e/U6JH5Pkc6bWcYbU70tEBy3db9ZDY/QdOBZdijIagUuWyiiHqAEWwC1vCXqQ1/0AZwh71DKTD
PFI0cImTC3ahMJMtvl/X7SnWJVxVz3AMBqXnTqjMXOpHDXQnAgPw4kcTNqZMNT1OOvaYmcCGZ6Tko7HPygy1n+
ZUV/GajAlwTmCfKr0DT/O3ebi9OF7SK6A5eJeGCVBRv2BdOhL/uWzuaMSP6vMk+hiWkX0lNl6iOUIo4PCHW8kH
m6FcaJAmG0MKVw8M2dDo0osTtUhz

------------------------------------------------------------
```

admin upgrade software

Обновить ПО ViPNet Coordinator HW вручную с USB-носителя или CD-диска.

Синтаксис

```
admin upgrade software
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Для обновления ПО необходимо подключиться к ViPNet Coordinator HW с помощью консоли локально. Выполнить обновление в удаленной SSH-сессии невозможно.
- Для обновления ПО необходимы:

    - файл обновления ПО: `<платформа ViPNet Coordinator HW>_vipnet_base_x86_64_driv_<версия ViPNet Coordinator HW>.zip`, например, `hw1000_vipnet_base_x86_64_driv_5.0.0-2388.zip`;
    - файл ЭП обновления: `<платформа ViPNet Coordinator HW>_vipnet_base_x86_64_driv_<версия ViPNet Coordinator HW>.zip.sig`.
- Файл обновления ПО и файл ЭП обновления должны находиться в одном каталоге USB-носителя или CD-диска.
- После обновления ПО необходимо перезагрузить ViPNet Coordinator HW.
- Команда устанавливает глобальную блокировку управляющих запросов; сессии всех пользователей завершаются.

Пример использования

```
hostname# admin upgrade software
Insert USB flash drive or CD and press <Enter>
Checking integrity and signature of 'hw1000_vipnet_base_x86_64_driv_5.1.0-3669.zip'
Select file to use for software upgrade:
1 — /mnt/tmp/sdb1/hw1000_vipnet_base_x86_64_driv_5.1.0-3669.zip
Enter file number [1-1] or [q] to cancel: 1
Starting local upgrade...
...
System is upgrading and will be rebooted in process
```

Команды группы alg

Управление обработкой прикладных протоколов.

alg module direct-media

Настроить передачу медиапотоков между клиентами при обработке прикладных протоколов `H.323` или `SIP`.

Синтаксис

```
alg module <прикладной протокол> direct-media {on | off}
```

Параметры и ключевые слова

- `<прикладной протокол>` — протокол: `h323` или `sip`
- `on` — передача медиапотоков между клиентами через сервер.
- `off` — передача медиапотоков между клиентами напрямую.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию задана передача медиапотоков между клиентами через сервер.
- Если настроить передачу медиапотоков между клиентами напрямую, то определяющими будут настройки протокола на клиентах, в зависимости от которых медиапотоки могут передаваться или напрямую, или через сервер.
- Чтобы настройка вступила в силу, выполните:

  ```
  hostname# vpn stop
  hostname# vpn start
  ```

- На ViPNet Coordinator HW, установленном на границе защищаемой сети, рекомендуется запретить передачу медиапотоков между клиентами напрямую.

Пример использования

Чтобы настроить передачу медиапотоков между SIP-клиентами напрямую:

1 На ViPNet Coordinator HW выполните:

```
hostname# alg module sip direct-media off
```

```
hostname# vpn stop
hostname# vpn start
```

2 В настройках SIP-клиентов задайте передачу медиапотоков напрямую.

alg module h323 direct-h245

Настроить согласование параметров связи между клиентами при обработке сигнального протокола `H.245`.

Синтаксис

```
alg module h323 direct-h245 {on | off}
```

Параметры и ключевые слова

- `on` — согласование параметров связи между клиентами через сервер.
- `off` — согласование параметров связи между клиентами напрямую.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию задано согласование параметров связи между клиентами через сервер.
- Если настроить согласование параметров связи между клиентами напрямую, то определяющими будут настройки протокола H.245 на клиентах, в зависимости от которых параметры связи могут согласовываться или напрямую, или через сервер.
- Чтобы настройка вступила в силу, выполните:

  ```
  hostname# vpn stop
  hostname# vpn start
  ```

- На ViPNet Coordinator HW, установленном на границе защищаемой сети, рекомендуется запретить согласование параметров связи между клиентами напрямую.

Пример использования

Чтобы настроить согласование параметров связи между H.323-клиентами напрямую:

```
hostname# alg module h323 direct-h245 off
hostname# vpn stop
hostname# vpn start
```

alg module process off

Выключить обработку прикладного протокола DNS, FTP, H.323, SCCP или SIP.

Синтаксис

```
alg module <прикладной протокол> process off
```

Параметры и ключевые слова

<прикладной протокол> — имя прикладного протокола: dns, ftp, h323, sccp или sip.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

По умолчанию включена обработка всех прикладных протоколов.

Пример использования

Чтобы выключить обработку прикладного протокола DNS:

```
hostname# alg module dns process off
```

alg module process on

Включить обработку прикладного протокола DNS, FTP, H.323, SCCP, SIP, или изменить параметры обработки этого протокола.

Синтаксис

```
alg module <прикладной протокол> process {tcp | udp} <порты> on
```

Параметры и ключевые слова

- <прикладной протокол> — имя обрабатываемого прикладного протокола: dns, ftp, h323, sccp или sip.
- tcp — транспортный протокол TCP для обработки прикладного протокола sip, h323, ftp или sccp.
- udp — транспортный протокол UDP для обработки прикладного протокола sip, h323 или dns.
- <порты> — номера портов для обработки.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию включена обработка всех прикладных протоколов.
- В качестве портов можно указать один порт, диапазон портов либо список портов и диапазонов портов, перечисленных через запятую.

Пример использования

Чтобы включить обработку прикладного протокола `FTP` по портам `20`, `21` и `26` для протокола `TCP`:

```
hostname# alg module ftp process tcp 20-21,26 on
```

alg show

Просмотреть текущие параметры обработки прикладных протоколов `DNS`, `FTP`, `H.323`, `SCCP`, `SIP`.

Синтаксис

```
alg show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- На экране отображаются:
  - `H323 direct media` — передача медиапотоков между клиентами: `ON` (через сервер) или `OFF` (напрямую).
  - `H323 direct h245` — согласование параметров связи между клиентами: `ON` (через сервер) или `OFF` (напрямую).
  - `SIP direct media` — передача медиапотоков между клиентами: `ON` (через сервер) или `OFF` (напрямую).
  - `ALG TCP connections synchronization` — состояние синхронизации сессий прикладных протоколов:
    - `ON` — включена, система защиты от сбоев в режиме кластера.
    - `OFF` — выключена, система защиты от сбоев в режиме кластера.
    - `Failover daemon is stopped` — система защиты от сбоев в одиночном режиме.

- SERVICE — прикладной протокол: DNS, FTP, H.323, SCCP, SIP.
- PROTOCOL — транспортный протокол: TCP, UDP.
- PORTS — порты TCP, UDP.
- ON/OFF — состояние обработки: ON (включена) или OFF (выключена).

- В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname> alg show

H323 direct media: off

H323 direct h245: off

SIP direct media: off

ALG TCP connections synchronization: ON
================================================================================
SERVICE        PROTOCOL PORTS                                           ON/OFF
================================================================================
FTP            TCP      21                                              ON
--------------------------------------------------------------------------------
DNS            UDP      53                                              ON
--------------------------------------------------------------------------------
H323           TCP      1720                                            ON
--------------------------------------------------------------------------------
H323           UDP      1719                                            ON
--------------------------------------------------------------------------------
SCCP           TCP      2000                                            ON
--------------------------------------------------------------------------------
SIP            TCP      5060,5080                                       ON
--------------------------------------------------------------------------------
SIP            UDP      5060,5080                                       ON
--------------------------------------------------------------------------------
```

Команды группы failover

Настройка и управление системой защиты от сбоев ViPNet Coordinator HW.

failover config edit

Редактировать конфигурационный файл системы защиты от сбоев failover.ini.

Синтаксис

```
failover config edit
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- После изменения файла `failover.ini` перезапустите службу `failoverd` с помощью команд failover stop и failover start.
- В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname# failover config edit
GNU nano 2.3.6     File: /etc/failover.ini
[network]
checktime = 10
timeout = 2
activeretries = 3
channelretries = 3
synctime = 5
fastdown = yes
...
The file failover.ini is changed
Changes will be applied after restart of failover daemon
```

failover config mode

Задать режим работы системы защиты от сбоев.

Синтаксис

```
failover config mode {single | cluster}
```

Параметры и ключевые слова

- `single` — одиночный режим.
- `cluster` — режим кластера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию установлен одиночный режим (`single`).
- В кластере команда доступна для выполнения на обоих узлах.
- При переключении в режим кластера автоматически будет завершена работа драйверов и служб, которые в нем не поддерживаются.

Пример использования

Чтобы переключить систему защиты от сбоев в режим кластера:

```
hostname# failover config mode cluster
Note: the following services are NOT allowed to run in cluster mode:
        DHCP
If any of them are currently running, stop them.
Do you want to stop all services that are not allowed to run in cluster mode now?[Yes/No]:
Yes
You have approved services stopping. Proceeding...
Switching to cluster mode. Attempt to stop the following service: DHCP
DHCP server is STOPPED. Command is ignored
Installing ViPNet failover system
```

failover show active-mac-address

Просмотреть доступность активного узла кластера со стороны пассивного узла.

Синтаксис

```
failover show active-mac-address
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Команда выполняется на пассивном узле кластера.
- При доступности активного узла кластера будет выведен список активных интерфейсов кластера, заданных параметрами `device` и `activeip` секций `[channel` (см. Секция [channel]), и их MAC-адреса.

Пример использования

- Если активный узел кластера доступен:

```
hostname> failover show active-mac-address
Address check is in progress …
Interface          IP-address           MAC-address
eth0               10.0.2.10            38:D5:47:C9:DA:4C
eth1               10.0.3.10            C9:DA:4C:C9:DA:4C
```

- Если активный узел кластера недоступен:

```
hostname> failover show active-mac-address
eth0         10.0.2.10  NA
eth1         10.0.3.10  NA
```

failover show config

Просмотреть конфигурационный файл системы защиты от сбоев failover.ini.

Синтаксис

```
failover show config
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Чтобы завершить просмотр файла конфигурации, нажмите **Q**.
- В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname> failover show config
[network]
checktime = 10
timeout = 2
```

```
activeretries = 3
channelretries = 3
synctime = 5
fastdown = yes
...
```

failover show info

Просмотреть текущее состояние системы защиты от сбоев.

Синтаксис

```
failover show info
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются:

- `versions` — версии ПО ViPNet Coordinator HW и системы защиты от сбоев;
- `ID` — идентификатор и имя узла ViPNet;
- `workstation time` — локальное время на узле ViPNet;
- `failover mode` — система защиты от сбоев:
  - `single` — одиночный режим;
  - `active` — режим активного узла кластера;
  - `passive` — режим пассивного узла кластера;
- `failover uptime` — время непрерывной работы системы защиты от сбоев;
- `total cpu` — общая загруженность процессора;
- `total memory` — общий объем памяти;
- `available memory` — объем доступной памяти;
- сведения о текущем состоянии служб failover, iplir, mftp, webgui, uc, controld, aad, external-controld, licd (см. Список служб ПО ViPNet Coordinator HW):
  - статус службы:
    - `initializing` — загружается;
    - `works` — работает;
    - `stopped` — работа завершена;

- `unknown` — неизвестно (например, если произошел сбой в работе службы, была произведена попытка ее перезапуска, и данных о ее состоянии пока нет);

- сведения о ресурсах процессора, используемых службой.

Пример использования

```
hostname> failover show info

Running failover info

Versions: ViPNet 5.3.1 (2763), daemon 1.5 (1)

Workstation configured for ID 383D009A (Coordinator_HW)

The workstation works in a single mode of protection against failures

Workstation time (utc: 1636536224) Wed Nov 10 12:23:44 2024

failover mode       * single

failover uptime           * 0d 19:45

total cpu                 * 0%

total memory              * 2053620 Kb

available memory          * 1423600 Kb

failover state            * works

failover cpu              * 0%

iplir state               * works

iplir cpu                 * 0%

mftp state                * works

mftp cpu                  * 0%

webgui state              * works

webgui cpu                * 0%

uc state                  * stopped

controld state            * works

controld cpu              * 0%

aad state                 * works

aad cpu                   * 0%

external-controld state   * works

external-controld cpu     * 0%

licd state                * works

licd cpu                  * 0%
```

failover show sync-connections

Просмотреть количество сетевых соединений в кеше узла кластера.

Синтаксис

```
failover show sync-connections
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Для выполнения команды включите в синхронизацию соединений в кластере (см. описание параметра `syncconnections` секции `[misc]` конфигурационного файла `failover.ini`).
- Команда доступна для выполнения только в кластере.

Пример использования

```
hostname> failover show sync-connections

Synchronized connections count         150000
```

failover start

Запустить службу системы защиты от сбоев `failoverd`.

Синтаксис

```
failover start [{active | passive}]
```

Параметры и ключевые слова

Режим узла в кластере:

- `active` — активный;
- `passive` — пассивный.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- В кластере команда доступна для выполнения на обоих узлах.
- Параметры `active` и `passive` доступны, если для системы защиты от сбоев задан режим кластера.
- Если в режиме кластера не указан режим узла, служба `failoverd` будет запущена в том режиме, в котором она находилась до завершения работы.
- Перед запуском службы `failoverd` в активном режиме узла убедитесь, что на другом узле кластера служба `failoverd` запущена в пассивном режиме. Запуск службы `failoverd` в активном режиме на обоих узлах кластера приведет к конфликту IP-адресов.

Пример использования

Чтобы запустить службу `failoverd` в пассивном режиме работы узла:

```
hostname# failover start passive
```

failover stop

Завершить работу службы системы защиты от сбоев `failoverd`.

Синтаксис

```
failover stop
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname# failover stop
Shutting down failover daemon
```

failover view

Просмотреть журнал переключений кластера за заданный период времени.

Синтаксис

```
failover view <начало> <конец>
```

Параметры и ключевые слова

- `<начало>` — начало периода. Указывается в формате `DD.MM.YYYY[.hh.mm.ss]`, где `DD` — день, `MM` — месяц, `YYYY` — год, `hh` — час, `mm` — минуты, `ss` — секунды. Время можно не задавать.
- `<конец>` — конец периода. Указывается в том же формате, что и начало периода.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Команда доступна только в кластере.
- Чтобы завершить просмотр журнала, нажмите **Q**.

Пример использования

```
hostname> failover view 09.03.2024.08.00.00 23.03.2024.19.00.00
  View journal of failover switching
  Versions: ViPNet 5.3.1 (3935), daemon 1.5 (1)
  Workstation configured for ID 1031F
  The workstation works in a cluster mode of protection against failures
  Workstation time (utc: 1174916969) Mon Mar 29 17:49:29 2024

  09 Mar 2024 12:51:42     <P_START> Start failover daemon in passive mode
  22 Mar 2024 12:27:27     <A_START> Start failover daemon in active mode
  22 Mar 2024 14:10:35     <A_START> Start failover daemon in active mode
  22 Mar 2024 15:30:46     <BOOT> Boot the system
23 Mar 2024 11:09:07       <SWITCH> Switch server from passive mode to active mode
```

Команды группы firewall

Работа с сетевыми фильтрами, правилами трансляции адресов и группами объектов.

firewall add

Создать сетевой фильтр или правило трансляции адресов.

Синтаксис

```
firewall <тип> add [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя>
[<транспортный протокол>] [dpiapp <приложение>] [dpiprotocol <прикладной протокол>]
[dpigroup <группа приложений>] [dnuser <пользователь>] [<расписание>] [log {on | off}]
<действие>
```

Параметры и ключевые слова

- `<тип>` — тип создаваемого сетевого фильтра или указание на создание правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `tunnel` — фильтр туннелируемых узлов;
  - `vpn` — фильтр защищенной сети;
  - `nat` — правило трансляции адресов;
- `<номер>` — порядковый номер фильтра или правила трансляции в таблице, определяющий его приоритет;
- `<имя>` — имя фильтра или правила трансляции;
- `<адрес отправителя>` — адрес отправителя IP-пакетов;
- `<адрес получателя>` — адрес получателя IP-пакетов;
- `<транспортный протокол>` — транспортный протокол, по которому передаются IP-пакеты;
- для фильтров туннелируемых узлов и транзитных фильтров открытой сети:
  - `<приложение>` — приложение;
  - `<прикладной протокол>` — прикладной протокол;
  - `<группа приложений>` — группа приложений;
  - `<пользователь>` — пользователь Active Directory или Captive Portal.
- `<расписание>` — расписание применения фильтра или правила трансляции;
- `log` — регистрация IP-пакетов при срабатывании фильтра в журнале IP-пакетов;

- `<действие>` — действие с IP-пакетами, соответствующими условиям фильтра или правила трансляции.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если номер не указан, фильтр (правило трансляции) добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика в последнюю очередь.
- Если указанный номер меньше последнего номера в таблице, нумерация фильтров (правил трансляции), следующих за новым фильтром (правилом трансляции), будет автоматически изменена (их номера будут увеличены на 1).
- В качестве адреса отправителя или получателя можно указать следующее:
  - для локальных фильтров открытой сети — IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску адресов подсети, доменное имя сети, системную группу объектов `any`, `local` или `remote`, одну или несколько пользовательских групп IP-адресов;
  - для транзитных фильтров открытой сети: то же, что для локальных фильтров открытой сети, но в таких фильтрах нельзя использовать системные группы объектов;
  - для фильтров защищенной сети — идентификатор узла или сети ViPNet, список идентификаторов узлов и сетей ViPNet, системные группы объектов `any`, `allcoordinators`, `allclients`, `local` или `remote`, одну или несколько пользовательских групп узлов ViPNet; кроме того:
    - один из адресов (отправителя или получателя) должен быть `local`;
    - если адрес источника не `local`, то адрес получателя должен быть `local`/`broadcast`.
  - для фильтров туннелируемых узлов — то же, что для локальных фильтров открытой сети и фильтров защищенной сети, но в таких фильтрах можно использовать только системные группы объектов `any`, `allcoordinators`, `allclients` или `tunneledip`;
  - для правил трансляции адресов — IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску адресов подсети, доменное имя сети, одну или несколько пользовательских групп IP-адресов.
- В качестве адреса отправителя для локальных и транзитных фильтров открытой сети, а также фильтров туннелируемых узлов можно указать сетевой интерфейс собственного узла в виде:

  ```
  src interface {<системное имя интерфейса> | @<имя группы интерфейсов> | byip {<IP-адрес> | <диапазон IP-адресов> | <маска подсети>}}
  ```

- В качестве адреса отправителя для локальных и транзитных фильтров открытой сети, а также фильтров туннелируемых узлов одновременно можно указать и системную группу объектов (`local`, `remote`, `multicast`, `broadcast` кроме `any`), и сетевой интерфейс собственного узла:

  ```
  src <системная группа объектов> interface {<системное имя интерфейса> | @<имя группы интерфейсов> | byip {<IP-адрес> | <диапазон IP-адресов> | <маска подсети>}}
  ```

- В качестве адреса получателя можно указать:
  - для локальных фильтров открытой сети — системную группу `broadcast` или `multicast`;
  - для фильтров защищенной сети — системную группу `broadcast`.
- При задании доменного имени в качестве адреса получателя нельзя использовать кириллицу.
- Транспортный протокол можно указать, используя следующее:
  - имена протоколов, написанные строчными буквами и разделенные пробелами. При этом можно также задать дополнительные параметры для протоколов:
    - TCP и UDP: `sport` (порт или диапазон портов источника пакета) и/или `dport` (порт или диапазон портов назначения пакета). При использовании обоих этих параметров сначала необходимо указать параметр `sport`, затем — параметр `dport`. Возможно указать несколько портов или диапазонов портов, в этом случае необходимо указать название протокола (`tcp` или `udp`) перед каждым номером порта (диапазоном портов). Например: `tcp sport 2525 tcp dport 443 tcp dport 4444-4445`.
    - ICMP: только параметр `type` (тип пакета) либо параметр `type` вместе с параметром `code` (код пакета). Если параметр `code` не задан, то под условие будут подпадать все ICMP-пакеты указанного типа;
  - номера протоколов. При этом перед номером каждого протокола необходимо указать ключевое слово `proto`;
  - пользовательские группы протоколов в виде: `service @<имя группы>`.

  При создании правила трансляции с использованием порта назначения указание адреса назначения и транспортного протокола TCP или UDP обязательно.
- Приложение необходимо указывать по его названию (см. документ «Настройка с помощью командного интерпретатора», приложение «Поддерживаемые приложения»). Вы можете указать несколько приложений в списке через запятую. При задании приложения, содержащего пробелы, его название необходимо заключить в двойные кавычки:

  ```
  dpiapp "Google Mail",Skype,Facebook
  ```
- Прикладной протокол необходимо указывать по его названию (см. документ «Настройка с помощью командного интерпретатора», приложение «Поддерживаемые прикладные протоколы»). Вы можете указать несколько протоколов в списке через запятую. При задании протокола, содержащего пробелы, его название необходимо заключить в двойные кавычки:

  ```
  dpiprotocol "Skype for Business",HTTP,SSL
  ```

  Если вы задали в фильтре приложение, то вы можете указать только те прикладные протоколы, которые относятся к этому приложению.
- Группу приложений необходимо указывать по ее названию (см. документ «Настройка и управление с помощью командного интерпретатора», приложение «Поддерживаемые группы приложений»). Вы можете указать несколько групп приложений в списке через запятую. При задании группы приложений, содержащей пробелы, ее название необходимо заключить в двойные кавычки:

  ```
  dpigroup "Voice over IP","Remote Control",Streaming
  ```

В одном фильтре указывать к группам приложений и прикладных протоколов `dpigroup` дополнительные приложения `dpiapp` и прикладные протоколы `dpiprotocol` запрещено.

- Пользователя необходимо указывать, используя его доменное имя (без указания имени самого домена) или имя, зарегистрированное на Captive portal. Вы можете указать несколько пользователей в списке через запятую:

  `dnuser ivanov_v,petrov_a`

- Расписание задается одной из следующих лексем:
  - `daily <чч:мм>-<чч:мм>` — фильтр действует ежедневно в течение заданного интервала времени. Время указывается в 24-часовом формате: `чч` — часы, `мм` — минуты.
  - `weekly [mo] [tu] [we] [th] [fr] [sa] [su] [at <чч:мм>-<чч:мм>]` — фильтр действует еженедельно в заданные дни недели:
    - `mo` — понедельник,
    - `tu` — вторник,
    - `we` — среда,
    - `th` — четверг,
    - `fr` — пятница,
    - `sa` — суббота,
    - `su` — воскресенье.
  - `calendar <дд.мм.гггг>-<дд.мм.гггг> [at <чч:мм>-<чч:мм>]` — фильтр действует в заданные даты и интервал времени. Дата указывается в следующем формате:
    - `дд` — день,
    - `мм` — месяц,
    - `гггг` — год.
  - `schedule @<имя группы объектов>` — фильтр действует по расписанию, описанному группой объектов соответствующего типа.

  Также для задания расписания можно использовать соответствующие пользовательские группы объектов.

  

  Примечание. Расписание действует для новых сессий. Если сессия была открыта до начала действия расписания, то она будет работать до момента ее завершения. Например, в сетевом фильтре, разрешающем работу по протоколу RDP, задано расписание с 9:00 до 20:00. В этом случае пользователь, открывший RDP-сессию до 20:00, сможет работать в ней и после 20:00 до тех пор, пока она не будет завершена. После этого пользователь уже не сможет открыть новую RDP-сессию.

- Регистрация IP-пакетов при срабатывании фильтра в журнале IP-пакетов задается лексемой `log`:
  - `on` — регистрировать IP-пакеты;
  - `off` — не регистрировать IP-пакеты.

Значение по умолчанию:

- `off` — для фильтра с действием пропускать (`pass`);
- `on` — для фильтра с действием блокировать (`drop`) или отклонить (`reject`).

- Действие задается одной из следующих лексем:
  - для сетевых фильтров:
    - `pass` — пропускать IP-пакеты;
    - `drop` — блокировать IP-пакеты;
  - для сетевых фильтров при необходимости отклонить IP-пакеты с отправкой ICMP-сообщения об ошибке:
    - `reject` — отправляет сообщение `Destination port unreachable`;
    - `rej-net-unreachable` — отправляет сообщение `Destination net unreachable`;
    - `rej-host-unreachable` — отправляет сообщение `Destination host unreachable`;
    - `rej-proto-unreachable` — отправляет сообщение `Destination protocol unreachable`;
    - `rej-net-prohibited` — отправляет сообщение `Network administratively prohibited`;
    - `rej-host-prohibited` — отправляет сообщение `Host administratively prohibited`;
    - `rej-admin-prohibited` — отправляет сообщение `Communication administratively prohibited`;
    - `rej-tcp-reset` — отправляет сообщение `TCP reset` (только для TCP-пакетов);

    

    Внимание! При создании сетевых фильтров нельзя задавать блокировку IP-пакетов с отправкой ICMP-сообщения совместно с параметрами, задающими фильтрацию по пользователю, приложению или прикладному протоколу. Такие параметры задаются следующими лексемами: `dpiapp, dpiprotocol, dpigroup, dnuser`.

  - для правил трансляции адресов:
    - `change src {<адрес отправителя> | auto}` — заменять адрес отправителя пакетов на указанный адрес (внешний адрес координатора или адрес из другой сети) или автоматически на публичный адрес внешнего сетевого интерфейса координатора;

      

      Примечание. При использование в `change src` IP-адреса, не принадлежащего ViPNet Coordinator HW, на сетевом устройстве, расположенным за ViPNet Coordinator HW, настройте обратную маршрутизацию на ViPNet Coordinator HW (или на другое устройство, например для балансировки) для корректной обработки ответного трафика.

      Если на сетевом устройстве нельзя настроить обратную маршрутизацию, используйте в `change src` только IP-адреса, принадлежащие ViPNet Coordinator HW, или автоматическое определение адреса исходящего интерфейса (`auto`).

    - `change dst <адрес>:[<порт>]` — перенаправлять пакеты на указанные адрес и порт.

Подробнее см. в документе «Настройка с помощью командного интерпретатора», в главах «Настройка сетевых фильтров» и «Настройка правил трансляции адресов».

Примеры использования

- Чтобы создать локальный фильтр, блокирующий IP-пакеты, отправляемые узлом с адресом 192.168.30.1 через порт 2525 на порты 443, 4444-4445 открытого узла с адресом 172.16.35.1 по протоколу TCP/IP, выполните команду:

  ```
  hostname# firewall local add 2 rule "Rule 2" src 192.168.30.1 dst 172.16.35.1 tcp sport 2525 tcp dport 443 tcp dport 4444-4445 drop
  ```

- Чтобы создать фильтр, разрешающий отправку IP-пакетов от защищенного узла с идентификатором 0x1234abab туннелируемому узлу с адресом 192.168.0.1 ежедневно в интервал с 8 утра до 8 вечера и регистрировать его срабатывание в журнале IP-пакетов, выполните команду:

  ```
  hostname# firewall tunnel add src 0x1234abab dst 192.168.0.1 daily 8:00-20:00 log on pass
  ```

- Чтобы при отправке пакета внешним узлом с адресом mydomain.ru узлу с адресом 192.168.20.1 по протоколу TCP/IP через порт 8080 ViPNet Coordinator HW подменял адрес получателя (публичный IP-адрес ViPNet Coordinator HW) на локальный адрес, создайте правило трансляции адреса назначения с помощью команды:

  ```
  hostname# firewall nat add src mydomain.ru dst 192.168.20.1 tcp dport 8080 change dst 10.0.0.7:8080
  ```

- Чтобы при отправке пакета узлом с адресом 10.0.0.1 внешнему узлу с адресом 192.168.20.1 частный адрес отправителя пакета заменялся на публичный адрес внешнего сетевого интерфейса ViPNet Coordinator HW, создайте правило трансляции адреса источника с помощью команды:

  ```
  hostname# firewall nat add src 10.0.0.1 dst 192.168.20.1 change src auto
  ```

- Чтобы создать транзитный фильтр, блокирующий IP-пакеты приложения Skype по протоколу SSL для пользователя `ivanov`, выполните команду:

  ```
  hostname# firewall forward add src @any dst @any dpiapp skype dpiprotocol SSL dnuser ivanov drop
  ```

- Чтобы создать транзитный фильтр с номером 333, запрещающий MPEG и SSL трафик с ресурсов Youtube и Vimeo для пользователей `PetrovPP` и `SidorovKP`, выполните команду:

  ```
  hostname# firewall forward add 333 src @any dst @any dpiapp Youtube,Vimeo dpiprotocol MPEG,SSL dnuser PetrovPP,SidorovKP drop
  ```

- Чтобы создать транзитный фильтр открытой сети с номером 444, запрещающий трафик мессенджеров и онлайн-трансляций (группа `Messaging` и `Streaming`) для пользователей `PetrovPP` и `SidorovKP`, выполните команду:

  ```
  hostname# firewall forward add 444 src @any dst @any dpigroup Messaging,Streaming dnuser PetrovPP,SidorovKP drop
  ```

- Чтобы создать локальный фильтр, блокирующий все IP-пакеты, отправляемые на порт 3128 по протоколу TCP/IP с отправкой icmp-уведомления `destination host unreachable`, выполните команду:

  ```
  hostname# firewall local add src @any dst @any tcp dport 3218 rej-host-unreachable
  ```

firewall add name

Создать группу объектов заданного типа.

Синтаксис

```
firewall <тип> add name @<имя> <состав> [exclude <исключения>]
```

Параметры и ключевые слова

- `<тип>` — тип объектов. Можно указать одно из следующих значений:
  - `ip-object` — IP-адреса;
  - `vpn-object` — сетевые узлы ViPNet;
  - `interface-object` — сетевые интерфейсы;
  - `service-object` — протоколы;
  - `schedule-object` — расписания.
- `<имя>` — имя группы объектов.
- `<состав>` — объекты, входящие в группу.
- `<исключения>` — объекты, не входящие в группу.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Имя группы объектов должно быть уникальным и не должно содержать пробелов и символов «"».
- Сетевые интерфейсы разделяйте пробелом, и перед именем каждого сетевого интерфейса укажите слово `interface`.
- Синтаксис протокола и расписания — тот же, что при создании сетевого фильтра или правила трансляции адресов с помощью команды firewall add.

Примеры использования

- Чтобы создать группу IP-адресов, содержащую сегмент сети за исключением нескольких IP-адресов:

  ```
  hostname# firewall ip-object add name @IP_group_1 110.35.14.0/24 exclude
  110.35.14.3,110.35.14.13
  ```

- Чтобы создать группу расписания, содержащую выходные дни с 9 до 23 часов:

```
hostname# firewall schedule-object add name @weekend weekly sa su at 09:00-23:00
```

- Чтобы создать группу сетевых интерфейсов, содержащую интерфейсы `eth0` и `eth1`:

```
hostname# firewall interface-object add name @intgroup interface eth0 interface eth1
```

firewall change append

Добавить адрес отправителя, адрес получателя, протокол или расписание в сетевой фильтр или правило трансляции адресов.

Синтаксис

```
firewall <тип> change append [<номер>] [rule <имя>] src <адрес отправителя> dst <адрес получателя> [<транспортный протокол>] [dpiapp <приложение>] [dpiprotocol <прикладной протокол>] [dpigroup <группа приложений>] [dnuser <пользователь>] [<расписание>] log {on | off}
```

Параметры и ключевые слова

- `<тип>` — тип изменяемого сетевого фильтра или указание на изменение правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `tunnel` — фильтр туннелируемых узлов;
  - `vpn` — фильтр защищенной сети;
  - `nat` — правило трансляции адресов.
- `<номер>` — порядковый номер фильтра или правила трансляции в таблице.
- `<имя>` — имя фильтра.
- `<адрес отправителя>` — добавляемый адрес отправителя IP-пакетов.
- `<адрес получателя>` — добавляемый адрес получателя IP-пакетов.
- `<транспортный протокол>` — добавляемый протокол, по которому передаются IP-пакеты.
- Для транзитных фильтров открытой сети и фильтров туннелируемых узлов:
  - `<приложение>` — приложение.
  - `<прикладной протокол>` — прикладной протокол.
  - `<группа приложений>` — группа приложений.
  - `<пользователь>` — пользователь Active Directory или LDAP-сервера.
- `<расписание>` — добавляемое расписание применения фильтра или правила трансляции;
- `log` — регистрация IP-пакетов при срабатывании фильтра в журнале IP-пакетов:
  - `on` — регистрировать IP-пакеты;

- `off` — не регистрировать IP-пакеты.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Синтаксис адреса отправителя, адреса получателя, транспортного протокола, приложения, прикладного протокола, группы приложений, пользователя и расписания — тот же, что при создании сетевого фильтра или правила трансляции с помощью команды firewall add.
- Можно указать несколько параметров.
- Для транзитных фильтров открытой сети и фильтров туннелируемых узлов можно задать несколько значений параметров `<приложение>`, `<прикладной протокол>`, `<группа приложений>` и `<пользователь>`. Значения в списке разделяются запятой. Значение, содержащее пробелы, заключается в двойные кавычки.

Пример использования

Пусть существует локальный фильтр открытой сети, созданный с помощью следующей команды:

```
hostname# firewall local add 8 rule "Rule8" src 192.168.1.0/24 dst 10.0.0.1 drop
```

Чтобы добавить в этот фильтр еще один адрес отправителя и расписание, по которому фильтр будет применяться только в выходные дни с 9 до 23 часов, выполните команду:

```
hostname# firewall local change append 8 src 192.168.2.2 weekly sa su at 09:00-23:00
```

Чтобы к транзитному фильтру открытой сети с номером 333 добавить запрет Flash трафика, ресурса Вконтакте и пользователей MakarovTP и DeryuginAA, выполните команду:

```
hostname# firewall forward change append 333 dpiapp VK dpiprotocol Flash dnuser
MakarovTP,DeryugiAA
```

Чтобы к транзитному правилу открытой сети с номером 333 добавить запрет игрового трафика (группа приложений Gaming) для пользователей MakarovTP и DeryuginAA, выполните команду:

```
hostname# firewall forward change append 333 dpigroup Gaming dnuser MakarovTP,DeryuginAA
```

firewall delete

Удалить сетевой фильтр или правило трансляции адресов.

Синтаксис

```
firewall <тип> delete <параметры>
```

Параметры и ключевые слова

- `<тип>` — тип удаляемого сетевого фильтра или указание на удаление правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `tunnel` — фильтр туннелируемых узлов;
  - `vpn` — фильтр защищенной сети;
  - `nat` — правило трансляции адресов.
- `<параметры>` — параметры фильтра или правила трансляции для удаления. Можно указать следующие параметры: порядковый номер, имя, адрес отправителя, адрес получателя, протокол, действие фильтра или правила.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Синтаксис адреса отправителя, адреса получателя, протокола и расписания — тот же, что при создании фильтра или правила трансляции с помощью команды firewall add.
- Можно указать несколько параметров.
- Поиск фильтров или правил трансляции для удаления осуществляется по строгому совпадению с заданными параметрами.
- Номера фильтров или правил трансляции, следующих за удаленным фильтром или правилом трансляции, автоматически уменьшаются на 1.

Пример использования

Чтобы удалить локальный фильтр открытой сети с номером 7:

```
hostname# firewall local delete 7
================================================================================
Num    Name                                          Option  Schedule
Act    Protocol               Source                -> Destination
                                                     DomainUser
================================================================================
7      Allow DHCP server req                         User
pass   udp:                   @local                -> @any
        from 67
        to 68                                        @any
       @any                   @any
--------------------------------------------------------------------------------
Do you want to perform the action on the above rule? [Yes/No]:y
```

firewall move rule

Изменить порядковый номер (приоритет) сетевого фильтра или правила трансляции адресов в таблице.

Синтаксис

```
firewall <тип> move rule <текущий номер> to <новый номер>
```

Параметры и ключевые слова

- `<тип>` — тип изменяемого сетевого фильтра или указание на изменение правила трансляции адресов:
  - `local` — локальный фильтр открытой сети;
  - `forward` — транзитный фильтр открытой сети;
  - `tunnel` — фильтр туннелируемых узлов;
  - `vpn` — фильтр защищенной сети;
  - `nat` — правило трансляции адресов.
- `<текущий номер>` — текущий порядковый номер фильтра (правила трансляции).
- `<новый номер>` — новый порядковый номер фильтра (правила трансляции).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При изменении порядкового номера соответственно изменяется приоритет фильтра (правила трансляции) при обработке трафика.
- Нумерация фильтров (правил трансляции), следующих за перемещенным фильтром (правилом трансляции), изменяется автоматически (их номера увеличиваются на 1).
- Невозможно изменить порядковый номер, если новый номер больше последнего номера в таблице.

Пример использования

Чтобы переместить локальный фильтр с девятого на восьмое место в таблице (то есть сделать его более приоритетным):

```
hostname# firewall local move rule 9 to 8
```

firewall object delete

Удалить группу объектов с заданным именем.

Синтаксис

```
firewall object delete @<имя>
```

Параметры и ключевые слова

`<имя>` — имя группы объектов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если группа используется в каких-либо сетевых фильтрах, правилах трансляции адресов или других группах объектов, то в результате выполнения данной команды появится сообщение об ошибке, содержащее список всех фильтров, правил или групп, которые используют данную группу. В этом случае сначала удалите эти фильтры, правила и группы, а затем выполните команду для удаления группы еще раз.
- Для команды не поддерживается автодополнение.

Пример использования

Чтобы удалить группу объектов с именем `IP_group`:

```
hostname# firewall object delete @IP_group
```

firewall object show

Просмотреть все группы объектов.

Синтаксис

```
firewall object show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Группы каждого типа объектов выводятся в отдельной таблице, где:
  - `Num` — порядковый номер группы;
  - `Name` — имя группы;
  - `Creation Type` — вид группы: для групп из Policy Management (модуль ViPNet Prime) — `Policy`, для пользовательских групп — `User`;
  - `Inclusion` — объекты, входящие в группу;
  - `Exclusion` — объекты, не входящие в группу;
- Чтобы завершить просмотр, нажмите **Q**.

Пример использования

```
hostname> firewall object show
Ip Objects
================================================================================
Num  Name                                          Creation type
Inclusion                          Exclusion
================================================================================
1    PrivateNetworkIP                              User
10.0.0.0/255.0.0.0, 172.16.0.0/
255.240.0.0, 192.168.0.0/255.255.0.0
--------------------------------------------------------------------------------
2    InternetIP                                    User
@any                               @PrivateNetworkIP
--------------------------------------------------------------------------------
Service Objects
================================================================================
Num  Name                                          Creation type
Inclusion                          Exclusion
================================================================================
1    DHCP                                          User
udp: from 67-68 to 67-68
--------------------------------------------------------------------------------
2    CITRIX                                        User
tcp: to 1494
--------------------------------------------------------------------------------
...
```

firewall rules log-blocked

Включить регистрацию IP-пакетов при срабатывании всех настраиваемых фильтров с действиями блокировать (`drop`) и отклонить (`reject`).

Синтаксис

```
firewall rules log-blocked
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При выполнении команды необходимо подтвердить действие — ввести `Yes` и нажать **Enter**.

Пример использования

```
hostname# firewall rules log-blocked
This will turn on logging for all user rules with action drop or reject.
Continue? [Yes/No]: Yes
```

firewall rules show

Просмотреть все сетевые фильтры и правила трансляции адресов, заданные в ViPNet Coordinator HW.

Синтаксис

```
firewall rules show [{pass | drop | reject}]
```

Параметры и ключевые слова

- `pass` — отображать сетевые фильтры с действием `pass`.
- `drop` — отображать сетевые фильтры с действием `drop`.
- `reject` — отображать сетевые фильтры с действием `reject`.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Для завершения просмотра нажмите клавишу **Q**.
- Если параметр не указан, будут выведены все сетевые фильтры и правила трансляции адресов.
- Каждый тип сетевых фильтров и правила трансляции адресов выводятся в отдельной таблице, содержащей:

- `Num` — порядковый номер фильтра или правила трансляции в таблице.
- `Rule ID-Name` — идентификатор и имя фильтра или правила трансляции. Если для фильтра включена регистрация IP-пакетов при его срабатывании, то перед именем фильтра отображается префикс `[LOG]`.
- `Option` — категория фильтра или правила трансляции.
- `Schedule` — расписание применения фильтра или правила трансляции.
- `Act` — действие фильтра или правила трансляции.
- `Protocol` — протокол, по которому передаются IP-пакеты.
- `Source` — адрес отправителя IP-пакетов.
- `Destination` — адрес получателя IP-пакетов.
- Для транзитных фильтров открытой сети и фильтров туннелируемых узлов:
  - `DpiProtocol` — прикладной протокол.
  - `DpiApp` — приложение.
  - `[G]DpiGroup` — группа приложений.
  - `DomainUser` — пользователь Active Directory или Captive Portal.

Пример использования

В примере показаны только правила с номером 1 для каждого типа фильтров или правил:

```
hostname> firewall rules show

 Service Vpn Rules:

================================================================================

Num    Name                                          Option  Schedule

Act    Protocol               Source                 -> Destination

       DpiProtocol            [G]DpiGroup, DpiApp       DomainUser

================================================================================

1      Block not original udp                           Generated

drop   port                   @local                 -> @any

       udp:

        from 0-2045

        to 2046,

       udp:

        from 2047-65535                                 @any

        to 2046               @any

       @any
```

```
--------------------------------------------------------------------------------
 Vpn Rules:
================================================================================
Num    Name                                          Option  Schedule
Act    Protocol               Source                -> Destination
       DpiProtocol            [G]DpiGroup, DpiApp       DomainUser
================================================================================
1      ICMP redirect in                                 User
drop   icmp: 5                @any                  -> @local
                                                        @any
       @any                   @any
--------------------------------------------------------------------------------
empty rule for  Nat Rules:
 Tunnel Rules:
================================================================================
Num    Name                                          Option  Schedule
Act    Protocol               Source                -> Destination
       DpiProtocol            [G]DpiGroup, DpiApp       DomainUser
================================================================================
1      To all tunnel nodes                              User
pass   @any                   @any                  -> @tunneledip
                                                        @any
       @any                   @any
--------------------------------------------------------------------------------
 Service Local Rules:
================================================================================
Num    Name                                          Option  Schedule
Act    Protocol               Source                -> Destination
       DpiProtocol            [G]DpiGroup, DpiApp       DomainUser
================================================================================
1      ViPNet Service Common                            Generated
drop   In                     @any                  -> @local
       tcp/udp:
        to 2046,
```

```
       tcp/udp:
        to 2047,
       tcp/udp:
        to 10096,
       tcp/udp:
        to 5100,
       tcp/udp:                                          @any
        to 10092              @any
       @any
-------------------------------------------------------------------------------
 Local Rules:
===============================================================================
Num    Name                                             Option  Schedule
Act    Protocol               Source                 -> Destination
       DpiProtocol            [G]DpiGroup, DpiApp       DomainUser
===============================================================================
1      ICMP redirect out                                User
drop   icmp: 5                @local                 -> @any
                                                        @any
       @any                   @any
-------------------------------------------------------------------------------
empty rule for  Forward Rules:
```

firewall settings

Задать параметры межсетевого экрана ViPNet Coordinator HW.

Синтаксис

```
firewall settings <параметр> <значение>
```

Параметры и ключевые слова

- `antispoofing` —фильтрация в режиме Strict Reverse Path Forwarding по RFC3704: включена — `on` или выключена — `off` (по умолчанию);

- `block-fragmented-packets` — блокирование входящих фрагментированных IP-пакетов, принимаемых на всех сетевых интерфейсах: включено — `on` или выключено — `off` (по умолчанию);
- `bypass-tunnel-ips-dpi` — обход обработки туннельного трафика подсистемами DPI и IPS: включен — `on` или выключен — `off` (по умолчанию);
- `connection-ttl-ip` — время жизни соединений по протоколам, отличным от TCP, UDP и ICMP, при отсутствии в них активности; возможные значения: 0–65535 секунд; по умолчанию — 60;
- `connection-ttl-tcp` — время жизни TCP-соединений при отсутствии в них активности; возможные значения: 0–65535 секунд; по умолчанию — 1800;
- `connection-ttl-udp` — время жизни UDP-соединений при отсутствии в них активности; возможные значения: 0–65535 секунд; по умолчанию — 300;
- `max-connections` — максимальное количество одновременно открытых соединений; значение по умолчанию и максимальное значение параметра зависят от исполнения ViPNet Coordinator HW.

Таблица 1. Значения max-connections для исполнений ViPNet Coordinator HW на аппаратных платформах

Аппаратная платформа	По умолчанию	Максимальное
HW50 N1, N2, N3, N4	150000	150000
HW100 N1, N2, N3, Q1, Q2,	150000	150000
HW1000 Q4, Q5, Q6	800000	1000000
HW1000 Q7	1000000	1500000
HW1000 Q8, Q9	2500000	5000000
HW2000 Q4	2500000	3000000
HW2000 Q5	5500000	10000000
HW5000 Q1	6000000	6500000
HW5000 Q2	5500000	10000000

Таблица 2. Значения max-connections для вариантов исполнения ViPNet Coordinator VA

Вариант исполнения	По умолчанию	Максимальное
ViPNet Coordinator VA100	150000	150000
ViPNet Coordinator VA500	400000	500000
ViPNet Coordinator VA1000	800000	1000000
ViPNet Coordinator VA2000	2500000	3000000
ViPNet Coordinator VA5000	6000000	6500000

Режимы командного интерпретатора

Режим настройки.

Пример использования

Включить антиспуфинг:

```
hostname# firewall settings antispoofing on
```

Задать время жизни соединений по протоколу IP, равным 120 секундам:

```
hostname# firewall settings connection-ttl-ip 120
```

Задать максимальное количество одновременно открытых соединений, равным 7500000:

```
hostname# firewall settings max-connections 7500000
```

firewall settings show

Просмотреть параметры межсетевого экрана ViPNet Coordinator HW.

Синтаксис

```
firewall settings show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются параметры межсетевого экрана (значение времени указывается в секундах):

- `Antispoofing` — статус фильтрации в режиме Strict Reverse Path Forwarding по RFC3704;
- `Block fragmented packets` — статус блокирования входящих фрагментированных пакетов на всех сетевых интерфейсах;
- `Bypass tunnel ips-dpi` — статус обхода обработки туннельного трафика подсистемами DPI и IPS;
- `Connection ttl TCP` — время жизни TCP-соединения;
- `Connection ttl UDP` — время жизни UDP-соединения;
- `Connection ttl IP` — время жизни соединений по протоколам, отличным от TCP, UDP и ICMP;
- `Connection ttl stream UDP` — время жизни потокового UDP-соединения;
- `ICMP timeout` — время жизни ICMP-соединения;

- `Max connections` — максимальное количество одновременных соединений;
- время жизни TCP-соединения до перехода в состояние «установлено»:
  - `TCP SYN RECV timeout` — в режиме ожидания установки соединения;
  - `TCP SYN SENT timeout` — в режиме запроса установки соединения;
- `TCP WAIT timeout` — максимальное время ожидания продолжения TCP-соединения.

Пример использования

```
hostname# firewall settings show
Antispoofing                on
Block fragmented packets    on
Bypass tunnel ips-dpi       on
Connection ttl TCP          3600
Connection ttl UDP          40
Connection ttl IP           300
Connection ttl stream UDP   180
ICMP timeout                10
Max connections             250000
TCP SYN RECV timeout        30
TCP SYN SENT timeout        30
TCP WAIT timeout            30
```

firewall show

Просмотреть конкретные группы объектов, сетевые фильтры заданного типа, а также правила трансляции адресов.

Синтаксис

```
firewall <тип> show [<параметры>]
```

Параметры и ключевые слова

- `<тип>` — тип групп объектов или сетевых фильтров, правила трансляции адресов:
  - `ip-object` — группы IP-адресов;
  - `vpn-object` — группы узлов ViPNet;
  - `interface-object` — группы интерфейсов;
  - `service-object` — группы протоколов;

- `schedule-object` — группы расписаний;
- `local` — локальный фильтр открытой сети;
- `forward` — транзитный фильтр открытой сети;
- `tunnel` — фильтр туннелируемых узлов;
- `vpn` — фильтр защищенной сети;
- `nat` — правило трансляции адресов.

- `<параметр>` — параметры фильтров или правил трансляции, отбираемых для просмотра:
  - `Num` — порядковый номер фильтра или правила трансляции в таблице;
  - `Rule ID-Name` — идентификатор и имя фильтра или правила трансляции;
  - `Act` — действие фильтра или правила трансляции;
  - `Protocol` — протокол, по которому передаются IP-пакеты;
  - `Source` — адрес отправителя IP-пакетов;
  - `Destination` — адрес получателя IP-пакетов;
  - для транзитных фильтров открытой сети и фильтров туннелируемых узлов:
    - `DpiProtocol` — прикладной протокол;
    - `DpiApp` — приложение;
    - `[G]DpiGroup` — группа приложений;
    - `DomainUser` — пользователь Active Directory или Captive Portal.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Указать параметры для групп объектов нельзя.
- Синтаксис адреса отправителя, адреса получателя, протокола, расписания и действия — тот же, что при создании фильтра или правила трансляции с помощью команды firewall add.
- Можно указать несколько параметров.
- При просмотре транзитных фильтров открытой сети возможно использование нескольких значений параметров `<прикладной протокол>`, `<приложение>`, `<группа приложений>` и `<пользователь>`. Значения в списке разделяются запятой; значение, содержащее пробелы, заключается в двойные кавычки.
- Поиск фильтров или правил трансляции осуществляется по строгому совпадению с указанными параметрами.

- В результате выполнения команды отображается таблица, содержащая соответствующие типы групп объектов, сетевых фильтров или правил трансляции адресов.
- Если для фильтра включена регистрация IP-пакетов при его срабатывании, то перед именем фильтра отображается префикс `[LOG]`.

Пример использования

Просмотреть локальные фильтры открытой сети, в которых используется протокол ICMP (показаны настраиваемые фильтры 1, 2 и 3):

```
hostname> firewall local show icmp

 User:

Current Rules Set Id: 184

================================================================================================

Num     UID-Name                                              Option  Schedule

Act     Protocol                    Source                 -> Destination

        DpiProtocol                 [G]DpiGroup, DpiApp       DomainUser

================================================================================================

1       4000056 - ICMP redirect out                           User

drop    icmp: 5                     @local                 -> @any

                                                              @any

        @any                        @any

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

2       4000057 - ICMP redirect in                            User

drop    icmp: 5                     @any                   -> @local

                                                              @any

        @any                        @any

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

3       4000058 - [LOG] Block ICMP                            User

drop    timestamp response          @local                 -> @any

        icmp: 14                                              @any

                                    @any

        @any

------------------------------------------------------------------------------------------------
```

Команды группы inet

Настройка и управление сетевыми интерфейсами, прикладными сервисами, маршрутизацией и мониторингом.

inet bgp

Включить или выключить BGP-маршрутизацию.

Синтаксис

```
inet bgp {on | off}
```

Параметры и ключевые слова

- `on` — включить BGP-маршрутизацию, в том числе при перезагрузке ViPNet Coordinator HW.
- `off` — выключить BGP-маршрутизацию и не включать при перезагрузке ViPNet Coordinator HW.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet bgp on
  Starting BGP... Done
  ```
- ```
  hostname# inet bgp off
  Stopping BGP... Done
  ```

inet bgp as-path-filter add

Создать AS-path-фильтр.

Синтаксис

```
inet bgp as-path-filter add <name>
```

Параметры и ключевые слова

`<name>` — имя AS-path-фильтра.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Требования к имени AS-path-фильтра:
  - длина: 1–64 символов;
  - использование пробелов запрещено;
  - допустимые символы: `A–Z, a–z, 0–9, ` ~ ! @ # $ % ^ & * ( ) - _ = + { } [ ] | \ / : ; " < > , ;`
  - имя должно быть уникальным.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp as-path-filter add Test
AS-path filter Test has been added
```

inet bgp as-path-filter clear seq

Удалить регулярное выражение из AS-path-фильтра.

Синтаксис

```
inet bgp as-path-filter <name> clear seq <num>
```

Параметры и ключевые слова

- `<name>` — имя AS-path-фильтра;
- `seq <num>` — номер регулярного выражения.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp as-path-filter Test clear seq 5

Seq 5 was deleted from AS-path filter Test
```

inet bgp as-path-filter delete

Удалить AS-path-фильтр.

Синтаксис

```
inet bgp as-path-filter delete <name>
```

Параметры и ключевые слова

`<name>` — имя AS-path-фильтра.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp as-path-filter delete Test

AS-path filter Test was deleted
```

inet bgp AS-path-filter seq

Добавить или изменить регулярное выражение в AS-path-фильтре.

Синтаксис

```
inet bgp as-path-filter <name> [seq <num>] {permit | deny}
```

Параметры и ключевые слова

- `<name>` — имя AS-path-фильтра;
- `seq <num>` — номер регулярного выражения;

- `permit` — разрешить встраивание или передачу маршрута при совпадении значения AS-path с регулярным выражением;
- `deny` — запретить встраивание или передачу маршрута при совпадении значения AS-path с регулярным выражением

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Регулярное выражение задается в интерактивном режиме.
- Требования к регулярному выражению:
  - формат POSIX 1003.2;
  - длина: 1–128 символов;
  - разрешено использование пробелов;
  - допустимые символы: `0123456789_^|[, {}() ]$*+.?-\`;

Таблица 3. Значения символов регулярного выражения

Символ	Значение
.	Любой отдельный символ, включая пробел
*	Ноль или более повторений шаблона
+	Один или более повторений шаблона
?	Один или ни одного повторения шаблона
^	Начало строки
$	Конец строки
_	Любой разделитель включая начало строки, конец строки, пробел, табуляцию, запятую); равнозначно (`^|[,{}()]|$`)
\	Удалить следующее специальное значение символа
[]	Сопоставить один символ в диапазоне
|	Логическое ИЛИ

- Номер регулярного выражения: целое число из диапазона 1–4294967295.
- Правила нумерации:
  - Без указания номера регулярное выражение добавляется в конец AS-path-фильтра. Первое регулярное выражение добавляется под номером 5, если не было указано иное. Далее при автонумерации шаг равен 5.

- Если в AS-path-фильтре есть регулярные выражения, при добавлении которых был указан номер, при автонумерации номер последнего регулярного выражения будет увеличен на 5.
- Если значение номера станет больше, чем 4294967291, то добавить регулярное выражение без указания номера будет невозможно.

- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet bgp AS-path-filter Test permit
  Enter regular expression or Ctrl+C to abort: ^$
  Seq 5 permit ^$ was added to AS-path filter Test
  ```
- ```
  hostname# inet bgp AS-path-filter seq 1 Test permit
  Enter regular expression or Ctrl+C to abort: ^$
  Seq 1 permit ^$ was added to AS-path filter Test
  ```

inet bgp clear

Перезапустить BGP-сессии со всеми соседями или с выбранным соседом.

Синтаксис

```
inet bgp clear {all | <IP-address>}
```

Параметры и ключевые слова

- `all` — перезапустить BGP-сессии со всеми соседями;
- `<IP-address>` — IP-адрес соседа, сессия с которым будет перезапущена.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp clear all
BGP sessions were cleared
```

inet bgp community-list add

Создать комьюнити-лист.

Синтаксис

```
inet bgp community-list add <name>
```

Параметры и ключевые слова

`<name>` — имя комьюнити-листа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Требования к имени комьюнити-листа:
  - длина: 1–64 символов;
  - использование пробелов запрещено;
  - допустимые символы: `A–Z`, `a–z`, `0–9`, `` `~!@#$%^&*()-_=+{}[]|\/:;"<>,; ``
  - имя должно быть уникальным.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp community-list add Test
Community list Test has been added
```

inet bgp community-list clear seq

Удалить правило из комьюнити-листа.

Синтаксис

```
inet bgp community-list <name> clear seq <num>
```

Параметры и ключевые слова

- `<name>` — имя комьюнити-листа;
- `seq <num>` — номер правила.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp community-list Test clear seq 5
Seq 5 was deleted
```

inet bgp community-list delete

Удалить комьюнити-лист.

Синтаксис

```
inet bgp community-list delete <name>
```

Параметры и ключевые слова

`<name>` — имя комьюнити-листа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp community-list delete Test
Community list was deleted
```

inet bgp community-list seq

Добавить или изменить правило в комьюнити-листе.

Синтаксис

```
inet community-list <name> [seq <num>] {permit | deny} <community-line>
```

Параметры и ключевые слова

- `<name>` — имя комьюнити-листа;
- `seq <num>` — номер правила;
- `permit` — разрешить комьюнити;
- `deny` — запретить комьюнити;
- `<community-line>` — строка комьюнити.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Номер правила: целое число из диапазона 1–4294967295.
- Правила нумерации:
  - По умолчанию правило добавляется в конец комьюнити-листа. Первое правило добавляется под номером 5, если не было указано иное. Далее при автонумерации шаг равен 5.
  - Если в комьюнити-листе есть правила, при добавлении которых был указан номер, при автонумерации номер последней последовательности будет увеличен на 5.
  - Если значение номера станет больше, чем 4294967291, то добавить правила без указания номера будет невозможно.
- Требования к комьюнити: целое число в формате AA:NN, где AA и NN — целое числа из диапазона 0–65535.
- Требования к строке комьюнити:
  - длина: 3–256 символов;
  - строка не может начинаться с пробела;
  - содержит:
    - одно или более комьюнити, разделенные пробелом;
    - одно или более well-known регистрозависимых комьюнити: internet, no-export, no-advertise, local-AS.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- `hostname# inet bgp community-list Test permit 1000:2000`

```
Sequence 5 was added
```

- `hostname# inet bgp community-list Test seq 1 deny 1000:2020 internet`

  `Sequence 1 was added`

inet bgp neighbor add

Добавить соседа.

Синтаксис

```
inet bgp neighbor add <IP-address> remote-as <as-number> [port <portnumber>]
```

Параметры и ключевые слова

- `<IP-address>` — IP-адрес соседа;
- `<as-number>` — номер автономной системы соседа;
- `<portnumber>` — номер tcp-порта для установления BGP-сессии.

Значения по умолчанию

Без указания параметра `port <portnumber>` используется стандартный порт 179.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor add 192.168.1.1 remote-as 200 port 5284
New neighbor 192.168.1.1:5284 from AS 200 was added
```

inet bgp neighbor delete

Удалить соседа.

Синтаксис

```
inet bgp neighbor <IP-address> delete
```

Параметры и ключевые слова

`<IP-address>` — IP-адрес соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 delete
Neighbor 192.168.1.1 was deleted
```

inet bgp neighbor remove advertise-map

Выключить условное анонсирование для выбранного соседа.

Синтаксис

```
inet bgp neighbor <IP-address> remove advertise-map
```

Параметры и ключевые слова

`<IP-address>` — IP-адрес соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- После запуска команда проверяет настройки условного анонсирования для выбранного соседа и его доступность.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 remove advertise-map
Advertise map was removed
```

inet bgp neighbor remove AS-path-filter

Отключить AS-path-фильтр для соседа.

Синтаксис

```
inet bgp neighbor <IP-адрес> remove AS-path-filter {in | out}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес соседа;
- `in` — отключить для входящих маршрутов;
- `out` — отключить для исходящих маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 remove AS-path-filter out
AS-path filter for neighbor 192.168.1.1 outgoing routes was removed
```

inet bgp neighbor remove password

Выключить аутентификацию соседа и удалить пароль.

Синтаксис

```
inet bgp neighbor <IP-address> remove password
```

Параметры и ключевые слова

`<IP-address>` — IP-адрес соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 remove password
Password was removed and authentication disabled
```

inet bgp neighbor remove prefix-list

Отключить префикс-лист для соседа.

Синтаксис

```
inet bgp neighbor <IP-адрес> remove prefix-list {in | out}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес соседа;
- `in` — отключить для входящих маршрутов;
- `out` — отключить для исходящих маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 remove prefix-list out
Prefix-list for neighbor 192.168.1.1 outgoing routes was removed
```

inet bgp neighbor remove route-map

Отключить карту маршрутов для соседа.

Синтаксис

```
inet bgp neighbor <IP-адрес> remove route-map {in | out}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес соседа;
- `in` — отключить для входящих маршрутов;
- `out` — отключить для исходящих маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 remove route-map out

Route map was removed
```

inet bgp neighbor set advertise-map

Включить условное анонсирование для выбранного соседа.

Синтаксис

```
inet bgp neighbor <ip-address> set advertise-map <ad_name> {exist-map | non-exist-map}
<map_name>
```

Параметры и ключевые слова

- `<IP-address>` — IP-адрес соседа;
- `<ad_name>` — имя существующей карты маршрутов, которая будет применяться при совпадении одного из заданных условий (`exist-map или non-exist-map`);
- `<map_name>` — имя карты маршрутов, по которой проверяется наличие маршрутов в BGP-таблице;
- `exist-map` — проверять наличие маршрута в карте, заданной параметром `<map_name>`;
- `non-exist-map` — проверять отсутствие маршрута в карте, заданной параметром `<map_name>`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 set advertise-map ADV-MAP exist-map MAP123
Advertise-map with exist-map was applied
```

inet bgp neighbor set AS-path-filter

Применить AS-path-фильтр к входящим или исходящим маршрутам, которыми обмениваются маршрутизатор и сосед.

Синтаксис

```
inet bgp neighbor <IP-адрес> set AS-path-filter <name> {in | out}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес соседа;
- `<name>` — имя AS-path-фильтра;
- `in` — применить к входящим маршрутам;
- `out` — применить к исходящим маршрутам.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Для фильтрации по каждому направлению используется последний примененный AS-path-фильтр.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 set AS-path-filter Test in
AS-path filter Test applied for neighbor 192.168.1.1 incoming routes
```

inet bgp neighbor set default-originate

Включить или выключить анонсирование маршрута по умолчанию для соседа.

Синтаксис

```
inet bgp neighbor <IP-address> set default-originate {on | off}
```

Параметры и ключевые слова

- `<IP-address>` — IP-адрес соседа;
- `on` — включить анонсирование маршрута по умолчанию;
- `off` — выключить анонсирование маршрута по умолчанию.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 set default-originate on
Originating default network 0.0.0.0/0 was enabled
```

inet bgp neighbor set ebgp-multihop

Настроить eBGP-multihop для соседа.

Синтаксис

```
inet bgp neighbor <IP-address> set ebgp-multihop {<ttl> | off}
```

Параметры и ключевые слова

- `<IP-address>` — IP-адрес соседа.
- `<ttl>` — TTL для исходящих пакетов BGP-сессии, целое число из диапазона 2–255.
- `off` — выключить eBGP-multihop для соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Выполнение команды невозможно, если для соседа уже настроен TTL Security.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- `hostname# inet bgp neighbor 192.168.1.1 set ebgp-multihop 2`
  `eBGP-multihop was enabled. TTL = 2`
- `hostname# inet bgp neighbor 192.168.1.1 set ebgp-multihop off`
  `eBGP-multihop was disabled.`

inet bgp neighbor set next-hop-self

Включить или выключить замену next-hop для соседа на собственный адрес.

Синтаксис

```
inet bgp neighbor <IP-address> set next-hop-self {on | off}
```

Параметры и ключевые слова

- `<IP-address>` — IP-адрес соседа;
- `on` — включить замену next-hop;
- `off` — выключить замену next-hop.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 set next-hop-self on
Next-hop change for neighbor 192.168.1.1 was enabled
```

inet bgp neighbor set password

Включить аутентификацию с соседом и задать пароль.

Синтаксис

```
inet bgp neighbor <IP-address> set password
```

Параметры и ключевые слова

`<IP-address>` — IP-адрес соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Требования к паролю:
  - длина: 1–80 символов;
  - использование пробелов запрещено;
  - допустимые символы: `A–Z`, `a–z`, `0–9`, `` `~!@#$%^&*()-_=+{}[]|\/:;"'<>,. ``
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 set password
Set password:
Confirm password:
Password was set and authentication enabled
```

inet bgp neighbor set port

Задать номера TCP-порта соседа.

Синтаксис

```
inet bgp neighbor <IP-address> set port <portnumber>
```

Параметры и ключевые слова

- `<IP-address>` — IP-адрес соседа.

- `<portnumber>` — номер tcp-порта для установления BGP-сессии.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 port 5252

New TCP port was set
```

inet bgp neighbor set prefix-list

Назначить префикс-лист для фильтрации входящих или исходящих маршрутов, которыми обмениваются маршрутизатор и сосед.

Синтаксис

```
inet bgp neighbor <IP-адрес> set prefix-list <name> {in | out}
```

Параметры и ключевые слова

- `<name>` — имя префикс-листа;
- `<IP-адрес>` — IP-адрес соседа;
- `in` — назначить для входящих маршрутов;
- `out` — назначить для исходящих маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Для фильтрации по каждому направлению используется последний назначенный префикс-лист.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 set prefix-list Test out
```

```
Prefix-list Test applied for neighbor 192.168.1.1 outgoing routes
```

inet bgp neighbor set remote-as

Изменить номер автономной системы соседа.

Синтаксис

```
inet bgp neighbor <IP-address> set remote-as <as-number>
```

Параметры и ключевые слова

- <IP-address> — IP-адрес соседа.
- <as-number> — новый номер автономной системы соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 set remote-as 200
ASN for Neighbor 192.168.1.1 was changed
```

inet bgp neighbor set route-map

Применить карту маршрутов к входящим или исходящим маршрутам, которыми обмениваются маршрутизатор и сосед.

Синтаксис

```
inet bgp neighbor <ip-address> set route-map <name> {in|out}
```

Параметры и ключевые слова

- `<IP-address>` — IP-адрес соседа;
- `<name>` — имя карты маршрутов;
- `in` — применить к входящим маршрутам;
- `out` — применить к исходящим маршрутам.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Для фильтрации по каждому направлению используется последняя примененная карта маршрутов.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp neighbor 192.168.1.1 set route-map Test in

Route map was applied
```

inet bgp neighbor set ttl-security

Настроить TTL Security для соседа.

Синтаксис

```
inet bgp neighbor <IP-address> set ttl-security {<hops> | off}
```

Параметры и ключевые слова

- `<IP-address>` — IP-адрес соседа.
- `<hops>` — максимальное число переходов до соседа, целое число из диапазона 1–254.
- `off` — выключить TTL Security для соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Выполнение команды невозможно, если для соседа уже настроен eBGP-multihop.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet bgp neighbor 192.168.1.1 set ttl-secuirty 2

  TTL Security was enabled. Maximum hops = 2
  ```
- ```
  hostname# inet bgp neighbor 192.168.1.1 set ttl-secuirty off

  TTL Security was disabled
  ```

inet bgp network add

Добавить анонсируемую подсеть.

Синтаксис

```
inet bgp network add <subnet> netmask <netmask>
```

Параметры и ключевые слова

- `<subnet>` — IP-адрес подсети.
- `<netmask>` — маска подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- IP-адреса подсети автоматически корректируется в соответствии с маской.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet bgp network add 192.168.1.0 netmask 255.255.255.0
  Network 192.168.1.0 with netmask 255.255.255.0 has been added
  ```
- ```
  hostname# inet bgp network add 192.168.1.1 netmask 255.255.255.0
  Subnet has been automatically adjusted according to netmask
  Network 192.168.1.0 with netmask 255.255.255.0 has been added
  ```

inet bgp network delete

Удалить анонсируемую посеть.

Синтаксис

```
inet bgp network delete <subnet> netmask <netmask>
```

Параметры и ключевые слова

- `<subnet>` — IP-адрес подсети.
- `<netmask>` — маска подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp network delete 192.168.1.0 netmask 255.255.255.0
Network 192.168.1.0 with netmask 255.255.255.0 has been deleted
```

inet bgp network redistribute

Включить или выключить перераспределение маршрутов.

Синтаксис

```
inet bgp network redistribute {connected | static} {on | off}
```

Параметры и ключевые слова

- `connected` — подключенные маршруты;
- `static` — статические маршруты;
- `on` — включить перераспределение маршрутов;
- `off` — выключить перераспределение маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp network redistribute connected on
Connected routes redistribution was enabled
```

inet bgp network redistribute route-map

Назначить или удалить карту маршрутов, применяемую к распространяемым маршрутам.

Синтаксис

```
inet bgp network redistribute {connected | static} route-map {name <name> | clear}
```

Параметры и ключевые слова

- `<name>` — имя назначаемой карты маршрутов;
- `clear` — удалить назначенную карту маршрутов;
- `connected` — назначить или удалить карту маршрутов для подключенных маршрутов;
- `static` — назначить или удалить карту маршрутов для статических маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet bgp network redistribute connected route-map name Test
  Route Map Test was applied to connected routes
  ```
- ```
  hostname# inet bgp network redistribute connected route-map clear
  Route Map for connected routes was cleared
  ```

inet bgp router as

Задать или изменить номер автономной системы маршрутизатора.

Синтаксис

```
inet bgp router as <as-number>
```

Параметры и ключевые слова

`<as-number>` — номер автономной системы маршрутизатора, целое число из диапазона 1–4294967295.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp router as 100
AS Number for BGP router was set
```

inet bgp router bestpath AS-path-relax

Включить или выключить проверку AS-path при встраивании эквивалентных маршрутов (AS-path relax).

Синтаксис

```
inet bgp router bestpath AS-path-relax {on | off}
```

Параметры и ключевые слова

- `on` — игнорировать содержимое AS-path.
- `off` — не игнорировать содержимое AS-path.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp router bestpath AS-path-relax {on|off}
AS-path relax mode was turned on
```

inet bgp router bestpath bandwith

Задать режим обработки эквивалентных (multipath) маршрутов с расширенным комьюнити `Link bandwidth`.

Синтаксис

```
inet bgp router bestpath bandwith {ignore | skip | min | default}
```

Параметры и ключевые слова

- `ignore` — значение `Link bandwidth` будет проигнорировано, все эквивалентные маршруты будут встроены с весом 1;
- `skip` — маршруты из набора эквивалентных маршрутов без `Link bandwidth` будут проигнорированы и не будут встроены в таблицу маршрутизации;
- `min` — маршруты из набора эквивалентных маршрутов без `Link bandwidth` будут встроены в таблицу маршрутизации с весом 1;
- `default` — возвращает поведение по умолчанию: если хотя бы один маршрут из набора эквивалентных маршрутов будет без `Link bandwidth`, маршруты будут встроены в таблицу маршрутизации с весом 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp router bestpath bandwidth ignore
Link bandwidth mode was switched
```

inet bgp router conditional-advertisement-timer

Задать период опроса BGP-таблицы для условного анонсирования.

Синтаксис

```
inet bgp router conditional-advertisement-timer <период>
```

Параметры и ключевые слова

- `<период>` — период опроса в секундах. Допустимое значение — от 5 до 240 секунд.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp router conditional-advertisement-timer 5
Timer was set
```

inet bgp router id

Задать идентификатор маршрутизатора (router id) вручную или назначить его автоматически.

Синтаксис

```
inet bgp router id {<a.b.c.d> | auto}
```

Параметры и ключевые слова

- `<a.b.c.d>` — router id, может принимать значение от 0.0.0.1 до 255.255.255.255.
- `auto` — назначить router id автоматически как наибольший IP-адрес среди адресов интерфейсов ViPNet Coordinator HW.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию router id назначается автоматически.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet bgp router id 1.1.1.1
  New Router ID for BGP router was set
  ```
- ```
  hostname# inet bgp router id auto
  ```

```
Router ID for BGP router will be set automatically
```

inet bgp router reset

Сбросить настройки маршрутизатора, в том числе номер автономной системы, соседей и анонсированные подсети.

Синтаксис

```
inet bgp router reset
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Для подтверждения сброса настроек введите `Yes`.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp router reset
All BGP router settings will be deleted. Continue? [Yes/No]: Yes
BGP router was reseted
```

inet bgp route-reflector client add

Добавить iBGP-соседа в список RR-клиентов.

Синтаксис

```
inet bgp route-reflector client add <IP-address>
```

Параметры и ключевые слова

`<IP-address>` — IP-адрес iBGP-соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp route-reflector client add 1.1.1.1
New route-reflector client 1.1.1.1 was added
```

inet bgp route-reflector client delete

Удалить iBGP-соседа из списка RR-клиентов.

Синтаксис

```
inet bgp route-reflector client delete <IP-адрес>
```

Параметры и ключевые слова

`<IP-адрес>` — IP-адрес iBGP-соседа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp route-reflector client delete 1.1.1.1
Route-reflector client 1.1.1.1 was deleted
```

inet bgp route-reflector cluster-id

Задать идентификатор RR-кластера вручную или назначить его автоматически.

Синтаксис

```
inet bgp route-reflector cluster-id {<a.b.c.d> | auto}
```

Параметры и ключевые слова

- `<a.b.c.d>` — идентификатор RR-кластера, может принимать значение от 0.0.0.1 до 255.255.255.255.
- `auto` — назначить идентификатор RR-кластера автоматически.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию идентификатор RR-кластера (cluster-id) равен идентификатору маршрутизатора (router-id).
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp route-reflector cluster-id 1.1.1.1
New Cluster ID for BGP route-reflector was setinet bgp router id 1.1.1.1
```

inet bgp route-reflector outbound-policy

Разрешить или запретить применение исходящих карт маршрутов к отраженным маршрутам.

Синтаксис

```
inet bgp route-reflector outbound-policy {on | off}
```

Параметры и ключевые слова

- `on` — разрешить применение исходящих карт маршрутов к отраженным маршрутам;
- `off` — запретить применение исходящих карт маршрутов к отраженным маршрутам.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp route-reflector outbound-policy off
```

```
Outbound policy for BGP route-reflector was disabled. Outgoing Route-Maps now will not
affect reflected routes.
```

inet bgp show

Просмотреть всю BGP-таблицу или маршруты, через которые доступна выбранная подсеть.

Синтаксис

```
inet bgp show [<подсеть>]
```

Параметры и ключевые слова

`<подсеть>` — IP-адрес подсети в формате CIDR.

Значения по умолчанию

Без указания подсети отображается вся BGP-таблица.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде без указания подсети отображаются список маршрутов и их параметры:
  - значение next-hop;
  - значение атрибута MED (при наличии);
  - значение атрибута Local Preference (при наличии);
  - вес маршрута;
  - значение атрибута AS-path;
  - значение атрибута Origin;
  - статус валидности маршрута;
  - статус выбора маршрута в качестве лучшего;
  - статус получения от iBGP-соседа.
- По команде с указанием подсети отображаются:
  - список маршрутов, через которые подсеть доступна, и их параметры:
    - значение атрибута Origin;
    - значение next-hop;

        - значение атрибута MED (при наличии);
        - значение атрибута Local Preference (при наличии);
        - значение атрибута AS-path;
        - статус валидности маршрута;
        - статус выбора маршрута в качестве лучшего;
        - значение атрибута комьюнити (при наличии);
        - время последнего обновления маршрута;
    - признак, по которому маршрут был выбран в качестве лучшего;
    - список соседей, которым был передан маршрут.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Просмотреть BGP-таблицу:

```
hostname# inet bgp show
BGP table version is 15, local router ID is 255.255.255.255, vrf id 0
Default local pref 100, local AS 1
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.10.1.0/24     0.0.0.0                  0         32768 ?
*>                  0.0.0.0                  0         32768 i
*> 10.10.2.0/24     192.168.1.2              0             0 2 i
*> 10.10.200.0/24   192.168.1.2                            0 2 2 2 3 4 5 6 2 i
```

Просмотреть маршруты BGP-таблицы для подсети 10.10.1.0/24:

```
hostname# inet bgp show 10.10.1.0/24
BGP routing table entry for 10.10.1.0/24
Paths: (2 available, best #2, table default)
  Advertised to non peer-group peers:
  192.168.1.2
  Local
```

```
    0.0.0.0 from 0.0.0.0 (255.255.255.255)
      Origin incomplete, metric 0, weight 32768, valid, sourced
      Last update: Mon Oct 17 11:45:04 2022
  Local
    0.0.0.0 from 0.0.0.0 (255.255.255.255)
      Origin IGP, metric 0, weight 32768, valid, sourced, local, best (Local Route)
      Last update: Mon Oct 17 11:44:59 2022
```

inet bgp show AS-path-filter

Просмотреть список AS-path-фильтров или состав выбранного AS-path-фильтра.

Синтаксис

```
inet bgp show AS-path-filter [<name>]
```

Параметры и ключевые слова

`<name>` — имя AS-path-фильтра.

Значения по умолчанию

Отображается список AS-path-фильтров.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet bgp show AS-path-filter
  AS-path filters:
  Test
  Test2
  User
  ```
- ```
  hostname# inet bgp show AS-path-filter Test
  AS-path filter Test:
  ```

```
seq 5 deny _21_
seq 10 permit .*
```

inet bgp show bestpath

Просмотреть настройки выбора лучшего маршрута.

Синтаксис

```
inet bgp show bestpath
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде отображаются:
  - статус игнорирования AS-path (multipath-relax);
  - настройка обработки комьюнити `Link Bandwidth`.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet show bgp bestpath
AS-path relax: on
Link Bandwidth: default
```

inet bgp show community-list

Просмотреть список комьюнити-листов или состав выбранного комьюнити-листа.

Синтаксис

```
inet bgp show community-list [<name>]
```

Параметры и ключевые слова

`<name>` — имя комьюнити-листа.

Значения по умолчанию

Отображается список комьюнити-листов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet prefix-list show
  Community-lists:
  Test
  Test2
  User
  ```
- ```
  hostname# inet bgp show community-list Test
  Community-list Test:
  seq 5 permit 1000:2000 local-AS
  seq 10 deny internet
  ```

inet bgp show neighbors

Просмотреть сведения о всех соседях или выбранном соседе.

Синтаксис

```
inet bgp show neighbors [<IP-адрес> [{advertised | learned}]]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес соседа;
- `advertised` — показывать маршруты, анонсированные соседу, после фильтрации;
- `learned` — показывать маршруты из BGP-таблицы, полученные от соседа, после фильтрации.

Значения по умолчанию

Без указания параметров отображаются подробные сведения о всех соседях.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде без указания параметров отображаются сведения обо всех соседях:
  - IP-адрес соседа;
  - номер AS соседа;
  - Router-ID соседа;
  - текущее состояние сессии;
  - статистика отправки и получения сообщений;
  - входящий IP-адрес и TCP-порт сессии;
  - исходящий IP-адрес и TCP-порт сессии;
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Просмотреть сведения обо всех соседях:

```
hostname# inet bgp show neighbors

BGP neighbor is 172.16.1.2, remote AS 2, local AS 2, internal link

Hostname: FRR2-1

  BGP version 4, remote router ID 172.16.1.2, local router ID 192.168.1.2

  BGP state = Established, up for 05:25:55

  Last read 00:00:54, Last write 00:00:09

  Hold time is 180, keepalive interval is 60 seconds

  Neighbor capabilities:

    4 Byte AS: advertised and received

    AddPath:

      IPv4 Unicast: RX advertised IPv4 Unicast and received

    Route refresh: advertised and received(old & new)

    Address Family IPv4 Unicast: advertised and received

    Hostname Capability: advertised (name: FRR2,domain name: n/a) received (name:
FRR2-1,domain name: n/a)

    Graceful Restart Capability: advertised and received

      Remote Restart timer is 120 seconds
```

```
    Address families by peer:
      none
 Graceful restart information:
   End-of-RIB send: IPv4 Unicast
   End-of-RIB received: IPv4 Unicast
   Local GR Mode: Helper*
   Remote GR Mode: Helper
   R bit: True
   Timers:
     Configured Restart Time(sec): 120
     Received Restart Time(sec): 120
   IPv4 Unicast:
     F bit: False
     End-of-RIB sent: Yes
     End-of-RIB sent after update: No
     End-of-RIB received: Yes
     Timers:
       Configured Stale Path Time(sec): 360
 Message statistics:
   Inq depth is 0
   Outq depth is 0
                        Sent       Rcvd
   Opens:                 1          1
   Notifications:         0          0
   Updates:              12          2
   Keepalives:          326        326
   Route Refresh:         0          0
   Capability:            0          0
   Total:               339        329
 Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
 Update group 4, subgroup 2
 Packet Queue length 0
```

```
  NEXT_HOP is always this router
  Community attribute sent to this neighbor(all)
  1 accepted prefixes


  Connections established 1; dropped 0
  Last reset 05:26:08,  No AFI/SAFI activated for peer
Local host: 172.16.1.1, Local port: 179
Foreign host: 172.16.1.2, Foreign port: 48356
Nexthop: 172.16.1.1
Nexthop global: fe80::a00:27ff:fe31:fbce
Nexthop local: fe80::a00:27ff:fe31:fbce
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Read thread: on  Write thread: on  FD used: 24


BGP neighbor is 192.168.1.1, remote AS 1, local AS 2, external link
Hostname: FRR1
  BGP version 4, remote router ID 0.0.0.0, local router ID 192.168.1.2
  BGP state = Active
  Last read 00:00:24, Last write 00:00:07
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 120
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                 16          5
    Notifications:          2          8
```

```
    Updates:                16          16
    Keepalives:            309         309
    Route Refresh:           0           0
    Capability:              0           0
    Total:                 343         338
  Minimum time between advertisement runs is 0 seconds


 For address family: IPv4 Unicast
  Not part of any update group
  Community attribute sent to this neighbor(all)
  Outbound path policy configured
  Route map for outgoing advertisements is *COM2
  0 accepted prefixes


  Connections established 4; dropped 4
  Last reset 00:00:09,  Peer closed the session
  Message received that caused BGP to send a NOTIFICATION:
    FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
    004D0104 000100B4 FFFFFFFF 30020601
    04000100 01020280 00020202 00020641
    04000000 01020645 04000101 01020849
    06044652 52310002 04400200 78
Local host: 192.168.1.2, Local port: 51118
Foreign host: 192.168.1.1, Foreign port: 179
Nexthop: 192.168.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Next connect timer due in 112 seconds
Read thread: off  Write thread: off  FD used: -1
```

Просмотреть маршруты, анонсируемые соседу 172.16.1.2:

```
hostname# inet bgp show neighbors 172.16.1.2 advertised
```

```
BGP table version is 11, local router ID is 192.168.1.2, vrf id 0
Default local pref 100, local AS 2
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.1.0/24     0.0.0.0                  0    100      0 1 i
*> 10.10.2.0/24     0.0.0.0                  0    100  32768 i
```

Просмотреть маршруты, полученные от соседа 172.16.1.2:

```
hostname# inet bgp show neighbors 172.16.1.2 learned
BGP table version is 11, local router ID is 192.168.1.2, vrf id 0
Default local pref 100, local AS 2
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i10.10.200.0/24   172.16.1.2               0    100      0 i
```

inet bgp show neighbors filters

Просмотреть список AS-Path-фильтров, префикс-листов и карт маршрутов всех соседей или только выбранного соседа.

Синтаксис

```
inet bgp show neighbors filters [<ip-адрес>]
```

Параметры и ключевые слова

`<ip-адрес>` — имя IP-адреса соседа.

Значения по умолчанию

Без указания IP-адреса соседа отображается список AS-Path-фильтров, префикс-листов и карт маршрутов всех соседей.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде отображаются сведения о соседях (всех или выбранном):
  - IP-соседа;
  - `AS-path filter`, `Prefix-list` и `Route-map`, применяемые к `Incoming` (входящим) и `Outgoing` (исходящим) маршрутам;
  - если настроено условное анонсирование маршрутов:
    - карта маршрутов условного анонсирования `Advertise map`;
    - карта `Exist-map` или `Non-exist-map`;
    - при просмотре всех соседей — значение таймера условного анонсирования.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet bgp show neighbors filters 1.1.1.1
  Neighbor 1.1.1.1
      Incoming
          AS-path filter: Not set
          Prefix-list: 404
          Route-map: Hello
      Outgoing
          AS-path filter: Test
          Prefix-list: 503
          Route-map: Goodbye
  ```
- ```
  hostname# inet bgp show neighbors filters 1.1.1.1
  Neighbor 1.1.1.1
      Incoming
          AS-path filter: Not set
          Prefix-list: 404
          Route-map: Hello
      Outgoing
  ```

```
        AS-path filter: Test
        Prefix-list: 503
        Route-map: Goodbye
    Advertise map: ADV-MAP
        Exist-map: EXIST-MAP
```

inet bgp show neighbors list

Просмотреть список соседей и атрибутов доступа к ним.

Синтаксис

```
inet bgp show neighbors list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Атрибуты соседа:
  - `Neighbor` — IP-адрес соседа;
  - `ASN` — номер автономной системы;
  - `Port` — tcp-порт доступа;
  - `TTL Secuirty` — включен или выключен, количество переходов;
  - `eBgp-multihop` — включен или выключен, значение TTL;
  - `Authentication` — аутентификации: включена или выключена;
  - `Next-hop-self` — включен или выключен.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp show neighbors list
Neighbor   ASN   Port   TTL Security   eBGP-multihop   Authentication   Next-hop-self
--------   ---   ----   ------------   -------------   --------------   -------------
1.1.1.1    100   179    Off            Off             On                 On
2.2.2.2    200   179    Off            2               Off                Off
3.3.3.3    200   5252    1             Off             Off                Off
```

inet bgp show network

Просмотреть настройки анонсирования подсетей и перераспределения маршрутов.

Синтаксис

```
inet bgp show network
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде отображаются:
  - настройки перераспределения подключенных маршрутов, наличии или отсутствии назначенной карты маршрутов для них;
  - настройки перераспределения статических маршрутов, наличии или отсутствии назначенной карты маршрутов для них;
  - список соседей, для которых включено анонсирование маршрута по умолчанию;
  - список анонсированных подсетей.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp show network

Routes          Redistribution      Route Map

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

Connected       ON                  Test

Static          ON                  Not set


Originating default network for neighbors:

1.1.1.1

2.2.2.2


Announced networks:

Destination     Netmask

-----------     -------
```

```
172.20.20.0     255.255.255.0
10.10.0.0       255.255.0.0
```

inet bgp show route-reflector

Просмотреть настройки отражения маршрутов (Route Reflector).

Синтаксис

```
inet bgp show route-reflector
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде отображаются:
  - `Cluster-ID` — идентификатор RR-кластера;
  - `Outbound-policy` — политика применения исходящих карт маршрутов к отраженным маршрутам;
  - список RR-клиентов.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet bgp show route-reflecor
Cluster-ID: auto
Outbound-policy: on
Route-reflector clients are:
1.1.1.1
2.2.2.2
3.3.3.3
```

inet bgp show summary

Просмотреть список сессий и состояние каждой из них.

Синтаксис

```
inet bgp show summary
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде отображаются список сессий и состояние каждой из них:
  - IP-адрес соседа;
  - номер AS соседа;
  - время нахождения сессии в текущем состоянии;
  - если сессия активна — выводится количество полученных префиксов;
  - количестве отправленных префиксов.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname#inet bgp show summary

IPv4 Unicast Summary:

BGP router identifier 192.168.1.2, local AS number 2 vrf-id 0

BGP table version 12

RIB entries 3, using 576 bytes of memory

Peers 2, using 43 KiB of memory


Neighbor    V  AS  MsgRcvd  MsgSent  TblVer  InQ OutQ  Up/Down State/PfxRcd  PfxSnt

172.16.1.2  4   2      344      356       0    0    0 05:40:58            1       1

192.168.1.1 4   1      358      363       0    0    0 00:00:06       Active       0
```

inet bonding add mode slaves

Создать агрегированный интерфейс.

Синтаксис

```
inet bonding add <номер> mode <режим> slaves <интерфейс 1> [<интерфейс 2>] ... [<интерфейс N>]
```

Параметры и ключевые слова

- `<номер>` — номер создаваемого агрегированного интерфейса. Возможные значения: 0, 1, 2, 3, 4, 5, 6, 7.
- `<режим>` — режим работы агрегированного интерфейса:
  - `balance-rr` — режим, при котором исходящие пакеты, попадающие на агрегированный интерфейс, отправляются через подчиненные физические интерфейсы поочередно: первый пакет отправляется через один подчиненный интерфейс, второй пакет — через следующий подчиненный интерфейс и так далее.
  - `balance-xor` — режим, при котором подчиненный физический интерфейс, через который отправляется тот или иной пакет, выбирается на основе значения хэш-функции, вычисляемой по алгоритму, задаваемому с помощью команды inet ifconfig bonding xmit-hash-policy. В результате пакеты от одного и того же отправителя к одному и тому же получателю всегда будут отправляться через один и тот же подчиненный интерфейс.
  - `balance-tlb` — режим, при котором ведется подсчет размера исходящих пакетов, переданных через каждый из подчиненных физических интерфейсов, и на основе этого выполняется балансировка исходящего трафика между подчиненными интерфейсами.
  - `802.3ad` — режим динамического агрегирования с использованием протокола LACP, в котором:
    - среди подчиненных физических интерфейсов формируются группы — «агрегаторы», скорость передачи данных на интерфейсах которых одинакова;
    - один из агрегаторов выбирается активным в соответствии с алгоритмом, задаваемым с помощью команды inet ifconfig bonding ad-select;
    - внутри агрегатора подчиненный физический интерфейс, через который отправляются исходящие пакеты, выбирается аналогично режиму `balance-xor`;
    - в случае сбоя на физическом интерфейсе, входящем в агрегатор, или при добавлении нового подчиненного физического интерфейса в качестве активного выбирается другой агрегатор (также в соответствии с алгоритмом, задаваемым с помощью команды inet ifconfig bonding ad-select);
    - с другим сетевым оборудованием происходит обмен пакетами LACP с периодичностью, задаваемой с помощью команды inet ifconfig bonding lacp-rate, что позволяет определить сбой подчиненного интерфейса даже в том случае, если этот интерфейс подключен к другому сетевому узлу не напрямую (например, через медиаконвертер).
  - `active-backup` — режим, в котором один из подчиненных физических интерфейсов назначается основным (автоматически или явно с помощью команды inet ifconfig bonding primary) и все исходящие пакеты отправляются через него. В случае сбоя на основном подчиненном интерфейсе пакеты будут отправляться через другие подчиненные интерфейсы.
  - `broadcast` — режим, при котором пакеты, попадающие на агрегированный интерфейс, отправляются через все подчиненные физические интерфейсы одновременно.

- `<интерфейс 1>`, `<интерфейс 2>`, `<интерфейс N>` — физические интерфейсы, подчиненные создаваемому агрегированному интерфейсу. Ограничений на количество физических интерфейсов в агрегированном нет.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Можно создать до восьми агрегированных интерфейсов с именами `bond<номер>`.
- Подчиненные физические интерфейсы должны относиться к классу `slave` (см. inet ifconfig class).
- При создании агрегированного интерфейса задайте хотя бы один подчиненный ему физический интерфейс. Затем вы можете добавить подчиненные физические интерфейсы с помощью команды inet ifconfig bonding add.
- Режим `broadcast` требует специальной настройки сетевого оборудования, предотвращающей дальнейшую передачу по сети нескольких копий пакетов данных.
- Если агрегированный канал работает в режиме `broadcast`, его нельзя использовать для объединения сегментов сети по L2OverIP.
- Для работы агрегированного интерфейса в режиме `balance-tlb` подключите все подчиненные физические интерфейсы к сети через коммутатор.
- Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.
- Механизм MC-LAG (MLAG) в режиме 802.3ad не поддерживается. Поэтому физические порты разных ViPNet Coordinator HW нельзя использовать в одном агрегированном интерфейсе.

Пример использования

Чтобы добавить агрегированный интерфейс `bond1`, работающий в режиме `balance-rr`, с подчиненными физическими интерфейсами `eth0` и `eth1`:

```
hostname# inet ifconfig eth0 class slave

Attention: Upon changing the network interface settings, make similar changes to the
services that use this interface

and then restart them.

eth0 set to slave class.

hostname# inet ifconfig eth1 class slave

Attention: Upon changing the network interface settings, make similar changes to the
services that use this interface

and then restart them.

eth1 set to slave class.
```

```
hostname# inet bonding add 1 mode balance-rr slaves eth0 eth1
New bond interface bond1 was created
```

inet bonding delete

Удалить агрегированный интерфейс.

Синтаксис

```
inet bonding delete <номер>
```

Параметры и ключевые слова

`<номер>` — номер удаляемого агрегированного интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Имена агрегированных интерфейсов имеют вид `bond<номер>`.
- Если вы хотите удалить агрегированный интерфейс класса `trunk` (см. inet ifconfig class), предварительно удалите все соответствующие ему виртуальные интерфейсы с помощью команды inet ifconfig vlan delete.

Пример использования

```
hostname# inet bonding delete 1
```

inet clear mac-address-table

Очистить ARP-таблицу (таблицу преобразования IP-адресов в MAC-адреса).

Синтаксис

```
inet clear mac-address-table
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet clear mac-address-table
This command clears the MAC addresses table.
Are you sure you want to execute this command? [Yes/No]: Yes
```

inet dgd configuration default

Сбросить параметры службы DGD на значения по умолчанию:

- interval-time — частота проверки состояния шлюза;
- response-time — время ожидания ответа от тестового IP-адреса шлюза;
- retries-count — число неудачных проверок шлюза, после которого шлюз считается нерабочим;
- syslog-level — максимальный уровень событий DGD, записываемых в системный журнал.

Синтаксис

```
inet dgd configuration default
```

Значения по умолчанию

После выполнения команды параметры службы DGD сбрасываются на следующие значения по умолчанию:

- interval-time — 3 секунды;
- response-time — 3 секунды;
- retries-count — 3 проверки;
- syslog-level — 3-й уровень событий.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба DGD должна быть запущена (см. inet dgd mode).

Пример использования

Чтобы сбросить параметры службы DGD на значения по умолчанию:

```
hostname# inet dgd configuration default
Are you sure to reset DGD settings to default values? [Yes/No]: y
```

inet dgd configuration interval-time

Задать частоту проверки соединения с тестовым IP-адресом шлюза (см. inet dgd next-hop add).

Синтаксис

```
inet dgd configuration interval-time <интервал>
```

Параметры и ключевые слова

`<интервал>` — время в секундах, через которое производится проверка соединения с тестовым IP-адресом шлюза. Возможные значения от 1 до 120 секунд.

Значения по умолчанию

По умолчанию соединение проверяется каждые 3 секунды.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Служба DGD должна быть запущена (см. inet dgd mode).
- Значение, заданное командой, действует для всех шлюзов, добавленных с помощью команды inet dgd next-hop add.
- При нестабильном соединении (например, при использовании сети 3G или Wi-Fi) рекомендуется увеличить интервал проверки соединения со шлюзом.

Пример использования

Чтобы проверять соединение с тестовым IP-адресом шлюза каждые 10 секунд:

```
hostname# inet dgd configuration interval-time 10
```

inet dgd configuration response-time

Задать время ожидания ответа от тестового IP-адреса шлюза (см. inet dgd next-hop add).

Синтаксис

```
inet dgd configuration response-time <время>
```

Параметры и ключевые слова

`<время>` — время в секундах, в течение которого ожидается ответ от тестового IP-адреса шлюза. Возможные значения от 1 до 120 секунд.

Значения по умолчанию

По умолчанию время ожидания ответа составляет 3 секунды.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Служба DGD должна быть запущена (см. inet dgd mode).
- Значение, заданное командой, действует для всех шлюзов, добавленных с помощью команды inet dgd next-hop add.
- При нестабильном соединении (например, при использовании сети 3G или Wi-Fi) рекомендуется увеличить время ожидания ответа от шлюза.

Пример использования

Чтобы задать время ожидания ответа от тестового IP-адреса шлюза 10 секунд:

```
hostname# inet dgd configuration response-time 10
```

inet dgd configuration retries-count

Задать число проверок IP-адреса шлюза, при достижении которого шлюз считается нерабочим.

Синтаксис

```
inet dgd configuration retries-count <число проверок>
```

Параметры и ключевые слова

`<число проверок>` — число проверок IP-адреса шлюза, при достижении которого шлюз считается нерабочим. Возможные значения от 1 до 10.

Значения по умолчанию

По умолчанию проверка работоспособности шлюза выполняется 3 раза.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Служба DGD должна быть запущена (см. inet dgd mode).
- Значение, заданное командой, действует для всех шлюзов, добавленных с помощью команды inet dgd next-hop add.
- При нестабильном соединении (например, при использовании сети 3G или Wi-Fi) рекомендуется увеличить число проверок IP-адреса шлюза.

Пример использования

Чтобы считать шлюз нерабочим после 5 проверок:

```
hostname# inet dgd configuration retries-count 5
```

inet dgd configuration syslog-level

Изменить уровень важности событий службы DGD, записываемых в системный журнал.

Синтаксис

```
inet dgd configuration syslog-level <уровень важности>
```

Параметры и ключевые слова

`<уровень важности>` — уровень важности событий, записываемых в системный журнал. Возможные значения:

- `0` — критические события (critical);
- `1` — ошибки (error);
- `2` — извещения (notice);
- `3` — информационные сообщения (info);
- `4` — отладочные события (debug);

Каждый последующий уровень включает в себя предыдущие.

Значение `-1` отключает регистрацию событий службы DGD.

Значения по умолчанию

В системный журнал записываются события не выше 3-го уровня (`3`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба DGD должна быть запущена (см. inet dgd mode).

Пример использования

Чтобы записывать в системный журнал события службы DGD не выше 1-го уровня:

```
hostname# inet dgd configuration syslog-level 1
```

inet dgd next-hop add

Добавить проверку состояния шлюза с помощью отправки запросов на тестовый IP-адрес или IP-адрес шлюза (если тестовый IP-адрес не задан).

Синтаксис

```
inet dgd next-hop add <имя шлюза> {address <адрес шлюза> | interface <интерфейс>}
[test-address <тестовый адрес>] {check | no-check} {icmp | tcp80 | tcp443}
```

Параметры и ключевые слова

- `<имя шлюза>` — уникальное имя удалённого шлюза. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `<адрес шлюза>` — IP-адрес удалённого шлюза.
- `<интерфейс>` — имя сетевого интерфейса ViPNet Coordinator HW. Данный параметр доступен только для сетевых интерфейсов, получающих IP-адрес по протоколу DHCP.
- `<тестовый адрес>` — тестовый IP-адрес шлюза. Несколько шлюзов могут иметь один и тот же тестовый IP-адрес. Он может совпадать с IP-адресом самого шлюза. Если значение параметра не задано, то в качестве тестового IP-адреса используется IP-адрес шлюза.

  Не используйте одинаковые IP-адреса для проверки шлюзов DGD и для параметров `testip` при работе в кластере — это может привести к циклической перезагрузке его узлов.
- `check` — включить проверку состояния шлюза.
- `no-check` — отключить проверку состояния шлюза.
- `icmp` — использовать широковещательный запрос ICMP для проверки состояния шлюза.
- `tcp80` — использовать TCP-соединение по порту 80 для проверки состояния шлюза.
- `tcp443` — использовать TCP-соединение по порту 443 для проверки состояния шлюза.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Служба DGD должна быть запущена (см. inet dgd mode).
- Если вы задали проверку шлюза с использованием TCP-соединения, создайте разрешающий сетевой фильтр:

  ```
  hostname# firewall local add src @local dst <тестовый адрес> tcp dport 80 tcp dport 443 pass
  ```

Пример использования

- Чтобы добавить проверку по протоколу ICMP состояния шлюза с именем `gateway1`, IP-адресом 192.168.23.56 и тестовым IP-адресом 192.168.23.1:

  ```
  hostname# inet dgd next-hop add gateway1 address 192.168.23.56 test-address 192.168.23.1 check icmp
  ```

- Чтобы отключить проверку по протоколу TCP (порт 443) состояния шлюза с именем `gateway2` по интерфейсу `eth1`:

  ```
  hostname# inet dgd next-hop add gateway2 interface eth1 no-check tcp443
  ```

inet dgd next-hop delete

Удалить ранее заданную проверку состояния шлюза (см. inet dgd next-hop add).

Синтаксис

```
inet dgd next-hop delete <имя шлюза>
```

Параметры и ключевые слова

`<имя шлюза>` — уникальное текстовое имя шлюза. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба DGD должна быть запущена (см. inet dgd mode).

Пример использования

Чтобы удалить проверку состояния шлюза с именем `gateway1`:

```
hostname# inet dgd next-hop delete gateway1
```

inet dgd mode

Включить или выключить автоматический запуск службы DGD при загрузке ViPNet Coordinator HW.

Синтаксис

```
inet dgd mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения по умолчанию

Автоматический запуск службы DGD выключен (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Выполнение команды также запускает (`on`) или останавливает (`off`) работу службы DGD.

Пример использования

Чтобы включить автоматический запуск службы DGD при загрузке ViPNet Coordinator HW (и немедленно запустить службу DGD):

```
hostname# inet dgd mode on
Starting dgd ...
```

inet dgd rule add action-priority

Задать действие, которое будет выполнено при совпадении всех состояний шлюзов, заданных командой inet dgd rule add match-next-hop.

Синтаксис

```
inet dgd rule add <имя правила> action-priority <приоритет> service {log command <текст сообщения> | route command policy active {<имя политики> | default}}
```

Параметры и ключевые слова

- `<имя правила>` — уникальное текстовое имя правила, ранее созданного командой inet dgd rule add match-next-hop. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `<приоритет>` — приоритет правила в списке, возможные значения от 1 до 255. Чем меньше значение, тем выше приоритет правила.
- `log command` — записать событие (совпадение всех состояний шлюзов) в системный журнал.
- `<текст сообщения>` — текст сообщения, который будет записан в системный журнал при наступлении события (совпадение всех состояний шлюзов). Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `route command` — при совпадении всех состояний шлюзов выполнить команду inet policy active, активирующую заданную политику маршрутизации.
- `<имя политики>` — уникальное текстовое имя ранее созданной политики маршрутизации (см. inet policy rule add match). Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `default` — сбросить настройки политик маршрутизации. Активируется политика маршрутизации по умолчанию.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба DGD должна быть запущена (см. inet dgd mode).

Пример использования

Чтобы в правило `rule1` добавить действие 1-го приоритета, при котором в случае совпадения всех состояний шлюзов будет включаться активная политика `policy1`:

```
hostname# inet dgd rule add rule1 action-priority 1 service route command policy active policy1
```

inet dgd rule add match-next-hop

Добавить правило проверки состояния шлюзов, заданных командой inet dgd next-hop add.

Синтаксис

```
inet dgd rule add <имя правила> match-next-hop <имя шлюза> {up | down}
```

Параметры и ключевые слова

- `<имя правила>` — уникальное текстовое имя правила. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `<имя шлюза>` — уникальное текстовое имя ранее заданного шлюза (см. inet dgd next-hop add). Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `up` — шлюз проверяется на доступность.
- `down` — шлюз проверяется на недоступность.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба DGD должна быть запущена (см. inet dgd mode).

Пример использования

Чтобы добавить правило проверки доступности ранее заданного шлюза `gateway1`:

```
hostname# inet dgd rule add gateway1-up match-next-hop gateway1 up
```

inet dgd rule clear

Удалить все проверки и действия из ранее заданных правил шлюзов.

Синтаксис

```
inet dgd rule clear <имя правила>
```

Параметры и ключевые слова

`<имя правила>` — уникальное текстовое имя правила. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Служба DGD должна быть запущена (см. inet dgd mode).
- При выполнении команды запрашивается подтверждение удаления всех проверок и действий из ранее заданного правила.

Пример использования

Чтобы удалить все проверки и действия из правила с именем `rule1`:

```
hostname# inet dgd rule clear rule1
Do you want to clear this rule? [Yes/No]: y
```

inet dgd rule delete action-priority

Удалить действие, ранее заданное командой inet dgd rule add action-priority.

Синтаксис

```
inet dgd rule delete <имя правила> action-priority <приоритет>
```

Параметры и ключевые слова

- `<имя правила>` — уникальное текстовое имя правила. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `<приоритет>` — приоритет правила в списке, возможные значения от 1 до 255. Чем меньше значение, тем выше приоритет правила.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба DGD должна быть запущена (см. inet dgd mode).

Пример использования

Чтобы из правила `rule1` удалить действие 2-го приоритета:

```
hostname# inet dgd rule delete rule1 action-priority 2
```

inet dgd rule delete match-next-hop

Удалить шлюз из правила проверки состояния шлюзов, заданного командой inet dgd next-hop add.

Синтаксис

```
inet dgd rule delete <имя правила> match-next-hop <имя шлюза> {up | down}
```

Параметры и ключевые слова

- `<имя правила>` — уникальное текстовое имя правила. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `<имя шлюза>` — уникальное текстовое имя ранее заданного шлюза. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `up` — если шлюз проверяется на доступность.
- `down` — если шлюз проверяется на недоступность.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба DGD должна быть запущена (см. inet dgd mode).

Пример использования

Чтобы удалить шлюз `gateway1` из правила `rule1`:

```
hostname# inet dgd rule delete rule1 match-next-hop gateway1 up
```

inet dhcp client route-default-metric

Изменить значение метрики по умолчанию для маршрутов, поступающих от DHCP-сервера. Эта метрика будет присваиваться маршрутам DHCP-сервера, если для сетевого интерфейса, на который они поступили, не задана специфичная метрика.

Синтаксис

```
inet dhcp client route-default-metric <1-255>
```

Параметры и ключевые слова

`<1–255>` — новое значение метрики по умолчанию.

Значения по умолчанию

```
70
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet dhcp client route-default-metric 60
```

inet dhcp client route-distance

Задать административную дистанцию маршрутам, поступающим от DHCP-сервера (с использованием DHCP-протокола).

Синтаксис

```
inet dhcp client route-distance <административная дистанция> [default-route
<административная дистанция>]
```

Параметры и ключевые слова

- `route-distance <административная дистанция>` — общая административная дистанция для всех маршрутов DHCP-сервера. Возможные значения: 1–255.
- `default-route <административная дистанция>` — административная дистанция для маршрутов по умолчанию. Возможные значения: 1–255.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Значение административной дистанции для маршрутов по умолчанию можно задать только вместе с административной дистанцией для всего протокола DHCP.

Пример использования

```
hostname# inet dhcp client route-distance 80 default-route 60

Set distance to 80, default distance to 60
```

inet dhcp relay add backup-interface

Добавить сетевой интерфейс, через который служба DHCP-relay будет связываться с запасным DHCP-сервером.

Синтаксис

```
inet dhcp relay [<номер копии>] add backup-interface <интерфейс> server <адрес>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой задается интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса, со стороны которого находится запасной DHCP-сервер.
- `<адрес>` — IP-адрес запасного DHCP-сервера.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из списка интерфейсов, которые имеются в системе, но отсутствуют в списке принимающих DHCP-запросы.
- Указанный в команде интерфейс должен иметь статический адрес.

Пример использования

Чтобы для копии 2 службы DHCP-relay использовать интерфейс `eth1` для связи с запасным DHCP-сервером, имеющим IP-адрес 172.16.1.1:

```
hostname# inet dhcp relay 2 add backup-interface eth1 server 172.16.1.1
```

inet dhcp relay add external-interface

Добавить сетевой интерфейс, через который служба DHCP-relay будет связываться с внешним DHCP-сервером.

Синтаксис

```
inet dhcp relay [<номер копии>] add external-interface <интерфейс> server <адрес>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой задается интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса, со стороны которого находится внешний DHCP-сервер.
- `<адрес>` — IP-адрес внешнего DHCP-сервера.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из списка интерфейсов, которые имеются в системе, но отсутствуют в списке принимающих DHCP-запросы.
- Указанный в команде интерфейс должен иметь статический адрес.
- В качестве сетевого интерфейса нельзя задать:
  - интерфейс модема (ppp0) — нет в исполнении ViPNet Coordinator VA;
  - интерфейс «внутренней петли» (loopback, localhost);
  - виртуальные интерфейсы, созданные после назначения дополнительных IP-адресов физическим интерфейсам (алиасы).

Пример использования

Чтобы для копии 2 службы DHCP-relay использовать интерфейс `eth1` для связи с внешним DHCP-сервером, имеющим адрес 172.16.1.1:

```
hostname# inet dhcp relay 2 add external-interface eth1 server 172.16.1.1
```

inet dhcp relay add listen-interface

Добавить сетевой интерфейс в список интерфейсов, принимающих запросы от DHCP-клиентов для их последующей ретрансляции на внешний DHCP-сервер.

Синтаксис

```
inet dhcp relay [<номер копии>] add listen-interface <интерфейс>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой задается интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя сетевого интерфейса.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из списка интерфейсов, которые имеются в системе, но отсутствуют в списке принимающих DHCP-запросы.
- Добавляемый интерфейс должен иметь статический адрес.
- Добавляемый интерфейс не должен использоваться в других копиях DHCP-relay.
- В качестве сетевого интерфейса нельзя задать:
  - интерфейс модема (ppp0) — нет в исполнении ViPNet Coordinator VA;
  - интерфейс «внутренней петли» (loopback, localhost);
  - виртуальные интерфейсы, созданные после назначения дополнительных IP-адресов физическим интерфейсам (алиасы).

Пример использования

Чтобы для копии DHCP-relay 2 добавить интерфейс `eth0` в список интерфейсов, принимающих запросы от DHCP-клиентов:

```
hostname# inet dhcp relay 2 add listen-interface eth0
```

inet dhcp relay delete backup-interface

Удалить сетевой интерфейс, через который служба DHCP-relay связывается с запасным DHCP-сервером.

Синтаксис

```
inet dhcp relay [<номер копии>] delete backup-interface <интерфейс> server <адрес>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой удаляется интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса, со стороны которого находится запасной DHCP-сервер.
- `<адрес>` — IP-адрес запасного DHCP-сервера.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка.

Пример использования

Чтобы для копии 2 службы DHCP-relay удалить интерфейс `eth1`, имеющий связь с запасным DHCP-сервером с IP-адресом 172.16.1.1:

```
hostname# inet dhcp relay 2 delete backup-interface eth1 server 172.16.1.1
```

inet dhcp relay delete external-interface

Удалить сетевой интерфейс, через который служба DHCP-relay связывается с внешним DHCP-сервером.

Синтаксис

```
inet dhcp relay [<номер копии>] delete external-interface <интерфейс> server <адрес>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой удаляется интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса, со стороны которого находится внешний DHCP-сервер.

- `<адрес>` — IP-адрес внешнего DHCP-сервера.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка.

Пример использования

Чтобы для копии 2 службы DHCP-relay удалить интерфейс `eth1` для связи с внешним DHCP-сервером, имеющим адрес 172.16.1.1:

```
hostname# inet dhcp relay 2 delete external-interface eth1 server 172.16.1.1
```

inet dhcp relay delete listen-interface

Удалить сетевой интерфейс из списка интерфейсов, принимающих запросы от DHCP-клиентов для их последующей ретрансляции на внешний DHCP-сервер.

Синтаксис

```
inet dhcp relay [<номер копии>] delete listen-interface <интерфейс>
```

Параметры и ключевые слова

- `<номер копии>` — копия процесса DHCP-relay, для которой задан интерфейс. Возможные значения от 1 до 32.
- `<интерфейс>` — имя интерфейса.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу службы DHCP-relay.
- При вводе интерфейса работают автозаполнение и подсказка.

Пример использования

Чтобы для копии DHCP-relay 2 удалить интерфейс `eth0` из списка интерфейсов, принимающих запросы от DHCP-клиентов:

```
hostname# inet dhcp relay 2 delete listen-interface eth0
```

inet dhcp relay mode

Включить или выключить автоматический запуск службы DHCP-relay при загрузке ViPNet Coordinator HW.

Синтаксис

```
inet dhcp relay mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения по умолчанию

Автоматический запуск службы DHCP-relay выключен (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По команде изменяется только настройка автоматического запуска службы DHCP-relay, ее текущее состояние не изменяется.
- Невозможно включить автоматический запуск в следующих случаях:
  - Включен автоматический запуск DHCP-сервера.
  - Не заданы какие-либо настройки службы DHCP-relay.

Пример использования

Чтобы включить автоматический запуск службы DHCP-relay:

```
hostname# inet dhcp relay mode on
```

inet dhcp relay reset

Сбросить настройки службы DHCP-relay, включая настройки автоматического запуска при загрузке ViPNet Coordinator HW, и завершить её работу.

Синтаксис

```
inet dhcp relay [<номер копии>] reset
```

Параметры и ключевые слова

`<номер копии>` — копия процесса DHCP-relay. Возможные значения от 1 до 32.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то настройки сбрасываются для всех копий.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда используется в случае, если требуется сбросить настройки службы DHCP-relay для последующего задания новых параметров.

Пример использования

```
hostname# inet dhcp relay reset
Are you sure to reset DHCP relay settings? [Yes/No]: Yes
```

inet dhcp relay start

Запустить службу DHCP-relay.

Синтаксис

```
inet dhcp relay [<номер копии>] start
```

Параметры и ключевые слова

`<номер копии>` — копия процесса DHCP-relay. Возможные значения от 1 до 32.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Невозможно запустить службу DHCP-relay в следующих случаях:

- Запущен DHCP-сервер.
- Не заданы какие-либо настройки службы DHCP-relay.
- Указан несуществующий номер копии процесса DHCP-relay.

Пример использования

Чтобы запустить копию 2 процесса DHCP-relay:

```
hostname# inet dhcp relay 2 start
```

inet dhcp relay stop

Завершить работу службы DHCP-relay.

Синтаксис

```
inet dhcp relay [<номер копии>] stop
```

Параметры и ключевые слова

`<номер копии>` — копия процесса DHCP-relay. Возможные значения от 1 до 32.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы завершить работу копии 2 процесса DHCP-relay:

```
hostname# inet dhcp relay 2 stop
```

inet dhcp server add default-lease-time

Задать значение по умолчанию времени аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay). Это значение используется клиентами DHCP-сервера, которые не запрашивают определенное время аренды IP-адресов.

Синтаксис

```
inet dhcp server add default-lease-time <время> [interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>]
```

Параметры и ключевые слова

- `<время>` — время аренды в секундах (от 1 до 4294967294).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается время аренды (лизинга) IP-адресов по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться время аренды IP-адресов по умолчанию. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается время аренды IP-адресов по умолчанию (в параметрах секции `[id]` указанного узла файла `iplir.conf`). Для узла должен быть предварительно зарезервирован IP-адрес с помощью команды inet dhcp server add host.

Значения по умолчанию

По умолчанию время аренды составляет 864000 секунд.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы установить время аренды по умолчанию 5 дней для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server add default-lease-time 432000 remote subnet 192.168.1.0 mask 255.255.255.0
```

inet dhcp server add dns

Задать IP-адрес DNS-сервера для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add dns <IP-адрес> [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес DNS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается IP-адрес DNS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться IP-адрес DNS-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается IP-адрес DNS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- С помощью последовательного выполнения команд можно добавить до 10 IP-адресов DNS-серверов.

Пример использования

- Чтобы добавить IP-адрес DNS-сервера 192.168.15.41 для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server add dns 192.168.15.41 interface eth1
  ```

- Чтобы задать IP-адрес DNS-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server add dns 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы задать IP-адрес DNS-сервера 192.168.15.41 для узла сети ViPNet с именем host123:

  ```
  hostname# inet dhcp server add dns 192.168.15.41 host host123
  ```

inet dhcp server add domain

Задать имя домена для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add domain <имя домена> [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<имя домена>` — имя домена, соответствующее формату FQDN.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается имя домена.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться имя домена. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается имя домена (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При добавлении более одного имени домена выдается сообщение, что предыдущее значение будет перезаписано.

Пример использования

- Чтобы добавить доменное имя dc.corp для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server add domain dc.corp interface eth1
  ```

- Чтобы задать доменное имя dc.corp для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server add domain dc.corp remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы задать доменное имя dc.corp для узла сети ViPNet с именем host123:

  ```
  hostname# inet dhcp server add domain dc.corp host host123
  ```

inet dhcp server add host

Зарезервировать в DHCP-сервере IP-адрес сетевого узла с заданными доменным именем и MAC-адресом. Информацию об этом DHCP-сервер передает своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add host <имя узла> hardware <MAC-адрес> address <IP-адрес> {interface <интерфейс> | remote subnet <подсеть> mask <маска>}
```

Параметры и ключевые слова

- `<имя узла>` — доменное имя сетевого узла, для которого резервируется IP-адрес. Может содержать символы латинского алфавита, цифры и знак дефиса («-»). Максимальная длина 32 символа.
- `<MAC-адрес>` — MAC-адрес сетевого узла, для которого резервируется IP-адрес.
- `<IP-адрес>` — IP-адрес, который резервируется DHCP-сервером для данного узла.
- `<интерфейс>` — название сетевого интерфейса в системе, на котором резервируется IP-адрес узла.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться информация о резервировании IP-адреса. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы зарезервировать IP-адрес 192.168.15.41 для узла с именем `host123` и MAC-адресом 00:50:56:C0:00:08 на сетевом интерфейсе `eth1`:

  ```
  hostname# inet dhcp server add host host123 hardware 00:50:56:C0:00:08 address 192.168.15.41 interface eth1
  ```

- Чтобы зарезервировать IP-адрес 192.168.15.41 для узла с именем `host123` и MAC-адресом 00:50:56:C0:00:08 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server add host host123 hardware 00:50:56:C0:00:08 address 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

inet dhcp server add interface

Задать рабочий интерфейс DHCP-сервера.

Синтаксис

```
inet dhcp server add interface <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- В качестве интерфейса можно указать Ethernet-, Wi-Fi-, VLAN- или агрегированный интерфейс (Wi-Fi- и агрегированного интерфейса нет в исполнении ViPNet Coordinator VA).
- Рабочий интерфейс DHCP-сервера должен иметь статический IP-адрес.
- IP-адрес рабочего интерфейса DHCP-сервера не должен принадлежать диапазону выделяемых IP-адресов, заданному командой inet dhcp server add range.

Пример использования

Чтобы задать интерфейс `eth1` в качестве рабочего для DHCP-сервера:

```
hostname# inet dhcp server add interface eth1
```

inet dhcp server add max-lease-time

Задать время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add max-lease-time <время> [{interface <интерфейс> | remote subnet
<подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<время>` — время аренды в секундах (от 1 до 4294967294).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться время аренды IP-адресов. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается время аренды IP-адресов (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Значения по умолчанию

Время аренды составляет 864000 секунд.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы установить время аренды 5 дней для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server add max-lease-time 432000 remote subnet 192.168.1.0 mask
255.255.255.0
```

inet dhcp server add ntp

Задать IP-адрес NTP-сервера для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add ntp <IP-адрес> [{interface <интерфейс> | remote subnet <подсеть> mask
<маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес NTP-сервера.

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается IP-адрес NTP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться IP-адрес NTP-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается IP-адрес NTP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- С помощью последовательного выполнения команд можно добавить до 10 IP-адресов NTP-серверов.

Пример использования

- Чтобы добавить IP-адрес NTP-сервера 192.168.15.41 для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server add ntp 192.168.15.41 interface eth1
  ```

- Чтобы задать IP-адрес NTP-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server add ntp 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы задать IP-адрес NTP-сервера 192.168.15.41 для узла сети ViPNet с именем `host123`:

  ```
  hostname# inet dhcp server add ntp 192.168.15.41 host host123
  ```

inet dhcp server add option

Добавить опцию DHCP-сервера в соответствии с RFC 2132.

Синтаксис

```
inet dhcp server add option <номер> {ip | ascii | hex} <значение> [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<номер>` — номер опции DHCP-сервера (от 1 до 254).
- `ip` — опция содержит IP-адрес.

- `ascii` — опция содержит текст в кодировке ASCII.
- `hex` — опция содержит разрядное шестнадцатеричное число (с точками разрядов, без учета регистра).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается опция DHCP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться опция DHCP-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается опция DHCP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При выполнении команды выдается предупреждение, что значения опций не проверяются на соответствие RFC 2132.

Пример использования

Чтобы добавить опцию DHCP-сервера 69 (сервер SMTP по умолчанию) со значением 10.0.0.25 для сетевого интерфейса `eth1`:

```
hostname# inet dhcp server add option 69 ip 10.0.0.25 interface eth1
```

inet dhcp server add range

Задать диапазон IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add range <начало диапазона> <конец диапазона> {interface <интерфейс> |
remote subnet <подсеть> mask <маска>}
```

Параметры и ключевые слова

- `<начало диапазона>` — начальный IP-адрес диапазона.
- `<конец диапазона>` — конечный IP-адрес диапазона.

- `<интерфейс>` — название сетевого интерфейса в системе, на котором задается диапазон IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться информация о диапазоне IP-адресов. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- Конечный адрес диапазона должен быть не меньше начального.
- В локальной сети, маршрутизируемой в интернет, рекомендуется, чтобы диапазон выделяемых адресов был из числа допустимых для частных сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

Пример использования

Чтобы DHCP-сервер выделял клиентам сети 192.168.10.0/24 адреса из диапазона 192.168.10.2–192.168.10.254:

```
hostname# inet dhcp server add range 192.168.10.2 192.168.10.254 remote subnet 192.168.10.0
mask 255.255.255.0
```

inet dhcp server add relay-interface

Задать сетевой интерфейс DHCP-сервера, на котором он будет обрабатывать запросы от агента DHCP-relay, работающего в удаленной подсети.

Синтаксис

```
inet dhcp server add relay-interface <интерфейс> remote subnet <подсеть> mask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса. Сетевой интерфейс должен быть предварительно задан в качестве рабочего интерфейса DHCP-сервера (см. inet dhcp server add interface).
- `<подсеть>` — IP-адрес удаленной подсети, в которой работает агент DHCP-relay.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- Максимально возможное количество удаленных подсетей —128.
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов, заданных командой inet dhcp server add interface.
- В качестве интерфейса можно указать Ethernet-, Wi-Fi-, VLAN- или агрегированный интерфейс (Wi-Fi- и агрегированного интерфейса нет в исполнении ViPNet Coordinator VA).
- Задаваемый интерфейс DHCP-сервера должен иметь статический IP-адрес.
- IP-адрес задаваемого интерфейса DHCP-сервера не должен принадлежать диапазону выделяемых IP-адресов, заданному командой inet dhcp server add range.

Пример использования

Чтобы задать интерфейс `eth1` в качестве сетевого интерфейса DHCP-сервера, на котором он будет обрабатывать запросы от агента DHCP-relay, работающего в удаленной подсети с адресом 192.168.10.0/24:

```
hostname# inet dhcp server add relay-interface eth1 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add router

Задать IP-адрес шлюза по умолчанию для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add router <IP-адрес> {interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес шлюза по умолчанию.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается IP-адрес шлюза по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться IP-адрес шлюза по умолчанию. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.

- `<имя узла>` — имя узла сети ViPNet, для которого задается IP-адрес шлюза по умолчанию (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- IP-адрес шлюза должен принадлежать сети интерфейса и не должен входить в диапазон IP-адресов, выделяемых клиентам.
- С помощью последовательного выполнения команд можно добавить до 10 IP-адресов шлюзов по умолчанию.

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 адрес шлюза по умолчанию 192.168.10.1:

```
hostname# inet dhcp server add router 192.168.10.1 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add subnet-mask

Задать маску подсети для передачи DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add subnet-mask <маска подсети> {interface <интерфейс> | remote subnet
<подсеть> mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<маска подсети>` — маска подсети, передаваемая DHCP-сервером.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается маска подсети.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться маска подсети. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается маска подсети (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При добавлении более одной маски подсети выдается сообщение, что предыдущее значение будет перезаписано.
- На основе указанной маски подсети будет автоматически задан широковещательный IP-адрес, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP-relay).

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 маску подсети 255.255.255.0:

```
hostname# inet dhcp server add subnet-mask 255.255.255.0 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add tftp

Задать IP-адрес или имя TFTP-сервера, а также имя передаваемого файла. Данная информация передается DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add tftp {<имя сервера> | <адрес сервера>} [file <путь к файлу>] [{interface
<интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<имя сервера>` — доменное имя TFTP-сервера, соответствующее формату FQDN.
- `<адрес сервера>` — IP-адрес TFTP-сервера.
- `<путь к файлу>` — путь к файлу, загружаемому по протоколу TFTP.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задаются параметры TFTP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будут передаваться параметры TFTP-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задаются параметры TFTP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При добавлении более одного адреса TFTP-сервера выдается сообщение, что предыдущее значение будет перезаписано.

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 IP-адрес TFTP-сервера 192.168.10.65:

```
hostname# inet dhcp server add tftp 192.168.10.65 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add voip

Задать IP-адрес TFTP-сервера Cisco VoIP. Данная информация передается DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add voip <адрес сервера> [{interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес TFTP-сервера Cisco VoIP.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задаются параметры TFTP-сервера Cisco VoIP.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будут передаваться параметры TFTP-сервера Cisco VoIP. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задаются параметры TFTP-сервера Cisco VoIP (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- С помощью последовательного выполнения команд можно добавить до 2 IP-адресов TFTP-сервера Cisco VoIP.

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 IP-адрес TFTP-сервера Cisco VoIP 192.168.10.65:

```
hostname# inet dhcp server add voip 192.168.10.65 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server add wins

Добавить адрес WINS-сервера в список адресов, передаваемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server add wins <адрес сервера> [interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес WINS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается IP-адрес WINS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться IP-адрес WINS-сервера. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается IP-адрес WINS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- С помощью последовательного выполнения команд можно добавить до 2 IP-адресов WINS-сервера.

Пример использования

Чтобы DHCP-сервер передавал клиентам сети 192.168.10.0/24 IP-адрес WINS-сервера 192.168.10.65:

```
hostname# inet dhcp server add wins 192.168.10.65 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server delete default-lease-time

Удалить значение по умолчанию времени аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete default-lease-time {interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого удаляется время аренды (лизинга) IP-адресов по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается время аренды IP-адресов по умолчанию.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задано время аренды IP-адресов по умолчанию (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить заданное время аренды по умолчанию для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server delete default-lease-time remote subnet 192.168.1.0 mask
255.255.255.0
```

inet dhcp server delete dns

Удалить IP-адрес DNS-сервера, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete dns <IP-адрес> [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес DNS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес DNS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес DNS-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес DNS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы удалить IP-адрес DNS-сервера 192.168.15.41 для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server delete dns 192.168.15.41 interface eth1
  ```

- Чтобы удалить IP-адрес DNS-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server delete dns 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы удалить IP-адрес DNS-сервера 192.168.15.41 для узла сети ViPNet с именем `host123`:

  ```
  hostname# inet dhcp server delete dns 192.168.15.41 host host123
  ```

inet dhcp server delete domain

Удалить доменное имя, передаваемое DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete domain [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задано имя домена.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается имя домена.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задано имя домена (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы удалить доменное имя для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server delete domain interface eth1
  ```

- Чтобы удалить доменное имя для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server delete domain remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы удалить доменное имя для узла сети ViPNet с именем `host123`:

  ```
  hostname# inet dhcp server delete domain host host123
  ```

inet dhcp server delete host

Удалить зарезервированный DHCP-сервером IP-адрес сетевого узла с заданными доменным именем и MAC-адресом.

Синтаксис

```
inet dhcp server delete host <имя узла> hardware <MAC-адрес> address <IP-адрес> {interface
<интерфейс> | remote subnet <подсеть> mask <маска>}
```

Параметры и ключевые слова

- `<имя узла>` — доменное имя сетевого узла, для которого зарезервирован IP-адрес. Может содержать символы латинского алфавита, цифры и знак дефиса («-»). Максимальная длина 32 символа.
- `<MAC-адрес>` — MAC-адрес сетевого узла, для которого зарезервирован IP-адрес.
- `<IP-адрес>` — IP-адрес, который зарезервирован DHCP-сервером для данного узла.
- `<интерфейс>` — название сетевого интерфейса в системе, на котором зарезервирован IP-адрес узла.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается информация о резервировании IP-адреса.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы удалить резервирование IP-адреса 192.168.15.41 для узла с именем `host123` и MAC-адресом 00:50:56:C0:00:08 на сетевом интерфейсе `eth1`:

  ```
  hostname# inet dhcp server delete host host123 hardware 00:50:56:C0:00:08 address
  192.168.15.41 interface eth1
  ```

- Чтобы удалить резервирование IP-адреса 192.168.15.41 для узла с именем `host123` и MAC-адресом 00:50:56:C0:00:08 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server delete host host123 hardware 00:50:56:C0:00:08 address
  192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

inet dhcp server delete interface

Удалить рабочий интерфейс DHCP-сервера.

Синтаксис

```
inet dhcp server delete interface <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- В качестве интерфейса можно указать Ethernet-, Wi-Fi-, VLAN- или агрегированный интерфейс (Wi-Fi- и агрегированного интерфейса нет в исполнении ViPNet Coordinator VA).

Пример использования

Чтобы удалить интерфейс `eth1` как рабочий интерфейс DHCP-сервера:

```
hostname# inet dhcp server delete interface eth1
```

inet dhcp server delete max-lease-time

Удалить ранее заданное время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete max-lease-time [{interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задано время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задано время аренды (лизинга) IP-адресов, выделяемых DHCP-сервером (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Значения по умолчанию

После выполнения команды время аренды сбрасывается на значение по умолчанию (864000 секунд).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить заданное время аренды для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server delete max-lease-time remote subnet 192.168.1.0 mask
255.255.255.0
```

inet dhcp server delete ntp

Удалить IP-адрес NTP-сервера, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete ntp <IP-адрес> [{interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес NTP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес NTP-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес NTP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

- Чтобы удалить IP-адрес NTP-сервера 192.168.15.41 для сетевого интерфейса `eth1`:

  ```
  hostname# inet dhcp server delete ntp 192.168.15.41 interface eth1
  ```

- Чтобы удалить IP-адрес NTP-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

  ```
  hostname# inet dhcp server delete ntp 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
  ```

- Чтобы удалить IP-адрес NTP-сервера 192.168.15.41 для узла сети ViPNet с именем `host123`:

  ```
  hostname# inet dhcp server delete ntp 192.168.15.41 host host123
  ```

inet dhcp server delete option

Удалить опцию DHCP-сервера в соответствии с RFC 2132.

Синтаксис

```
inet dhcp server delete option <номер> [{interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<номер>` — номер опции DHCP-сервера (от 1 до 254).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого удаляется опция DHCP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается опция DHCP-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задана опция DHCP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить опцию DHCP-сервера 69 (сервер SMTP по умолчанию) для сетевого интерфейса `eth1`:

```
hostname# inet dhcp server delete option 69 interface eth1
```

inet dhcp server delete range

Удалить диапазон IP-адресов, выделяемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete range <начало диапазона> <конец диапазона> {interface <интерфейс>
| remote subnet <подсеть> mask <маска>}
```

Параметры и ключевые слова

- `<начало диапазона>` — начальный IP-адрес диапазона.
- `<конец диапазона>` — конечный IP-адрес диапазона.
- `<интерфейс>` — название сетевого интерфейса в системе, на котором задан диапазон IP-адресов, выделяемых DHCP-сервером.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается информация о диапазоне IP-адресов.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить выделяемый DHCP-сервером клиентам сети 192.168.10.0/24 диапазон 192.168.10.2–192.168.10.254:

```
hostname# inet dhcp server delete range 192.168.10.2 192.168.10.254 remote subnet
192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete relay-interface

Удалить сетевой интерфейс DHCP-сервера, на котором обрабатываются запросы от агента DHCP-relay, работающего в удаленной подсети.

Синтаксис

```
inet dhcp server delete relay-interface <интерфейс> remote subnet <подсеть> mask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса. Сетевой интерфейс должен быть предварительно задан в качестве рабочего интерфейса DHCP-сервера (см. inet dhcp server add interface).
- `<подсеть>` — IP-адрес удаленной подсети, в которой работает агент DHCP-relay. Удаленная подсеть должна быть предварительно задана командой inet dhcp server add relay-interface.
- `<маска>` — маска удаленной подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов, заданных командой inet dhcp server add interface.

Пример использования

Чтобы удалить интерфейс `eth1`, на котором DHCP-сервер обрабатывает запросы от агента DHCP-relay, работающего в удаленной подсети с адресом 192.168.10.0/24:

```
hostname# inet dhcp server delete relay-interface eth1 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server delete router

Удалить IP-адрес шлюза по умолчанию, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete router <адрес> {interface <интерфейс> | remote subnet <подсеть>
mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес шлюза по умолчанию.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес шлюза по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес шлюза по умолчанию.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес шлюза по умолчанию.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить адрес шлюза по умолчанию 192.168.10.1, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

```
hostname# inet dhcp server delete router 192.168.10.1 remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete subnet-mask

Удалить маску подсети, передаваемую DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete subnet-mask {interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>}
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого задана маска подсети.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается маска подсети.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задана маска подсети (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).
- По команде будет автоматически удален широковещательный IP-адрес, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP-relay).

Пример использования

Чтобы удалить маску подсети, передаваемую DHCP-сервером клиентам сети 192.168.10.0/24:

```
hostname# inet dhcp server delete subnet-mask remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete tftp

Удалить настройки TFTP-сервера, передаваемые DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete tftp [{interface <интерфейс> | remote subnet <подсеть> mask <маска>
| host <имя узла>}]
```

Параметры и ключевые слова

- `<интерфейс>` — название сетевого интерфейса в системе, для которого заданы параметры TFTP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передаются параметры TFTP-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого заданы параметры TFTP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить IP-адрес TFTP-сервера 192.168.10.65, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

```
hostname# inet dhcp server delete tftp remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server delete voip

Удалить IP-адрес TFTP-сервера Cisco VoIP. Данная информация передается DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete voip <адрес сервера> [{interface <интерфейс> | remote subnet
<подсеть> mask <маска> | host <имя узла>}]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес TFTP-сервера Cisco VoIP.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого заданы параметры TFTP-сервера Cisco VoIP.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передаются параметры TFTP-сервера Cisco VoIP.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого заданы параметры TFTP-сервера Cisco VoIP (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Чтобы удалить IP-адрес TFTP-сервера Cisco VoIP 192.168.10.65, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

```
hostname# inet dhcp server delete voip 192.168.10.65 remote subnet 192.168.10.0 mask
255.255.255.0
```

inet dhcp server delete wins

Удалить адрес WINS-сервера из списка адресов, передаваемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

```
inet dhcp server delete wins <адрес сервера> [interface <интерфейс> | remote subnet <подсеть> mask <маска> | host <имя узла>]
```

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес WINS-сервера.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес WINS-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес WINS-сервера.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес WINS-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу DHCP-сервера (см. inet dhcp server stop).

Пример использования

Удалить IP-адрес WINS-сервера 192.168.10.65, передаваемый DHCP-сервером клиентам удаленной подсети 192.168.10.0/24:

```
hostname# inet dhcp server delete wins 192.168.10.65 remote subnet 192.168.10.0 mask 255.255.255.0
```

inet dhcp server mode

Включить или выключить автоматический запуск DHCP-сервера при загрузке ViPNet Coordinator HW.

Синтаксис

```
inet dhcp server mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения по умолчанию

Автоматический запуск DHCP-сервера выключен (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По команде изменяется только настройка автоматического запуска DHCP-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск в следующих случаях:
  - Включен автоматический запуск службы DHCP-relay.
  - Текущие настройки DHCP-сервера некорректны.

Пример использования

Чтобы включить автоматический запуск DHCP-сервера:

```
hostname# inet dhcp server mode on
```

inet dhcp server reset

Сбросить настройки DHCP-сервера, включая настройки автоматического запуска при загрузке ViPNet Coordinator HW, и завершить работу DHCP-сервера.

Синтаксис

```
inet dhcp server reset
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

После выполнения команды настройте параметры DHCP-сервера, иначе его запуск будет невозможен.

Пример использования

```
hostname# inet dhcp server reset
Are you sure to reset DHCP server settings to default values? [Yes/No]: Yes
```

inet dhcp server start

Запустить DHCP-сервер.

Синтаксис

```
inet dhcp server start
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Невозможно запустить DHCP-сервер в следующих случаях:

- Запущена служба DHCP-relay.
- Текущие настройки DHCP-сервера некорректны.

Пример использования

```
hostname# inet dhcp server start
Starting DHCP server ...
```

inet dhcp server stop

Завершить работу DHCP-сервера.

Синтаксис

```
inet dhcp server stop
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet dhcp server stop
Stopping DHCP server ...
```

inet dns clients add

Добавить адрес или подсеть в список клиентов DNS-сервера, развернутого на ViPNet Coordinator HW.

Синтаксис

```
inet dns clients add {<адрес>[/<длина маски>] | any}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес отдельного узла или подсети;
- `<длина маски>` — длина маски подсети;
- `any` — любые узлы.

Значения по умолчанию

По умолчанию список клиентов DNS-сервера содержит ключевое слово `any`.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы в список клиентов DNS-сервера добавить узлы из подсети 192.168.10.0/16:

```
hostname# inet dns clients add 192.168.10.0/16
Client '192.168.10.0/16' appended to the list of allowed clients
```

inet dns clients delete

Удалить адрес или подсеть из списка клиентов DNS-сервера, развернутого на ViPNet Coordinator HW.

Синтаксис

```
inet dns clients delete {<адрес>[/<длина маски>] | any}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес отдельного узла или подсети;
- `<длина маски>` — длина маски подсети;
- `any` — любые узлы.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При вводе адреса работают автодополнение и подсказка, данные для подсказки берутся из текущего списка клиентов DNS-сервера.

Пример использования

```
hostname# inet dns clients delete 192.168.0.7
Client '192.168.0.7' removed from the list of allowed clients
Reloading domain name service...: bind9.
```

inet dns clients list

Просмотреть список DNS-клиентов, которым разрешена передача запросов DNS-серверу.

Синтаксис

```
inet dns clients list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet dns clients list
Allow DNS requests from the following client(s):
192.168.0.4
192.168.0.3
192.168.0.5
```

```
any
```

inet dns forwarders add

Добавить сервер в список DNS-серверов перенаправления (forwarder), которые передают запросы DNS-серверу внешней сети. Дополнительно можно указать имя зоны, для которой осуществляется перенаправление запросов.

Синтаксис

```
inet dns forwarders add <адрес> [for-zone <имя зоны>]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес DNS-сервера.
- `<имя зоны>` — имя зоны (окончание доменного имени сетевых узлов, запросы от которых перенаправляются на DNS-сервер).

Режимы командного интерпретатора

Режим настройки

Особенности использования

- Если зона не указана, то DNS-серверу перенаправляются все запросы.
- Если IP-адрес DNS-сервера задается без зоны, то независимо от его предыдущего состояния (с зоной или без зоны), все запросы перенаправляются на DNS-сервер без зоны. При этом выводится сообщение:

  ```
  Forward DNS address <адрес> resolves both named zone and all requests
  ```

- Если IP-адрес DNS-сервера задается с зоной, то независимо от его предыдущего состояния (с зоной или без зоны), все запросы перенаправляются на DNS-сервер с зоной. При этом выводится сообщение:

  ```
  Forward DNS address <адрес> resolves both named zone and all requests
  ```

- Если DNS-сервер перенаправления не может разрешить доменное имя для указанной зоны, то для разрешения этого имени будут использоваться корневые DNS-серверы.

Примеры использования

- Чтобы в список DNS-серверов перенаправления добавить сервер с адресом 10.0.2.3:

  ```
  hostname# inet dns forwarders add 10.0.2.3
  ```

- Чтобы в список DNS-серверов перенаправления добавить сервер с адресом 10.0.2.4, который перенаправляет запросы от сетевых узлов зоны gov.ru:

  ```
  hostname# inet dns forwarders add 10.0.2.4 for-zone gov.ru
  ```

inet dns forwarders delete

Удалить сервер из списка DNS-серверов перенаправления (forwarder), которые передают запросы DNS-серверу внешней сети.

Синтаксис

```
inet dns forwarders delete <адрес> [for-zone <имя зоны>]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес удаляемого DNS-сервера.
- `<имя зоны>` — имя зоны, связанное с удаляемым DNS-сервером (окончание доменного имени сетевых узлов, запросы от которых перенаправляются на DNS-сервер).

Режимы командного интерпретатора

Режим настройки

Особенности использования

- При вводе адреса работают автодополнение и подсказка, данные для подсказки берутся из текущего списка DNS-серверов перенаправления (пересылки).
- Если удаляемый DNS-сервер был ранее связан с зоной, то в команде на удаление DNS-сервера эта зона должна быть указана.

Примеры использования

- Чтобы из списка DNS-серверов перенаправления удалить сервер с адресом 10.0.2.3:

  ```
  hostname# inet dns forwarders delete 10.0.2.3
  ```

- Чтобы из списка DNS-серверов перенаправления удалить сервер с адресом 10.0.2.4 и зоной gov.ru:

  ```
  hostname# inet dns forwarders delete 10.0.2.4 for-zone gov.ru
  ```

inet dns forwarders list

Просмотреть список DNS-серверов перенаправления (forwarder).

Синтаксис

```
inet dns forwarders list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Если адреса DNS-серверов перенаправления не заданы (список пустой), выводится информация о том, что используются корневые DNS-серверы.
- DNS-серверы, полученные по DHCP, отмечены как `from DHCP`.
- DNS-серверы, заданные пользователем, отмечены как `from USERS`.

Пример использования

```
hostname> inet dns forwarders list
Forward DNS requests to servers:
10.0.2.3 from USERS
10.0.2.4 from USERS for-zone gov.ru
```

inet dns mode

Включить или выключить автоматический запуск DNS-сервера при загрузке ViPNet Coordinator HW.

Синтаксис

```
inet dns mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения по умолчанию

Задается при установке справочников и ключей.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По команде изменяется только настройка автоматического запуска DNS-сервера, его текущее состояние не изменяется.

- Изменение настройки автоматического запуска не зависит от текущего состояния DNS-сервера (остановлен или запущен).

Пример использования

```
hostname# inet dns mode on

DNS server will be activated on next reboot

You need to start DNS server manually or reboot to have it running
```

inet dns querylog

Включить или выключить ведение журнала DNS-запросов.

Синтаксис

```
inet dns querylog {on | off}
```

Параметры и ключевые слова

- `on` — включить ведение журнала DNS-запросов;
- `off` — выключить ведение журнала DNS-запросов.

Значения по умолчанию

Ведение журнала включено и начинается после запуска DNS-сервера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если команда выполняется при запущенном DNS-сервере, он перезапускается.
- В кластере команда выполняется на активном узле.

Пример использования

```
hostname# inet dns querylog on

DNS requests logging was turned on

DNS requests log size: 50 MB
```

inet dns querylog show

Просмотреть журнал DNS-запросов.

Синтаксис

```
inet dns querylog show [filtered <строка>]
```

Параметры и ключевые слова

- `filtered` — отображает записи журнала DNS-запросов, которые содержат текст, заданный в параметре `<строка>`.
- `<строка>` — строка текста, по которой необходимо отфильтровать записи журнала DNS-запросов. Допустимые символы: `A-Z, a-z, 0-9, ! # $ % & () * + , - . / : ; < = > @ [ ] _ { | } ~`, а также пробел. Если в строке используется пробел — заключите её в двойные кавычки (`""`).

Значения по умолчанию

Без указания `filtered <строка>` постранично отображается весь журнал DNS-запросов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Команда отображает содержимое текущего файла и ротированных файлов.
- Чтобы завершить просмотр, нажмите **Q**.

Пример использования

```
hostname# inet dns querylog show filtered dns.msftncsi.com

17-Feb-2024 16:42:22.623 client @0x7f847c0a9070 192.168.56.33#50527 (dns.msftncsi.com):
query: dns.msftncsi.com IN A + (192.168.56.1)

17-Feb-2024 16:43:07.629 client @0x7f847c4ed450 192.168.56.33#59237 (dns.msftncsi.com):
query: dns.msftncsi.com IN A + (192.168.56.1)
```

inet dns querylog size

Задать размер журнала DNS-запросов.

Синтаксис

```
inet dns querylog size <размер>
```

Параметры и ключевые слова

`<размер>` — размер журнала DNS-запросов, МБайт:

- 1–50 — для исполнений с одним дисковым накопителем;
- 1–200 — для исполнений с двумя дисковыми накопителями.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если команда выполняется при запущенном DNS-сервере, он перезапускается.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet dns querylog size 100
DNS requests log size: 100 MB
```

inet dns start

Запустить DNS-сервер.

Синтаксис

```
inet dns start
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet dns start
Starting DNS server...
Starting domain name service...: bind9
```

inet dns stop

Завершить работу DNS-сервера.

Синтаксис

```
inet dns stop
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet dns stop
Stopping domain name service...: bind9.
```

inet ifconfig address

Настроить параметры сетевого интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> address <IP-адрес> netmask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<IP-адрес>` — IP-адрес.
- `<маска>` — маска подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе имени интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен относиться к классу `access` (см. inet ifconfig class).
- Если указанный интерфейс является рабочим для DHCP-сервера, то перед изменением его параметров завершите работу DHCP-сервера (см. inet dhcp server stop).

- При изменении адреса интерфейса в таблице маршрутизации автоматически изменяются все маршруты, связанные с этим интерфейсом. Скорректируйте маршрут по умолчанию и статические маршруты так, чтобы они стали удовлетворять новой адресации.
- Если ранее на указанном интерфейсе был установлен режим DHCP, то после установки параметров будет потеряна информация о DNS- и NTP-серверах, полученная от DHCP-сервера.
- В качестве IP-адреса нельзя использовать 0.0.0.0.
- В качестве маски подсети нельзя использовать маски 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети.
- Не изменяйте параметры сетевых интерфейсов, задействованных в работе кластера. Это приведет к сбою в его работе.

Пример использования

Чтобы на интерфейсе `eth1` установить IP-адрес 192.168.10.1 и маску подсети 255.255.255.0:

```
hostname# inet ifconfig eth1 address 192.168.10.1 netmask 255.255.255.0
```

inet ifconfig address add

Добавить дополнительный IP-адрес на сетевой интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> address add <IP-адрес> netmask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<IP-адрес>` — IP-адрес.
- `<маска>` — маска подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Интерфейс должен быть включен и относиться к классу `access` (см. inet ifconfig class).
- На интерфейсе не может быть установлен режим DHCP.

- По команде создается виртуальный интерфейс с именем `<интерфейс>:номер`, где `номер` — очередной свободный номер (нумерация дополнительных адресов начинается с 0). На созданном виртуальном интерфейсе задаются указанные IP-адрес и маска.
- В качестве IP-адреса нельзя использовать 0.0.0.0.
- В качестве маски подсети нельзя использовать маски 0.0.0.0, 255.255.255.254 и 255.255.255.255.
- Для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети.
- IP-адреса физического интерфейса `<интерфейс>` и созданных на нем виртуальных интерфейсов `<интерфейс>:номер`, могут относиться к одной подсети.

Пример использования

```
hostname# inet ifconfig eth1 address add 192.168.10.2 netmask 255.255.255.0

Attention: Upon changing the network interface settings, make similar changes to the
services that use this interface

and then restart them.
Alias eth1:0 was created.
```

inet ifconfig address delete

Удалить дополнительный IP-адрес с сетевого интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> address delete <IP-адрес> netmask <маска>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<IP-адрес>` — IP-адрес.
- `<маска>` — маска подсети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен быть включен и относиться к классу `access` (см. inet ifconfig class).

- При удалении дополнительного IP-адреса удаляется соответствующий ему виртуальный интерфейс.

Пример использования

Удалить дополнительный IP-адрес 192.168.10.2 с маской подсети 255.255.255.0 с интерфейса `eth1`:

```
hostname# inet ifconfig eth1 address delete 192.168.10.2 netmask 255.255.255.0

Attention: Upon changing the network interface settings, make similar changes to the
services that use this interface and then restart them.

Alias eth1:0 was deleted
```

inet ifconfig bonding add

Добавить подчиненный физический интерфейс в агрегированный интерфейс.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding add <подчиненный интерфейс>
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Подчиненный интерфейс должен относиться к классу `slave` (см. inet ifconfig class).
- Добавляемый подчиненный интерфейс не должен быть привязан ни к одному агрегированному интерфейсу.
- Ограничения на количество подчиненных интерфейсов в составе агрегированного интерфейса нет.
- Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

Пример использования

Чтобы в агрегированный интерфейс `bond1` добавить подчиненный интерфейс `eth2`:

```
hostname# inet ifconfig bond1 bonding add eth2
```

inet ifconfig bonding ad-select

Задать режим выбора активного агрегатора на агрегированном интерфейсе, работающем в режиме 802.3ad.

Синтаксис

```
inet ifconfig <интерфейс> bonding ad-select <режим>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `<режим>` — режим выбора активного агрегатора на агрегированном интерфейсе, работающем в режиме 802.3ad. Можно задать следующие значения этого параметра:
  - `stable` — режим, при котором первоначально выбирается агрегатор с наибольшей суммарной пропускной способностью подчиненных физических интерфейсов, а в дальнейшем выбор нового агрегатора выполняется только в случае сбоя всех подчиненных интерфейсов текущего агрегатора.
  - `bandwidth` — режим, при котором первоначально выбирается агрегатор с наибольшей пропускной способностью подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора.
  - `count` — режим, при котором первоначально выбирается агрегатор с наибольшим количеством подчиненных физических интерфейсов, а в дальнейшем, при добавлении, удалении или сбое подчиненных физических интерфейсов, в агрегаторах производится перегруппировка подчиненных физических интерфейсов и выполняется выбор нового агрегатора.

Значения по умолчанию

Используется режим `stable`.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме 802.3ad, активный агрегатор выбирался в соответствии с режимом `count`:

```
hostname# inet ifconfig bond1 bonding ad-select count
```

inet ifconfig bonding delete

Удалить подчиненный интерфейс из агрегированного.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding delete <подчиненный интерфейс>
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Если агрегированному интерфейсу подчинен только один физический интерфейс, то его удалить нельзя.

Пример использования

Чтобы удалить подчиненный физический интерфейс `eth2` из агрегированного интерфейса `bond1`:

```
hostname# inet ifconfig bond1 bonding delete eth2
```

inet ifconfig bonding lacp-rate

Задать частоту обмена пакетами по протоколу LACP для агрегированных интерфейсов, работающих в режиме 802.3ad.

Синтаксис

```
inet ifconfig <интерфейс> bonding lacp-rate {slow | fast}
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `slow` — обмен пакетами по протоколу LACP выполняется каждые 30 секунд.
- `fast` — обмен пакетами по протоколу LACP выполняется каждую секунду.

Значения по умолчанию

Обмен пакетами по протоколу LACP выполняется каждые 30 секунд (`slow`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме 802.3ad, обмен пакетами по протоколу LACP выполнялся каждую секунду:

```
hostname# inet ifconfig bond1 bonding lacp-rate fast
```

inet ifconfig bonding miimon

Задать частоту проверки соединения на подчиненных физических интерфейсах.

Синтаксис

```
inet ifconfig <интерфейс> bonding miimon <интервал>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.
- `<интервал>` — время в миллисекундах, через которое производится проверка соединения на подчиненных физических интерфейсах (от 1 до 1000 миллисекунд).

Значения по умолчанию

Соединение проверяется каждые 100 миллисекунд (0,1 секунды).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы на подчиненных интерфейсах агрегированного интерфейса `bond1` соединение проверялось каждые 0,5 секунды:

```
hostname# inet ifconfig bond1 bonding miimon 500
```

inet ifconfig bonding primary

Настроить агрегированный интерфейс, работающий в режиме `balance-tlb` или `active-backup`. Команда используется для принудительного выбора одного из подчиненных физических интерфейсов в качестве основного.

Синтаксис

```
inet ifconfig <агрегированный интерфейс> bonding primary {<подчиненный интерфейс> | none}
```

Параметры и ключевые слова

- `<агрегированный интерфейс>` — имя агрегированного интерфейса.
- `<подчиненный интерфейс>` — имя подчиненного интерфейса.
- `none` — отмена принудительного выбора основного интерфейса.

Значения по умолчанию

Основной интерфейс выбирается в соответствии с выбранным режимом работы агрегированного канала (`none`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме `active-backup`, принудительно выбрать в качестве основного интерфейса подчиненный интерфейс `eth1`:

```
hostname# inet ifconfig bond1 bonding primary eth1
```

inet ifconfig bonding xmit-hash-policy

Настроить агрегированный интерфейс, работающий в режиме `balance-xor` или `802.3ad`. Команда задает алгоритм вычисления хэш-функции, используемой при выборе подчиненного интерфейса, через который будет отправляться исходящий пакет.

Синтаксис

```
inet ifconfig <интерфейс> bonding xmit-hash-policy <layer2 | layer2+3 | layer3+4>
```

Параметры и ключевые слова

- `<интерфейс>` — имя агрегированного интерфейса.

- `layer2` — алгоритм, при котором для хэширования используются MAC-адреса отправителя и получателя пакета.
- `layer2+3` — алгоритм, при котором для хэширования используются MAC-адреса отправителя и получателя, а также IP-адреса отправителя и получателя (для протоколов IPv4 или IPv6).
- `layer3+4` — алгоритм, при котором для хэширования используются IP-адреса отправителя и получателя, а также номера портов TCP и UDP (при наличии).

Значения по умолчанию

По умолчанию используется алгоритм `layer2`.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы на агрегированном интерфейсе `bond1`, работающем в режиме `balance-xor`, при выборе подчиненного интерфейса, через который будет отправляться исходящий пакет, использовался алгоритм `layer2+3`:

```
hostname# inet ifconfig bond1 bonding xmit-hash-policy layer2+3
```

inet ifconfig class

Выбрать класс для сетевого интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> class {access | trunk | slave}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `trunk` — класс интерфейсов, предназначенных для передачи трафика из нескольких VLAN.
- `slave` — класс интерфейсов, предназначенных для использования в составе агрегированных интерфейсов.
- `access` — класс интерфейсов, предназначенных для использования во всех остальных случаях.

Значения по умолчанию

Все физические интерфейсы ViPNet Coordinator HW относятся к классу `access`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если для указанного интерфейса смена класса выполняется впервые, то будет запрошено подтверждение операции.
- Класс `trunk` можно установить только для физических и агрегированных интерфейсов. Виртуальные интерфейсы всегда относятся к классу `access`.
- Для агрегированных и виртуальных интерфейсов нельзя установить класс `slave`.
- Нельзя установить класс `trunk`, если на указанном интерфейсе запущен или настроен на автоматический запуск DHCP-сервер или служба DHCP-relay.
- Если на указанном интерфейсе задан один или несколько IP-адресов, то для установки класса `trunk` требуется дополнительное подтверждение. После установки класса `trunk` все адреса будут потеряны.
- Перед установкой класса `access` или `slave` требуется удалить все виртуальные интерфейсы, созданные на базе указанного интерфейса.
- Перед тем как изменить класс интерфейса `slave` на `access` или `trunk`, необходимо, чтобы он не был подчинен ни одному агрегированному интерфейсу.

Пример использования

Чтобы установить класс `trunk` на интерфейсе `eth1` для возможности создавать на его базе виртуальные интерфейсы:

```
hostname# inet ifconfig eth1 class trunk
```

inet ifconfig disable

Запретить прохождения IP-трафика через сетевой интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> disable
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда удаляет сетевой интерфейс `<интерфейс>` из конфигурационного файла `iplir.conf`.
- После выполнения команды выводится предупреждение о необходимости проверить, соответствуют ли сетевые фильтры политике безопасности вашей организации.

Пример использования

```
hostname# inet ifconfig eth1.10 disable

Set eth1.10 allowTraffic as off

Attention: Upon changing this parameter, make sure that firewall rules match your
organization's security policy.
```

inet ifconfig dhcp

Установить режим DHCP на сетевом интерфейсе.

Синтаксис

```
inet ifconfig <интерфейс> dhcp [<настройка> {on | off}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<настройка>` — название настройки, передаваемой с помощью DHCP. Можно указать одно из следующих значений:
  - `dns` — адреса DNS-серверов;
  - `route` — маршруты;
  - `ntp` — адреса NTP-серверов.
- `on` — включить автоматический приём указанной настройки.
- `off` — выключить автоматический приём указанной настройки.

Значения по умолчанию

Для всех настроек, передаваемых с помощью DHCP, автоматический прием включен (`on`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Интерфейс должен относиться к классу `access` (см. inet ifconfig class) или являться агрегированным интерфейсом.
- Если на интерфейсе заданы дополнительные адреса, они будут потеряны после установки режима DHCP.

Пример использования

- Чтобы только установить на интерфейсе `eth1` режим DHCP:

  ```
  hostname# inet ifconfig eth1 dhcp
  ```

- Чтобы установить на интерфейсе `eth2` режим DHCP и выключить автоматический прием маршрута по умолчанию:

  ```
  hostname# inet ifconfig eth2 dhcp route off
  ```

inet ifconfig dhcp route-metric

Задать специфичную метрику маршрутам, поступающим от DHCP-сервера, на сетевом интерфейсе ViPNet Coordinator HW.

Синтаксис

```
inet ifconfig <интерфейс> dhcp route-metric {<метрика> | none}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<метрика>` — метрика. Возможные значения: 1–255.
- `none` — удаляет метрику на сетевом интерфейсе.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если на сетевом интерфейсе не установлен режим DHCP (см. inet ifconfig dhcp), то заданная метрика будет сохранена. Но метрика начнет учитываться только после того, как режим DHCP будет установлен.
- Интерфейс должен относиться к классу `access` (см. inet ifconfig class) или являться агрегированным интерфейсом.

- При удалении специфичной метрики будет использоваться метрика по умолчанию для маршрутов DHCP-сервера (см. inet dhcp client route-default-metric).

Пример использования

- Чтобы назначить на сетевом интерфейсе `eth0` метрику 50:

  ```
  hostname# inet ifconfig eth0 dhcp route-metric 50
  ```

- Чтобы удалить метрику на сетевом интерфейсе `eth0`:

  ```
  hostname# inet ifconfig eth0 dhcp route-metric none
  ```

inet ifconfig down

Выключить сетевой интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> down
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если существуют виртуальные интерфейсы, созданные на базе указанного интерфейса, то требуется дополнительно подтвердить выключение интерфейса. Вместе с интерфейсом автоматически будут выключены все его виртуальные интерфейсы независимо от их текущего состояния.
- Если указанный интерфейс является рабочим для DHCP-сервера, то его нельзя выключить в следующих случаях:
  - DHCP-сервер запущен.
  - DHCP-сервер не запущен, но включен его автоматический запуск при загрузке ViPNet Coordinator HW.

Пример использования

Чтобы выключить виртуальный интерфейс `eth1.2`:

```
hostname# inet ifconfig eth1.2 down
```

inet ifconfig enable

Разрешить прохождения IP-трафика через сетевой интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> enable
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда добавляет сетевой интерфейс `<интерфейс>` в конфигурационный файл `iplir.conf`, если его нет.
- После выполнения команды выводится предупреждение о необходимости проверить, соответствуют ли сетевые фильтры политике безопасности вашей организации.

Пример использования

```
hostname# inet ifconfig eth1.10 enable

Set eth1.10 allowTraffic as on

Attention: Upon changing this parameter, make sure that firewall rules match your
organization's security policy.
```

inet ifconfig mtu

Изменить значение MTU для сетевого интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> mtu {<значение MTU> | auto}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<значение MTU>` — размер MTU в байтах. Допустимые значения: 1280–9000.
- `auto` — задает значение MTU по умолчанию (1500 байт).

Значения по умолчанию

По умолчанию используется значение MTU 1500 байт.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Ограничения ViPNet Coordinator VA на платформах виртуализации:
  - VMware Workstation и VMware vSphere — для изменения MTU предварительно настройте платформу виртуализации, разрешив использование Jumbo-кадров.
  - Oracle VM VirtualBox — изменение MTU не поддерживается при использовании сетевых устройств AMD.
- Команда не используется:
  - для сетевых интерфейсов подключения к беспроводной сети Wi-Fi или мобильной сети (`wlanX` и `pppX`);
  - для сетевых интерфейсов классов `vlan` и `slave`;
  - для интерфейсов синхронизации кластера.
- Значение MTU, заданное для интерфейса класса `trunk`, автоматически применяется ко всем виртуальным интерфейсам класса `vlan`, созданным на этом физическом интерфейсе.
- Значение MTU, заданное для интерфейса класса `bond`, будет использоваться на всех подчиненных физических интерфейсах класса `slave`.
- При создании агрегированного интерфейса с помощью командного интерпретатора для всех подчиненных физических интерфейсов автоматически задается значение MTU 1500 байт.
- Если вы исключаете подчиненный физический интерфейс из агрегированного, для него устанавливается значение MTU 1500 байт.

Пример использования

Задать размер MTU, равный 3000 байт, для интерфейса `eth0`:

```
hostname# inet ifconfig eth0 mtu 3000
```

inet ifconfig reset

Сбросить настройки одного сетевого интерфейса либо всех интерфейсов.

Синтаксис

```
inet ifconfig {<интерфейс> | all} reset
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `all` — все интерфейсы.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При выполнении команды с параметром `all` происходит сброс настроек всех физических интерфейсов. Все виртуальные интерфейсы при этом удаляются.
- Если вы хотите выполнить команду для физического интерфейса, для которого созданы `VLAN` или агрегированные (`bond`) интерфейсы, то сначала удалите эти интерфейсы с помощью команды iplir adapter delete. Иначе записи о VLAN и агрегированных интерфейсах останутся в конфигурационном файле `iplir.conf`, и их будет необходимо удалить вручную, чтобы еще раз использовать эти же имена интерфейсов.
- Команда используется для подготовки указанного интерфейса к установке новых параметров.
- По команде будут выполнены изменения в настройках указанного физического интерфейса:
  - Удалены все существующие дополнительные адреса интерфейса и виртуальные интерфейсы, созданные на его базе.
  - Удалена информация об IP-адресе и маске подсети.
  - Установлен режим автоматического определения параметров скорости интерфейса (см. inet ifconfig speed auto).
  - Интерфейс будет выключен.
- Для виртуальных интерфейсов класса `slave` команда не выполняется.
- Для виртуальных интерфейсов VLAN по команде не сбрасываются настройки:
  - Имя соответствующего физического интерфейса.
  - Номер виртуального интерфейса VLAN.
- Для агрегированных интерфейсов по команде не сбрасываются настройки:
  - Имя агрегированного интерфейса.
  - Режим работы агрегированного интерфейса.
  - Частота проверки соединения на подчиненных физических интерфейсах.

Пример использования

Чтобы сбросить настройки интерфейса `eth1`:

```
hostname# inet ifconfig eth1 reset
This command will reset eth1 interface settings to default. Are you sure? [Yes/No]: Yes
```

```
done.
```

inet ifconfig speed

Задать параметры скорости сетевого интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> speed <скорость> duplex {half | full} autoneg {on | off}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<скорость>` — скорость в Мбит/с. Возможные значения: `10`, `100`, `1000`, `10000` (для исполнений, оборудованных соответствующими интерфейсами).
- `duplex` — режим передачи данных:
  - `half` — полудуплекс;
  - `full` — полный дуплекс.
- `autoneg` — режим автосогласования скорости интерфейса (autonegotiation):
  - `on` — включен;
  - `off` — выключен.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Нельзя установить параметры скорости виртуального интерфейса, так как он наследует эти параметры от соответствующего физического интерфейса.
- Команда неприменима на ViPNet Coordinator VA.
- Команда неприменима к интерфейсам класса slave (см. inet ifconfig class).
- Установку параметров скорости интерфейса следует использовать только в тех случаях, когда это действительно необходимо — например, для согласования работы внешнего интерфейса ViPNet Coordinator HW и коммутационного оборудования, подключенного к данному интерфейсу.
- Нельзя изменить параметры скорости оптических интерфейсов (для исполнений, оборудованных соответствующими разъемами).

- На интерфейсах `eth0–eth3` исполнения ViPNet Coordinator HW100 (аппаратная платформа HW100 Q1, Q2) невозможно установить режим передачи данных `half`.

Пример использования

На интерфейсе `eth1` установить скорость 100 Мбит/с, режим полудуплекса и отключить режим автосогласования:

```
hostname# inet ifconfig eth1 speed 100 duplex half autoneg off
```

inet ifconfig speed auto

Установить режим автоматического определения параметров скорости на сетевом интерфейсе.

Синтаксис

```
inet ifconfig <интерфейс> speed auto
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- После выполнения команды режим автосогласования (autonegotiation) на интерфейсе принимает значение `on` (включен).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Нельзя установить параметры скорости виртуального интерфейса, так как он наследует эти параметры от соответствующего физического интерфейса.
- Команда неприменима на ViPNet Coordinator VA.
- Команда неприменима к интерфейсам класса slave (см. inet ifconfig class).

Пример использования

Установить режим автоматического определения параметров скорости на интерфейсе `eth1`:

```
hostname# inet ifconfig eth1 speed auto
```

inet ifconfig up

Включить сетевой интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> up
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если существуют виртуальные интерфейсы, созданные на базе указанного интерфейса, то требуется дополнительно подтвердить включение интерфейса. Вместе с интерфейсом автоматически будут включены все его виртуальные интерфейсы независимо от их текущего состояния.
- Нельзя включить виртуальный интерфейс, если выключен соответствующий физический интерфейс.

Пример использования

Чтобы включить виртуальный интерфейс `eth1.2`:

```
hostname# inet ifconfig eth1.2 up
```

inet ifconfig vlan add

Создать интерфейс для виртуальной сети с заданным номером.

Синтаксис

```
inet ifconfig <интерфейс> vlan add <номер>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<номер>` — номер виртуальной сети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Физический интерфейс должен относиться к классу `trunk` (см. inet ifconfig class).
- По команде будет создан виртуальный интерфейс с именем `<интерфейс>.<номер>`. Созданный интерфейс будет иметь то же состояние (включен или выключен), что и физический интерфейс.
- Максимальное количество интерфейсов в ViPNet Coordinator HW (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.
- Номер виртуальной сети `<номер>` должен находиться в диапазоне от 1 до 4094. Значения 0 и 4095 зарезервированы.

Пример использования

Чтобы на базе интерфейса `eth1` создать интерфейс для виртуальной сети с номером 2:

```
hostname# inet ifconfig eth1 vlan add 2
```

inet ifconfig vlan delete

Удалить виртуальный интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> vlan delete <номер>
```

Параметры и ключевые слова

- `<интерфейс>` — имя физического интерфейса.
- `<номер>` — номер виртуальной сети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе номера работают автодополнение и подсказка, данные для подсказки берутся из списка существующих виртуальных интерфейсов.
- Невозможно удалить виртуальный интерфейс, заданный как рабочий в параметрах функции L2OverIP, если эта функция включена (см. iplir set l2overip mode).

Пример использования

Чтобы удалить виртуальный интерфейс `eth1.2`:

```
hostname# inet ifconfig eth1 vlan delete 2
```

inet ntp add

Добавить сервер в список NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp add {server | peer} {<IP-адрес> | <доменное имя>}
```

Параметры и ключевые слова

- `server` — добавить NTP-сервер, работающий в одностороннем режиме (рассылка данных времени).
- `peer` — добавить NTP-сервер, работающий в двустороннем режиме (рассылка и получение данных времени).
- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<доменное имя>` — доменное имя NTP-сервера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда выполняется на активном узле.

Пример использования

Добавить сервер `ntp.psn.ru`, работающий в одностороннем режиме:

```
hostname# inet ntp add server ntp.psn.ru
NTP server ntp.psn.ru has been inserted successfully
```

inet ntp delete

Удалить сервер из списка NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp delete {server | peer} {<IP-адрес> | <доменное имя>}
```

Параметры и ключевые слова

- `server` — удалить NTP-сервер, работающий в одностороннем режиме (рассылка данных времени).
- `peer` — удалить NTP-сервер, работающий в двустороннем режиме (рассылка и получение данных времени).
- `<IP-адрес>` — IP-адрес NTP-сервера.
- `<доменное имя>` — доменное имя NTP-сервера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе IP-адреса или доменного имени работают автодополнение и подсказка, данные для подсказки берутся из текущего списка NTP-серверов.
- В кластере команда выполняется на активном узле.

Пример использования

Чтобы из списка NTP-серверов удалить сервер `ntp.psn.ru`, работающий в одностороннем режиме:

```
hostname# inet ntp delete server ntp.psn.ru
```

inet ntp list

Просмотреть список NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- NTP-серверы, заданные по умолчанию, отмечены как `from DEFAULT`.

- NTP-серверы, полученные по DHCP, отмечены как `from DHCP`.
- NTP-серверы, заданные пользователем, отмечены как `from USER`.

Пример использования

```
hostname> inet ntp list
NTP servers list:
server ntp1.vniiftri.ru from DEFAULT
server ntp2.vniiftri.ru from DEFAULT
server ntp.ix.ru from DEFAULT
server 10.0.2.1 from USER
peer 10.0.2.4 from USER
```

inet ntp mode

Включить или выключить автоматический запуск NTP-сервера при загрузке ViPNet Coordinator HW.

Синтаксис

```
inet ntp mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Значения по умолчанию

Задается при установке справочников и ключей.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда изменяет только настройку автоматического запуска NTP-сервера, его текущее состояние не изменяется.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Выключить автоматический запуск NTP-сервера:

```
hostname# inet ntp mode off
```

inet ntp orphan

Включить или выключить переход локального NTP-сервера в изолированный (orphan) режим при потере соединения с внешними NTP-серверами.

Синтаксис

```
inet ntp orphan {on <stratum> | off}
```

Параметры и ключевые слова

`<stratum>` — используется для задания уровня внешнего NTP-сервера. Если со всеми внешними NTP-серверами меньше указанного уровня не удается установить соединение в течение 5 минут, то локальный NTP-сервер переходит в изолированный режим. Допустимы значения 1–10, рекомендуемое значение 5.

Значения по умолчанию

По умолчанию для параметра `<stratum>` установлено значение 5.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда выполняется на активном узле.

Пример использования

Чтобы настроить переход локального NTP-сервера в изолированный режим при потере соединения с внешними NTP-серверами 5-го уровня:

```
hostname# inet ntp orphan on 5
```

inet ntp start

Запустить NTP-сервер.

Синтаксис

```
inet ntp start
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet ntp start
Starting NTP server...
```

inet ntp stop

Завершить работу NTP-сервера.

Синтаксис

```
inet ntp stop
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet ntp stop
Stopping NTP server: ntpd.
```

inet ospf area auth

Включить или выключить аутентификацию в протоколе OSPF.

Синтаксис

```
inet ospf area <0-4294967295> auth {on {pswd | md5} | off}
```

Параметры и ключевые слова

- `area <0-4294967295>` — область маршрутизации OSPF;
- `on` — включить аутентификацию для выбранной области. Методы аутентификации:
  - `pswd` — аутентификация на основе открытого пароля (Simple Password);
  - `md5` — аутентификация на основе MD5 HMAC.
- `off` — выключить аутентификацию для выбранной области.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При включении аутентификации для области маршрутизации выводится предупреждение о необходимости настройки идентификационной информации на интерфейсе.
- Если для области маршрутизации уже назначен метод аутентификации, команда изменяет этот метод.
- В кластере команда выполняется на активном узле.

Пример использования

Включить аутентификацию для области маршрутизации 1 с использованием MD5 HMAC:

```
hostname# inet ospf area 1 auth on md5

Area 1 authentication using MD5 is ON.

Make sure that authentication method is set up on the appropriate interface.
```

inet ospf interface keys add

Добавить ключ для аутентификации MD5 HMAC.

Синтаксис

```
inet ospf interface <интерфейс> keys add <keyid>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса (физический, `vlan`, `bond`);
- `<keyid>` — идентификатор ключа. Допустимые значения: `1–255`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Ключ вводится интерактивно.
- Требования к ключу:
  - длина : 1–16 символов;
  - допустимые символы: `A-Z, a-z, 0-9, ! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

- В кластере команда выполняется на активном узле.

Пример использования

Добавить ключ с идентификатором 1 на интерфейс `eth0`:

```
hostname# inet ospf interface eth0 keys add 1
Set key 1:
Confirm key 1:
Key 1 on eth0 added
```

inet ospf interface keys remove

Удалить ключ для аутентификации MD5 HMAC.

Синтаксис

```
inet ospf interface <интерфейс> keys remove {all | <keyid>}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса (физический, `vlan`, `bond`);
- `<keyid>` — идентификатор ключа. Допустимые значения: `1–255`;
- `all` — удалить все ключи на интерфейсе.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда выполняется на активном узле.

Пример использования

Удалить ключ на интерфейсе `eth0`:

```
hostname# inet ospf interface eth0 keys remove 1
Key 1 on eth0 removed
```

inet ospf interface password

Установить или удалить пароль для аутентификации на выбранном интерфейсе.

Синтаксис

```
inet ospf interface <интерфейс> password [remove]
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса (физический, `vlan`, `bond`);
- `remove` — удалить пароль.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Пароль вводится интерактивно.
- Требования к паролю:
  - длина пароля: 1–8 символов;
  - допустимые символы: `A-Z, a-z, 0-9, ! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- В кластере команда выполняется на активном узле.

Пример использования

- Установить пароль на интерфейсе `eth0`:

```
hostname# inet ospf interface eth0 password
Set password for eth0:
Confirm password for eth0:
Password on eth0 set.
```

- Удалить пароль на интерфейсе `eth0`:

```
hostname# inet ospf interface eth0 password remove
Password on eth0 removed
```

inet ospf mode

Включить или выключить использование протокола OSPF.

Синтаксис

```
inet ospf mode {on | off}
```

Параметры и ключевые слова

- `on` — включить использование протокола OSPF;
- `off` — выключить использование протокола OSPF.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet ospf mode on

Starting ospf...
```

inet ospf network add

Добавить сеть, в которой должна выполняться маршрутизация по протоколу OSPF.

Синтаксис

```
inet ospf network add <IP-адрес назначения> netmask <маска сети> area <0-4294967295>
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес сети.
- `<маска сети>` — маска сети.
- `area <0-4294967295>` — область маршрутизации.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Если использование протокола OSPF не включено, задать сеть невозможно.

Пример использования

```
hostname# inet ospf network add 10.0.5.0 netmask 255.255.255.0 area 1

The following OSPF network has been added:

Destination    Netmask          OSPF Area     Authentication

-----------    -------          ---------     ---------
```

```
10.0.5.0        255.255.255.0    1            No
```

inet ospf network delete

Удалить сеть, которая была указана как маршрутизируемая по протоколу OSPF.

Синтаксис

```
inet ospf network delete <IP-адрес назначения> netmask <маска сети> area <0-4294967295>
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес сети.
- `<маска сети>` — маска сети.
- `area <0-4294967295>` — область маршрутизации.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если использование протокола OSPF не включено, удалить сеть невозможно.
- Если в конфигурации протокола OSPF указанная сеть не будет найдена, ее удаление будет невозможно.

Пример использования

```
hostname# inet ospf network delete 10.0.5.0 netmask 255.255.255.0 area 1

The following OSPF network has been deleted:

Destination   Netmask       OSPF Area

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

10.0.5.0      255.255.255.0 1
```

inet ospf redistribute add

Включить перераспределение статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол OSPF.

Синтаксис

```
inet ospf redistribute add {static | dhcp}
```

Параметры и ключевые слова

- `static` — включить перераспределение статических маршрутов;
- `dhcp` — включить перераспределение маршрутов DHCP-сервера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда не будет выполнена в следующих случаях:

- Не включено использование протокола OSPF (см. inet ospf mode).
- Перераспределение указанного типа маршрутов было включено ранее.

Пример использования

```
hostname# inet ospf redistribute add static
Redistribution of static routes has been enabled.
```

inet ospf redistribute delete

Выключить перераспределение статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол OSPF.

Синтаксис

```
inet ospf redistribute delete {static | dhcp}
```

Параметры и ключевые слова

- `static` — выключить перераспределение статических маршрутов;
- `dhcp` — выключить перераспределение маршрутов DHCP-сервера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда не будет выполнена в следующих случаях:

- Не включено использование протокола OSPF (см. inet ospf mode).
- Перераспределение указанного типа маршрутов не было включено ранее.

Пример использования

```
hostname# inet ospf redistribute delete static

Redistribution of static routes has been disabled.
```

inet ospf priority

Задать приоритет ViPNet Coordinator HW.

Синтаксис

```
inet ospf priority <приоритет> [interface <интерфейс>]
```

Параметры и ключевые слова

- `<приоритет>` — целое число из диапазона 0–255.
- `<интерфейс>` — имя интерфейса.

Значения по умолчанию

Значение приоритета по умолчанию — 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Использование команды `inet ospf priority` разрешено, если на ViPNet Coordinator HW включен протокол маршрутизации OSPF (см. inet ospf mode).
- Чем больше значение приоритета, тем выше вероятность того, что ViPNet Coordinator HW будет выбран назначенным маршрутизатором DR или резервным назначенным маршрутизатором BDR.
- Если приоритет равен нулю, то ViPNet Coordinator HW не участвует в выборе DR или BDR.
- Если ключевое слово `interface` не задано, то значение приоритета для всех интерфейсов ViPNet Coordinator HW устанавливается равным параметру `<приоритет>`.

Пример использования

```
hostname# inet ospf priority 10
```

```
Stopping ospf ...

Starting ospf ...
```

inet ospf router-id

Задать идентификатор ViPNet Coordinator HW в формате адреса протокола IPv4.

Синтаксис

```
inet ospf router-id {<идентификатор> | auto}
```

Параметры и ключевые слова

- `<идентификатор>` — идентификатор ViPNet Coordinator HW в формате адреса протокола IPv4.
- `auto` — автоматический выбор идентификатора ViPNet Coordinator HW исходя из максимального значения IP-адреса, назначенного на интерфейсах ViPNet Coordinator HW.

Значения по умолчанию

Максимальное значение IP-адреса из назначенных на интерфейсах ViPNet Coordinator HW.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Использование команды разрешено, если на ViPNet Coordinator HW включен протокол маршрутизации OSPF (см. inet ospf mode).
- Если в сети со множественным доступом у двух маршрутизаторов будут одинаковые идентификаторы, то такие маршрутизаторы не смогут установить отношения соседства.

Пример использования

```
hostname# inet ospf router-id 172.16.12.1

Stopping ospf ...

Starting ospf ...

OSPF router-id 172.16.12.1 has been set for this router.
```

inet ospf show configuration

Просмотреть настройки протокола OSPF.

Синтаксис

```
inet ospf show configuration
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде выводится следующая информация:
  - состояние протокола OSPF: включен/выключен;
  - состояние автоматического запуска протокола OSPF при старте ViPNet Coordinator HW: включен/выключен;
  - идентификатор ViPNet Coordinator HW;
  - состояние перераспределения статических маршрутов: включены/выключены;
  - состояние перераспределения DHCP маршрутов: включены/выключены;
  - список сетей, в которых ViPNet Coordinator HW осуществляет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);
  - приоритеты ViPNet Coordinator HW на интерфейсах.
- В кластере команда выполняется на активном узле.

Пример использования

```
hostname> inet ospf show configuration


OSPF protocol autostart is on

OSPF protocol has been enabled

OSPF router id is 172.20.20.100

Redistribution of static routes is enabled.

Redistribution of DHCP routes is enabled.

Destination     Netmask         OSPF Area   Authentication

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

172.20.20.0     255.255.255.0   0           No

172.20.21.0     255.255.255.0   1           MD5

172.20.22.0     255.255.255.0   2           Password


Interface:  OSPF priority   Password    Keyid
```

```
------------------------------------------------
eth0:       1               No          1,2,3
eth1:       20              Yes         No
```

inet ospf show database

Просмотреть информацию о состоянии каналов связи между всеми OSPF-маршрутизаторами в базе данных (link state database).

Синтаксис

```
inet ospf show database
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet ospf show database

       OSPF Router with ID (10.0.5.2)

              Router Link States (Area 0.0.0.0)

Link ID      ADV Router   Age      Seq#         CkSum     Link count

10.0.3.2     10.0.3.2     155      0x8000017d   0x590a    2

10.1.30.5    10.1.30.5    220      0x8000029f   0x3fa0    2

              Net Link States (Area 0.0.0.0)

Link ID      ADV Router   Age      Seq#         CkSum

10.0.5.5     10.1.30.5    751      0x80000263   0x3541

              AS External Link States

Link ID      ADV Router   Age      Seq#         CkSum    Route

10.0.1.0     10.1.30.5    1551     0x80000182   0x9061   E2 10.0.1.0/24 [0x0]

10.0.2.0     10.1.30.5    1001     0x80000183   0x836c   E2 10.0.2.0/24 [0x0]

10.0.3.0     10.1.30.5    210      0x80000182   0x7a75   E2 10.0.3.0/24 [0x0]

10.0.4.0     10.1.30.5    341      0x80000182   0x6f7f   E2 10.0.4.0/24 [0x0]

10.100.1.0   10.1.30.5    911      0x8000029d   0xe1ad   E2 10.100.1.0/24 [0x0]
```

```
10.100.2.0    10.1.30.5    180      0x8000029f    0xe0aa    E2 10.100.2.0/24 [0x0]

192.168.0.0   10.1.30.5    821      0x80000182    0x6c27    E2 192.168.0.0/16 [0x0]
```

inet ospf show neighbour

Просмотреть сведения о соседних OSPF-маршрутизаторах, работающих в вашей сети по протоколу OSPF.

Синтаксис

```
inet ospf show neighbour
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet ospf show neighbour

Neighbor ID    Pri    State      Dead Time   Address    Interface       RXmtl   Rqstl   DBsml

10.1.30.5      1      Full/DR    33.310s     10.0.5.5   eth0:10.0.5.2   0       0       0
```

По команде выводится следующая информация для каждого маршрутизатора:

- IP-адрес активного сетевого интерфейса, по которому доступен маршрутизатор для обмена информацией по протоколу OSPF;
- порядковый номер маршрутизатора, под которым он известен другим маршрутизаторам при работе по протоколу OSPF;
- тип маршрутизатора (в приведенном примере маршрутизатор-сосед является назначенным, что показывает значение `DR` в поле `State`);
- интервал простоя маршрутизатора, по истечении которого он будет считаться неактивным (выключенным);
- другие параметры.

inet ping

Проверить соединение с сетевым узлом.

Синтаксис

```
inet ping <адрес> [count <value>] [iface <name>] [size <value>]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `count <value>` — число ICMP-запросов. Диапазон допустимых значений: 1–2147483647.
- `iface <name>` — имя сетевого интерфейса, с которого выполняется проверка соединения.
- `size <value>` — размер ICMP-запроса в байтах без учета ICMP-заголовка. Диапазон допустимых значений: 0–65507.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- IP-адреса сетевого узла и сетевого интерфейса, с которого выполняется проверка соединения, должны принадлежать одной подсети.
- Чтобы завершить проверку соединения, нажмите **Ctrl+C**.
- Если параметр `count` не задан, то ICMP-запросы выполняются циклически до завершения проверки соединения по **Ctrl+C**.
- Если параметр `size` не задан, то размер ICMP-запроса равен 64 байтам (56 байт + 8 байт ICMP-заголовка). Фактический размер отправляемого пакета — 84 байта (добавляется 20 байт TCP-заголовка).

Пример использования

```
hostname# inet ping 10.0.2.1 count 5
Pinging 10.0.2.1
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_req=1 ttl=255 time=2.98 ms
64 bytes from 10.0.2.1: icmp_req=2 ttl=255 time=1.60 ms
64 bytes from 10.0.2.1: icmp_req=3 ttl=255 time=1.14 ms
64 bytes from 10.0.2.1: icmp_req=4 ttl=255 time=1.71 ms

64 bytes from 10.0.2.1: icmp_req=5 ttl=255 time=1.33 ms
--- 10.0.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packets loss, time 3004ms
rtt min/avg/max/mdev = 1.144/1.862/2.983/0.683 ms
```

inet policy active

Задать действующую политику маршрутизации.

Синтаксис

```
inet policy active {<имя политики> | default}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации.
- `default` — политика маршрутизации по умолчанию.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда может быть использована в качестве параметра команды inet dgd rule add action-priority.

Пример использования

```
hostname# inet policy active policy1
Inet policy active was set to policy1
```

inet policy rule add match

Задать условие применения правила политики маршрутизации.

Синтаксис

```
inet policy rule add <имя политики> <приоритет> match {address {from | to} <IP-адрес/маска>
| {inbound-interface | outbound-interface} <интерфейс> | dscp <значение метки DSCP>}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа;
- `<приоритет>` — приоритет правила в списке, возможные значения от 1024 до 2048. Чем меньше значение, тем выше приоритет правила;
- `from` — IP-пакеты получены от указанной подсети;
- `to` — IP-пакеты отправлены в указанную подсеть;
- `<IP-адрес/маска>` — IP-адрес и маска подсети в формате `X.X.X.X/X`;

- `inbound-interface` — IP-пакеты поступили на указанный интерфейс;
- `outbound-interface` — IP-пакеты отправлены с указанного интерфейса;
- `<интерфейс>` — имя сетевого интерфейса;
- `dscp` — IP-пакет с меткой Differentiated Services Code Point (DSCP);
- `<значение метки DSCP>` — значение метки DSCP, шестнадцатеричное или цифро-буквенное значение из следующего списка:
  - 0x28 (AF11);
  - 0x30 (AF12);
  - 0x38 (AF13);
  - 0x48 (AF21);
  - 0x50 (AF22);
  - 0x58 (AF23);
  - 0x68 (AF31);
  - 0x70 (AF32);
  - 0x78 (AF33);
  - 0x88 (AF41);
  - 0x90 (AF42);
  - 0x98 (AF43);
  - 0x20 (CS1);
  - 0x40 (CS2);
  - 0x60 (CS3);
  - 0x80 (CS4);
  - 0xA0 (CS5);
  - 0xC0 (CS6);
  - 0xE0 (CS7);
  - 0xB8 (EF).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если политики с указанным именем не существует, создается новая.
- Если правило с указанным приоритетом существует, условие добавляется в него. Если нет — создается новое правило.

- Правило может содержать несколько условий, которые применяются одновременно.
- Чтобы правило с заданными условиями применялось, задайте действие с помощью команды inet policy rule add.
- Чтобы изменить условие применения правила, удалите его (inet policy rule delete match), а затем задайте новое.

Пример использования

- Создать правило высшего приоритета (1024) политики `policy1` для обработки IP-пакетов от подсети 192.168.1.0/30:

  ```
  hostname# inet policy rule add policy1 1024 match address from 192.168.1.0/30
  Inet policy policy1 1024 match from policy1 was created.
  ```

- Создать правило приоритета 1025 политики `policy2` для обработки IP-пакетов, поступающих на сетевой интерфейс `eth1`:

  ```
  hostname# inet policy rule add policy2 1025 match inbound-interface eth1
  Inet policy policy2 1025 match inbound-interface eth1 was created.
  ```

- Добавить для правила, созданного в предыдущем примере, обработку IP-пакетов, отправленных через интерфейс `eth2`:

  ```
  hostname# inet policy rule add policy2 1025 match outbound-interface eth2
  Inet policy policy2 1025 match outbound-interface eth2 was created.
  ```

- Создать правило приоритета 1026 политики `policy3` для обработки IP-пакетов с меткой DSCP со значением 0x80:

  ```
  hostname# inet policy rule add policy3 1026 match dscp 0x80
  Inet policy policy3 1026 match dscp 0x80 was created.
  ```

inet policy rule add

Задать действие правила политики маршрутизации.

Синтаксис

```
inet policy rule add <имя политики> <приоритет> {table {<номер таблицы> | name <имя таблицы>
| default} | block}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `<приоритет>` — приоритет таблицы маршрутизации, возможные значения от 1024 до 2048. Чем меньше значение, тем выше приоритет правила.
- `table` — обрабатывать IP-пакеты по указанной таблице маршрутизации.

- `<номер таблицы>` — номер пользовательской таблицы маршрутизации.
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации.
- `default` — таблица маршрутизации по умолчанию.
- `block` — блокировать IP-пакеты без ICMP-сообщений.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если политики с указанным именем не существует, создается новая.
- Если правила с указанным приоритетом не существует в политике маршрутизации, создается новое правило для обработки всех IP-пакетов. Чтобы определить условие применения правила, выполните команду inet policy rule add match.

Пример использования

- Для правила высшего приоритета политики `policy1` задать способ обработки IP-пакетов по пользовательской таблице маршрутизации `table1`:

  ```
  hostname# inet policy rule add policy1 1024 table name table1
  Inet policy policy1 1024 set table table1 was created.
  ```

- Создать правило приоритета 1027 политики `policy2` для обработки IP-пакетов по таблице маршрутизации по умолчанию:

  ```
  hostname# inet policy rule add policy2 1027 table default
  Inet policy policy2 1025 set table default was created.
  ```

inet policy rule clear

Удалить все правила политики маршрутизации или правила заданного приоритета.

Синтаксис

```
inet policy rule clear <имя политики> [priority <приоритет>]
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации;
- `<приоритет>` — приоритет правила в списке, возможные значения от 1024 до 2048.

Режимы командного интерпретатора

Режим настройки.

Пример использования

- Чтобы удалить все правила, заданные в политике маршрутизации `policy1`:

```
hostname# inet policy rule clear policy1
Delete all policy rules? [Yes/No]: Yes
Inet policy policy1 was deleted.
```

- Чтобы удалить только правила приоритета 1025, заданные в политике маршрутизации `policy2`:

```
hostname# inet policy rule clear policy2 priority 1025
Inet policy policy2 1025 was deleted.
```

inet policy rule delete match

Удалить условие применения правила политики маршрутизации.

Синтаксис

```
inet policy rule delete <имя политики> <приоритет> match {address {from | to}
<IP-адрес/маска> | {inbound-interface | outbound-interface} <интерфейс> | dscp <значение
метки DSCP>}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации;
- `<приоритет>` — приоритет правила в списке, возможные значения от 1024 до 2048;
- `from` — IP-пакеты получены от указанной подсети;
- `to` — IP-пакеты отправлены в указанную подсеть;
- `<IP-адрес/маска>` — IP-адрес и маска подсети в формате X.X.X.X./X;
- `inbound-interface` — IP-пакеты получены на указанный сетевой интерфейс;
- `outbound-interface` — IP-пакеты отправлены с указанного сетевого интерфейса;
- `<интерфейс>` — имя сетевого интерфейса;
- `dscp` — IP-пакет с меткой Differentiated Services Code Point (DSCP);
- `<значение метки DSCP>` — значение метки DSCP, шестнадцатеричное или цифро-буквенное значение (возможные значения см. в описании команды inet policy rule add match).

Режимы командного интерпретатора

Режим настройки.

Пример использования

- Чтобы в правиле приоритета 1025 политики `policy2` удалить условие обработки IP-пакетов от подсети 192.168.1.0/30:

  ```
  hostname# inet policy rule delete policy2 1025 match address from 192.168.1.0/30
  Inet policy policy2 1025 match from 192.168.1.0/30 was deleted.
  ```

- Чтобы в правиле приоритета 1026 политики `policy3` удалить условие обработки IP-пакетов при значении метки DSCP 0x80:

  ```
  hostname# inet policy rule delete policy3 1026 match dscp 0x80
  Inet policy policy3 1026 match dscp 0x80 was deleted.
  ```

inet policy rule delete

Удалить действие правила политики маршрутизации.

Синтаксис

```
inet policy rule delete <имя политики> <приоритет> {table {<номер таблицы> | name <имя таблицы> | default} | block}
```

Параметры и ключевые слова

- `<имя политики>` — имя политики маршрутизации;
- `<приоритет>` — приоритет правила в списке, возможные значения от 1025 до 2048;
- `table` — удалить таблицу маршрутизации, по которой обрабатываются IP-пакеты;
- `<номер таблицы>` — номер пользовательской таблицы маршрутизации;
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации;
- `default` — таблица маршрутизации по умолчанию;
- `block` — удалить блокировку IP-пакетов.

Режимы командного интерпретатора

Режим настройки.

Пример использования

- Чтобы в правиле приоритета 1025 политики `policy2` удалить обработку по пользовательской таблице маршрутизации `table2`:

  ```
  hostname# inet policy rule delete policy2 1025 table table2
  Inet policy policy2 1025 table table2 was deleted.
  ```

- Чтобы в правиле приоритета 1026 политики `policy3` удалить обработку по таблице маршрутизации по умолчанию:

```
hostname# inet policy rule delete policy3 1026 table default
Inet policy policy3 1026 table default was deleted.
```

inet prefix-list add

Создать префикс-лист.

Синтаксис

```
inet prefix-list add <name>
```

Параметры и ключевые слова

`<name>` — имя префикс-листа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Требования к имени префикс-листа:
  - длина: 1–64 символов;
  - использование пробелов запрещено;
  - допустимые символы: `A–Z`, `a–z`, `0–9`, `` `~!@#$%^&*()-_=+{}[]|\/:;"<>,; ``
  - имя должно быть уникальным.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet prefix-list add Test
Prefix-list Test has been added
```

inet prefix-list clear seq

Удалить правило из префикс-листа.

Синтаксис

```
inet prefix-list <name> clear seq <num>
```

Параметры и ключевые слова

- `<name>` — имя префикс-листа;
- `seq <num>` — номер правила.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet prefix-list Test clear seq 5
Seq 5 was deleted from prefix-list Test
```

inet prefix-list delete

Удалить префикс-лист.

Синтаксис

```
inet prefix-list delete <name>
```

Параметры и ключевые слова

`<name>` — имя префикс-листа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet prefix-list delete Test
Prefix-list Test was deleted
```

inet prefix-list seq

Добавить или изменить правило в префикс-листе.

Синтаксис

```
inet prefix-list <name> [seq <num>] {permit|deny} {<subnet> [le <len>][ge <len>] | any}
```

Параметры и ключевые слова

- `<name>` — имя префикс-листа;
- `seq <num>` — номер правила;
- `permit` — разрешить встраивание или передачу маршрута при совпадении префикса подсети в маршруте и правиле;
- `deny` — запретить встраивание или передачу маршрута при совпадении префикса подсети в маршруте и правиле;
- `<subnet>` — префикс подсети в формате CIDR;
- `le` — меньше или равно;
- `ge` — больше или равно;
- `<len>` — длина префикса, целое число из диапазона 0–32;
- `any` — любой префикс, равнозначно `0.0.0.0 le 32`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Номер правила: целое число из диапазона 1–4294967295.
- Правила нумерации:
  - По умолчанию правило добавляется в конец префикс-листа. Первое правило добавляется под номером 5, если не было указано иное. Далее при автонумерации шаг равен 5.
  - Если в префикс-листе есть правила, при добавлении которых был указан номер, при автонумерации номер последнего правила будет увеличен на 5.
  - Если значение номера станет больше, чем 4294967291, то добавить правило без указания номера будет невозможно.
- Без указания `le` и `ge` правило работает по точному совпадению префикса.
- Если указано только `le`, под правило попадают префиксы, длина которых меньше или равна значению `<len>` и соответствует с учетом уменьшения префикса.

- Если указано только `ge`, под правило попадают префиксы, длина которых больше или равна значению `<len>` и соответствует с учетом увеличения префикса.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet prefix-list Test permit any
  Seq 5 permit any was added to prefix-list Test
  ```
- ```
  hostname# inet prefix-list Test seq 1 deny 10.10.1.0/24 le 32 ge 28
  Seq 1 deny 10.10.1.0/24 ge 28 le 32 was added to prefix-list Test
  ```

inet prefix-list show

Просмотреть список префикс-листов или состав выбранного префикс-листа.

Синтаксис

```
inet prefix-list show [<name>]
```

Параметры и ключевые слова

`<name>` — имя префикс-листа.

Значения по умолчанию

Отображается список префикс-листов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet prefix-list show
  Prefix-lists:
  Test
  Test2
  User
  ```
  ```

- ```
  hostname# inet prefix-list show Test
  Prefix-list Test:
  seq 5 deny 10.10.1.0/24
  seq 10 permit any
  ```

inet route add

Добавить статический маршрут, в том числе в пользовательские таблицы маршрутизации.

Синтаксис

```
inet route add {<IP-адрес назначения> [netmask <маска>] | default} next-hop <IP-адрес шлюза> [table <номер таблицы> [name <имя таблицы>]] [distance <1-255> [weight <1-255>]]
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес назначения создаваемого маршрута.
- `default` — маршрут по умолчанию, по которому будут пересылаться IP-пакеты с адресом назначения в случае, если для них нет других маршрутов.
- `<IP-адрес шлюза>` — IP-адрес шлюза для доступа к IP-адресу назначения.
- `<маска>` — маска подсети.
- `<номер таблицы>` — номер пользовательской таблицы маршрутизации, в которую требуется добавить данный маршрут, может принимать значения `1024-2048`.
- `<имя таблицы>` — уникальное имя пользовательской таблицы маршрутизации, в которую требуется добавить данный маршрут. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `[distance <1-255>]` — административная дистанция.
- `[weight <1-255>]` — вес.

Значения по умолчанию

- Если маска не указана, то она принимает следующие значения:
  - 0.0.0.0 — если указано ключевое слово `default`;
  - 255.255.255.255 — в остальных случаях.
- Если административная дистанция не указана, то она принимает значение 10.
- Если вес не указан, то он принимает значение 1.

Режимы командного интерпретатора

Режим настройки.
```

Особенности использования

- Можно добавить несколько маршрутов по умолчанию.
- Если при добавлении нескольких маршрутов в одну и ту же сеть (включая и маршруты по умолчанию) не указывается их вес, то он назначается автоматически.
- Для маршрута по умолчанию не указывается маска подсети.
- Вес маршруту требуется задавать, если есть другой маршрут в ту же сеть через другой шлюз, и административная дистанция этих маршрутов совпадает.
- Нельзя задать вес равный `0`.
- Добавленный маршрут можно удалить только с помощью команды `inet route delete`.

Пример использования

- Чтобы добавить маршрут с адресом назначения 10.10.0.0, адресом шлюза 172.16.5.1, маской 255.255.0.0 и дистанцией 15:

  ```
  hostname# inet route add 10.10.0.0 netmask 255.255.0.0 next-hop 172.16.5.1 distance 15
  ```

- Чтобы добавить маршрут по умолчанию, для которого IP-пакеты будут передаваться на шлюз 172.16.5.2:

  ```
  hostname# inet route add default next-hop 172.16.5.2
  ```

- Чтобы добавить маршрут с адресом назначения 172.16.0.0, адресом шлюза 10.0.0.1, маской 255.255.0.0 и пользовательской таблицей маршрутизации `table1`:

  ```
  hostname# inet route add 172.16.0.0 netmask 255.255.0.0 next-hop 10.0.0.1 table 1234 name table1
  ```

- Чтобы добавить несколько маршрутов в одну сеть с разными шлюзами и настроить на них балансировку IP-трафика: в среднем по 50% от всего объема передаваемого IP-трафика на каждый маршрут:

  ```
  hostname# inet route add 10.0.5.0 netmask 255.255.255.0 next-hop 10.0.1.1 distance 20 weight 1
  ```

  ```
  hostname# inet route add 10.0.5.0 netmask 255.255.255.0 next-hop 10.0.4.3 distance 20 weight 1
  ```

  В результате последние два маршрута будут просуммированы — объединены в один маршрут с двумя шлюзами.

inet route clear

Удалить все маршруты, в том числе маршрут по умолчанию.

Синтаксис

```
inet route clear [table {<номер таблицы> | name <имя таблицы>}]
```

Параметры и ключевые слова

- `<номер таблицы>` — номер пользовательской таблицы маршрутизации (если используется несколько таблиц маршрутизации для одного статического маршрута).
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации (если используется несколько таблиц маршрутизации для одного статического маршрута). Максимальная длина 63 символа.

Значения по умолчанию

Команда без параметров удаляет все маршруты в таблице маршрутизации по умолчанию.

Режимы командного интерпретатора

Режим настройки.

Пример использования

- Чтобы удалить все маршруты:

```
hostname# inet route clear
Delete all the static routes? [Yes/No]: y
The static routes have been removed
```

- Чтобы удалить статические маршруты в пользовательской таблице маршрутизации с именем `table1`:

```
hostname# inet route clear table name TABLE1
Delete all the static routes? [Yes/No]: y
The static routes have been removed
```

inet route delete

Удалить маршрут.

Синтаксис

```
inet route delete {<IP-адрес назначения> [netmask <маска>] | default} [next-hop <IP-адрес шлюза>] [table {<номер таблицы> | name <имя таблицы>}]
```

Параметры и ключевые слова

- `<IP-адрес назначения>` — IP-адрес назначения.
- `<маска>` — маска подсети.
- `default` — маршрут по умолчанию.
- `<IP-адрес шлюза>` — IP-адрес шлюза.

- `<номер таблицы>` — номер пользовательской таблицы маршрутизации, из которой требуется удалить данный маршрут.
- `<имя таблицы>` — имя пользовательской таблицы маршрутизации, из которой требуется удалить данный маршрут.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если удалить единственный маршрут в таблице, не являющейся таблицей по умолчанию, то таблица тоже будет удалена.
- Если в удаляемом маршруте не указаны маска сети и IP-адрес шлюза, то выполняется поиск всех маршрутов в указанный IP-адрес назначения. Если будет найдено несколько маршрутов в указанный IP-адрес назначения, то в результате выполнения команды будет выдан список этих маршрутов. Вы можете подтвердить удаление всех маршрутов, для этого введите **y** и нажмите **Enter**. Аналогичная ситуация возникнет при удалении маршрута с несколькими шлюзами.

Пример использования

- Чтобы удалить маршрут с адресом назначения 10.0.14.0:

```
hostname# inet route delete 10.0.14.0
You are going to delete the following static routes:
Destination     Netmask          Next hop        Distance        Weight
-----------     -----------      -----------     -----------     -------
10.0.14.0       255.255.255.0    10.0.1.1        10              1
10.0.14.0       255.255.255.0    10.0.2.1        10              1
Continue? (y/n): y
Routes deleted.
```

- Чтобы удалить статический маршрут с адресом назначения 172.16.0.0 в пользовательской таблице маршрутизации `table1`:

```
hostname# inet route delete 172.16.0.0 netmask 255.255.255.0 next-hop 10.0.1.12 table
name table1
```

inet route-map add

Создать карту маршрутов.

Синтаксис

```
inet route-map add <name>
```

Параметры и ключевые слова

`<name>` — имя карты маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Требования к имени карты маршрутов:
  - имя должно быть уникальным;
  - длина: 1–64 символов;
  - допустимые символы: `A–Z`, `a–z`, `0–9`, `` `~!@#$%^&*()-_=+{}[]|\/:;"<>,; ``
  - использование пробелов запрещено.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet route-map add Test
Route map Test has been added
```

inet route-map clear

Удалить блок из карты маршрутов.

Синтаксис

```
inet route-map <name> clear <seq>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet prefix-list Test clear 5

Seq 5 was deleted
```

inet route-map delete

Удалить карту маршрутов.

Синтаксис

```
inet route-map delete <name>
```

Параметры и ключевые слова

`<name>` — имя карты маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# inet route-map delete Test

Route map was deleted
```

inet route-map match as-path

Добавить или заменить в блоке карты маршрутов проверку совпадения с AS-path-фильтром.

Синтаксис

```
inet route-map <name> <seq> match as-path <as-path-filter-name>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<as-path-filter-name>` — имя AS-path-фильтра.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если блок с номером `<seq>` уже содержит проверку, выполняется замена AS-path-фильтра.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet route-map Test permit 2
  Sequence 2 was added
  ```
- ```
  hostname# inet route-map Test deny 2
  Sequence 2 action was changed
  ```

inet route-map match community

Добавить или заменить в блоке карты маршрутов проверку совпадения с комьюнити-листом.

Синтаксис

```
inet route-map <name> <seq> match community <community-list-name> [exact-match]
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<community-list-name>` — имя комьюнити-листа;
- `[exact-match]` — точное совпадение комьюнити в маршруте и комьюнити-листе.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если блок с номером `<seq>` уже содержит проверку, выполняется замена комьюнити-листа.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet route-map Test 5 match community CL1
  Match community was added
  ```
  ```

- `hostname# inet route-map Test 5 match community CL2`
  `Match community was changed`

inet route-map match prefix-list

Добавить или заменить в блоке карты маршрутов проверку совпадения с префикс-листом.

Синтаксис

```
inet route-map <name> <seq> match prefix-list <prefix-list-name>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<prefix-list-name>` — имя префикс-листа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если блок с номером `<seq>` уже содержит проверку, выполняется замена префикс-листа.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- `hostname# inet route-map Test permit 2`
  `Sequence 2 was added`
- `hostname# inet route-map Test deny 2`
  `Sequence 2 action was changed`

inet route-map on-match

Добавить или заменить в блоке карты маршрутов директиву перехода в другой блок при совпадении условий.

Синтаксис

```
inet route-map <name> <seq> on-match {next|goto <number>}
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `next` — перейти в следующий блок;
- `<number>` — перейти в блок с указанным номером.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если блок с номером `<seq>` уже содержит директиву перехода, выполняется ее замена.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet route-map Test 2 on-match next
  On-match was added
  ```
- ```
  hostname# inet route-map Test 2 on-match goto 3
  On-match was changed
  ```

inet route-map seq

Изменить действие блока в карте маршрутов.

Синтаксис

```
inet route-map <name> {permit|deny} <seq>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `permit` — пропустить маршрут, попавший под совпадение в блоке;
- `deny` — заблокировать маршрут, попавший под совпадение в блоке;
- `<seq>` — номер блока в карте маршрутов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet route-map Test permit 2
  Sequence 2 was added
  ```
- ```
  hostname# inet route-map Test deny 2
  Sequence 2 action was changed
  ```

inet route-map set as-path-prepend

Добавить или заменить в блоке карты маршрутов установку дополнения атрибута AS-path.

Синтаксис

```
inet route-map <name> <seq> set as-path-prepend <string>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<string>` — строка текста, содержащая номера автономных систем.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Требования к строке текста, содержащей номера автономных систем:
  - длина: 1–256 символов;
  - допустимые символы: `0`–`9` и пробел;
  - не может начинаться и заканчиваться пробелом;
  - номера автономных систем разделяются пробелом.
- Если в блок с номером `<seq>` ранее была добавлена установка дополнения атрибута AS-path, выполняется его замена.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- `hostname# inet route-map Test 2 set as-path-prepend 2 2 2`

  `Set AS-path prepend was added`
- `hostname# inet route-map Test 2 set as-path-prepend 2 3 4`

  `Set AS-path prepend was changed`

inet route-map set community

Добавить или заменить в блоке карты маршрутов установку комьюнити маршрута.

Синтаксис

```
inet route-map <name> <seq> set community {[additive] <community-line>| none}
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `additive` — добавить комьюнити из `<community-line>` в атрибут маршрута;
- `<community-line>` — строка комьюнити;
- `none` — удалить все комьюнити маршрута.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Без указания параметра `additive` строка комьюнити будет перезаписана в атрибуте маршрута.
- Если в блок с номером `<seq>` ранее была добавлена установка комьюнити, выполняется его замена.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- `hostname# inet route-map Test 2 set community additive 1:1 no-export`
- `Set community was added`
- `hostname# inet route-map Test 2 set community none`

  `Set community was changed`

inet route-map set local-preference

Добавить или заменить в блоке карты маршрутов установку значения атрибута local-preference.

Синтаксис

```
inet route-map <name> <seq> set local-preference <local-preference>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<local-preference>` — значение атрибута local-preference, целое число из диапазона 0–4294967295.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если в блок с номером `<seq>` ранее была добавлена установка значения атрибута local-preference, выполняется его замена.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet route-map Test 2 set local-preference 200
  Set local preference was added
  ```
- ```
  hostname# inet route-map Test 2 set local-preference 300
  Set local preference was changed
  ```

inet route-map set metric

Добавить или заменить в блоке карты маршрутов установку значения атрибута MED.

Синтаксис

```
inet route-map <name> <seq> set metric <metric>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;

- `<seq>` — номер блока в карте маршрутов;
- `<metric>` — значение атрибута MED, целое число из диапазона -4294967295–4294967295.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если в блок с номером `<seq>` ранее была добавлена установка значения атрибута MED, выполняется его замена.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet route-map Test 2 set metric 200
  Set metric was added
  ```
- ```
  hostname# inet route-map Test 2 set metric 300
  Set metric was changed
  ```

inet route-map set next-hop

Добавить или заменить в блоке карты маршрутов установку next-hop маршрута.

Синтаксис

```
inet route-map <name> <seq> set next-hop <IP-address>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<IP-address>` — IP-адрес перехода.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если в блок с номером `<seq>` ранее была добавлена установка next-hop, выполняется замена IP-адрес перехода.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- `hostname# inet route-map Test 2 set next-hop 192.168.1.1`

  `Set next-hop was added`
- `hostname# inet route-map Test 2 set next-hop 192.168.1.1`

  `Set next-hop was changed`

inet route-map set weight

Добавить или заменить в блоке карты маршрутов установку веса маршрута.

Синтаксис

```
inet route-map <name> <seq> set weight <weight>
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `<seq>` — номер блока в карте маршрутов;
- `<weight>` — вес маршрута.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если в блок с номером `<seq>` ранее была добавлена установка веса маршрута, выполняется его замена.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- `hostname# inet route-map Test 2 set weight 200`

  `Set weight was added`
- `hostname# inet route-map Test 2 set weight 300`

  `Set weight was changed`

inet route-map show

Просмотреть список карт маршрутов, а также их состав и использование.

Синтаксис

```
inet route-map show [<name> [usage]]
```

Параметры и ключевые слова

- `<name>` — имя карты маршрутов;
- `usage` — показать список объектов, в которых используется карта маршрутов с именем `<name>`.

Значения по умолчанию

Отображается список карт-маршрутов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде с параметром `<name>` отображается состав этой карты маршрутов.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

- ```
  hostname# inet route-map show
  Route map list:
  Test1
  New
  ASNCOM
  ```
- ```
  hostname# inet route-map show Test1
  permit 1
      match ip address prefix-list NEW
      match community CL1
      set community 100:200 additive
      on-match next
  permit 2
      match as-path AS
      set weight 200
  ```
- ```
  hostname# inet route-map show Test1 usage
  Route map is used for:
  192.168.1.2 (in, advertise-map)
  172.1.1.1 (out, exist-map)
  ```
  ```

```
10.10.2.1 (in, out, non-exist-map)
static redistributed routes
ospf redistributed routes
directly connected redistributed routes
```

inet show dgd configuration

Просмотреть параметры службы DGD.

Синтаксис

```
inet show dgd configuration
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В выводе команды содержатся значения заданных параметров службы DGD, а также количество заданных шлюзов и правил.

Пример использования

Чтобы просмотреть заданные параметры службы DGD:

```
hostname> inet show dgd configuration
DGD is running
DGD autostart is on
Response-time = 2
Interval-time = 10
Retries-count = 3
Syslog-level= Error (1)
Next-hop configured = 3
Rules configured = 2
```

inet show dgd next-hop

Просмотреть настройки проверки шлюзов и их текущее состояние.

Синтаксис

```
inet show dgd next-hop [<имя шлюза>]
```

Параметры и ключевые слова

`<имя шлюза>` — имя шлюза.

Значения по умолчанию

Без указания имени шлюза отображаются настройки проверки и состояние всех шлюзов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде отображаются:
  - `Next-hop(s)configured` — общее количество шлюзов;
  - для каждого шлюза:
    - `Next-hop name` — имя шлюза;
    - `Mode` — проверка шлюза: включена (`check`) или выключена (`no check`);
    - `Type` — способ проверки: запрос ICMP (`icmp`) или TCP-соединение по порту 80 (`tcp80`) или TCP-соединение по порту 443 (`tcp443`);
    - `TestIP-address` — тестовый IP-адрес узла за шлюзом;

      

      Примечание. Если для шлюза указан интерфейс, то для него возможно наличие нескольких IP-адресов, полученных по DHCP/PPP.

    - `Interface (Global state)` — интерфейс (может отсутствовать) и его состояние;
    - `Gateway IP-address` — IP-адрес шлюза;
    - для каждой проверки IP-адреса шлюза:
      - `Success / Failed rate` — количество успешных / неуспешных проверок;

        

        Примечание. Подсчет количества успешных / неуспешных проверок ведётся с момента включения проверки; значения проверок сбрасываются при изменении состояния шлюза.

      - `State` — состояние шлюза: доступен (`Up`) или недоступен (`Down`);
      - `Last statechange` — время последнего изменения состояния шлюза.
- В кластере команда доступна для выполнения на обоих узлах.

Пример использования

Чтобы просмотреть настройки проверки всех шлюзов и их текущее состояние:

```
hostname# inet show dgd next-hop

Next-hop(s)configured: 3

 Next-hop name

 Mode      Type      TestIP-address            Interface (Global state)

 Gateway IP-address  Success / Failed rate     State    Last statechange

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

 Mars

 check     icmp      12.34.154.12              eth2 (Up)

 78.54.24.16         22 / 1                    Down     Apr 26 09:50:41 2023

 118.154.124.116     160 / 1                   Up       Apr 26 09:50:38 2023

 Jupiter

 no check  tcp80     12.34.134.12

 12.34.154.12

 Moon

 check     tcp80     13.34.152.12

 13.34.152.12        16070 / 1                 Up       Oct 16 16:07:41 2023
```

inet show dgd rule

Просмотреть параметры правил службы DGD.

Синтаксис

```
inet show dgd rule [<имя правила>]
```

Параметры и ключевые слова

`<имя правила>` — уникальное текстовое имя правила. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа. При указании данного параметра команда выводит информацию только для указанного правила. Если параметр не указан, выводится информация обо всех правилах службы DGD.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В выводе команды содержатся значения заданных параметров правил службы DGD, такие как:

- имя правила;
- имя шлюза;
- режим проверки шлюза;
- действие, выполняемое при совпадении всех признаков проверки шлюза.

Пример использования

Чтобы просмотреть заданные параметры всех правил службы DGD:

```
hostname> inet show dgd rule
```

inet show dhcp client

Просмотреть настройки DHCP на сетевых интерфейсах (настройки DHCP-клиента).

Синтаксис

```
inet show dhcp client
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде выводится следующая информация:

- `Administrative distance for DHCP/PPP routes` — административная дистанция, которая задана для маршрутов, поступающих от DHCP-сервера;
- `Default metric for DHCP/PPP routes` — метрика по умолчанию;
- `Interface` — список сетевых интерфейсов со следующими параметрами:
  - `DHCP` — статус режима DHCP: включен (`yes`) или выключен (`no`);
  - `Routes` — разрешение на автоматическое получение IP-адресов;
  - `Metric` — специфичные метрики на сетевых интерфейсах, если такие заданы;
  - `DNS` — разрешение на автоматическое получение адресов DNS-серверов;
  - `NTP` — разрешение на автоматическое получение адресов NTP-серверов.

Пример использования

```
hostname> inet show dhcp client

Administrative distance for DHCP/PPP routes: 80

Default metric for DHCP/PPP routes: 60

Interface    DHCP       Routes     Metric      DNS         NTP

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

eth0         no         yes        default     yes         yes

eth1         yes        yes        50          yes         yes

...
```

inet show dhcp server

Просмотреть настройки DHCP-сервера и его текущее состояние.

Синтаксис

```
inet show dhcp server
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet show dhcp server
DHCP server is off
DHCP server is RUNNING
start   172.16.1.2
end     172.16.1.254
interface       eth0
option subnet  255.255.255.0
option router  172.16.1.1
option wins    172.16.1.1
option lease   864000
max_leases 65533
```

inet show dhcp server lease

Просмотреть список клиентов DHCP-сервера.

Синтаксис

```
inet show dhcp server lease [{last | all | full}]
```

Параметры и ключевые слова

- `last` — вывести текущий список клиентов DHCP-сервера (по умолчанию).
- `all` — вывести полный список клиентов DHCP-сервера с историей аренды IP-адресов.
- `full` — вывести полный список клиентов DHCP-сервера без форматирования вывода (см. пример ниже).

Значения по умолчанию

По умолчанию команда без параметров выводит текущий список клиентов DHCP-сервера (`last`).

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Если среди клиентов DHCP-сервера присутствуют клиенты, подключенные к разным интерфейсам VLAN, у который один MAC-адрес, то по умолчанию в выводе команды отображаются IP-адреса клиентов только одного интерфейса VLAN. Для отображения информации о клиентах всех интерфейсов VLAN выполните команду с параметром a`ll` (`inet show dhcp server lease all`).

Пример использования

- Чтобы просмотреть текущий список клиентов DHCP-сервера:

```
hostname> inet show dhcp server lease
MAC                IP              hostname         valid until
================   =============   ==============   ========================
90:27:e4:f9:9d:d7  192.168.0.182   iMac-de-mac      2024-12-12 01:37:06
d8:a2:5e:94:40:81  192.168.0.178   foo-2            2024-12-12 01:04:56
e8:9a:8f:6e:0f:60  192.168.0.127   angela           2024-12-11 23:55:32
ec:55:f9:c5:f2:55  192.168.0.179   angela           2024-12-11 23:54:56
f0:4f:7c:3f:9e:dc  192.168.0.183   kindle-1234567   2024-12-11 23:54:31
f4:ec:38:e2:f9:67  192.168.0.185   -NA-             2024-12-11 23:55:40
f8:d1:11:b7:5a:62  192.168.0.184   -NA-             2024-12-11 23:57:34
```

- Чтобы просмотреть полный список клиентов DHCP-сервера без форматирования вывода:

```
hostname> inet show dhcp server lease full
lease 192.168.42.1 {
starts 0 2024/01/30 08:02:54;
ends 5 2024/02/04 08:02:54;
hardware ethernet
```

```
    00:50:04:53:D5:57;
    uid 01:00:50:04:53:D5:57;
    client-hostname "PC0097";
    }
    ...
```

inet show dhcp relay

Просмотреть настройки службы DHCP-relay и ее текущее состояние.

Синтаксис

```
inet show dhcp relay [<номер копии>]
```

Параметры и ключевые слова

`<номер копии>` — копия процесса DHCP-relay. Возможные значения от 1 до 32.

Значения по умолчанию

Если номер копии процесса DHCP-relay не задан, то используется номер 1.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

Чтобы просмотреть настройки 2-ой копии службы DHCP-relay:

```
hostname> inet show dhcp relay 2
DHCP relay 2 started
External DHCP server X.X.X.X
External DHCP server interface eth2
Backup DHCP server Y.Y.Y.Y
Backup DHCP server interface eth2
Internal listen interfaces eth3.1 eth3.2
```

inet show dns

Просмотреть информацию о состоянии DNS-сервера.

Синтаксис

```
inet show dns
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются:

- Автоматический запуск DNS-сервера: `on`/`off`.
- Состояние DNS-сервера: `RUNNING`/`STOPPED`.
- Ведение журнала DNS-запросов: `on`/`off`.
- Размер журнала DNS-запросов (Мбайт).

Пример использования

```
hostname# inet show dns
DNS server autostart is on
DNS server is RUNNING
DNS requests logging is on
DNS requests log size: 100 MB
```

inet show interface

Просмотреть параметры и состояние сетевого интерфейса.

Синтаксис

```
inet show interface [<имя интерфейса> | <имя интерфейса>:<номер>]
```

Параметры и ключевые слова

- `<имя интерфейса>` — имя физического интерфейса.
- `<имя интерфейса>:<номер>` — имя виртуального интерфейса, если основной интерфейс имеет дополнительный IP-адрес (alias).

Значения по умолчанию

Если интерфейс не указан, выводится информация обо всех интерфейсах, включая дополнительные IP-адреса интерфейсов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- При вводе интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Если в качестве параметра вы указали имя виртуального интерфейса, будет выведена краткая информация по основному интерфейсу.
- По команде выводится следующая информация:
  - MAC-адрес физического интерфейса.
  - IP-адрес.
  - Маска подсети.
  - Настройки получения информации от DHCP-сервера и заданная метрика для маршрутов DHCP-сервера, если на интерфейсе включен соответствующий режим.
  - Класс интерфейса (см. inet ifconfig class). В зависимости от класса выводится информация:
    - Для класса `trunk` — список существующих дочерних виртуальных интерфейсов.
    - Для класса `access` — информация о родительском интерфейсе данного виртуального интерфейса.
    - Для класса `slave` — информация о том, какому агрегированному интерфейсу подчинен данный интерфейс либо информация о том, что интерфейс пока не подчинен ни одному из агрегированных интерфейсов.
  - Состояние интерфейса (включен или выключен).
  - Для всех сетевых интерфейсов выводится максимальная возможная скорость 10 Гбит/с. Реальная скорость передачи данных через интерфейс зависит от характеристик аппаратного обеспечения, назначенного для виртуальной машины.
- Если в качестве параметра вы указали имя агрегированного интерфейса, дополнительно будет выведена информация:
  - режим работы агрегированного канала;
  - частота проверки соединения для подчиненных интерфейсов в миллисекундах;
  - в режиме `802.3ad` — режим выбора активного агрегатора и частоту обмена пакетами LACP;
  - в режиме `802.3ad` и `balance-xor` — алгоритм хэширования пакетов;
  - в режимах `active-backup`, `balance-tlb` — основной подчиненный интерфейс;
  - список подчиненных физических интерфейсов.

Текущее состояние сетевого интерфейса можно определить по сочетанию выводимых параметров и флагов:

Таблица 4. Состояния сетевого интерфейса

Состояние сетевого интерфейса	Выводимые параметры и флаги
Интерфейс включен и функционирует	Флаги: `<UP RUNNING>` — присутствуют Параметры: • `Link detected: yes` • `Speed: определено` • `Duplex: определено`
Интерфейс выключен программно	Флаги: `<UP RUNNING>` — отсутствуют Параметры: • `Link detected: no` • `Speed: определено` • `Duplex: определено`
Отключен сетевой кабель	Флаги: `<UP>` — присутствует `<RUNNING>` — отсутствует Параметры: • `Link detected: no` • `Speed: не определено (Unknown)` • `Duplex: не определено (Unknown)`

Пример использования

Просмотреть информацию об интерфейсе `eth0`:

```
hostname> inet show interface eth0

eth0      Link encap:Ethernet  HWaddr 00:15:17:e4:6c:5a
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:70
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

          Configured by DHCP: yes
          Information requested from DHCP server: IP address, routes, DNS servers,
          NTP servers
          DHCP route metric: default (70)
          Class: access
```

```
Speed: 1000Mb/s
Duplex: Full
Auto-negotiation: off
Link detected: yes
```

inet show interface state

Просмотреть статус сетевого интерфейса.

Синтаксис

```
inet show interface state [<интерфейс>]
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса.

Значения по умолчанию

Без указания имени интерфейса отображается статус подключения всех интерфейсов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображается статус подключения интерфейса:

- имя интерфейса;
- тип интерфейса относительно защищаемой сети:
  - `internal` — внутренний;
  - `external` — внешний.
- передача IP-трафика через интерфейс:
  - `enabled` — разрешена;
  - `disabled` — запрещена.

Пример использования

```
hostname# inet show interface state


Interface   Type         State
```

```
-------------------------------------
eth0        internal     enabled
eth0.1      internal     enabled
eth0.2      internal     enabled
eth1        external     enabled
eth2        external     disabled
```

inet show mac-address-table

Просмотреть ARP-таблицу (таблицу, содержащую записи о преобразованиях IP-адресов в MAC-адреса).

Примечание. Если узел недоступен, время жизни записей в ARP-таблице от 5 до 10 минут.

Синтаксис

```
inet show mac-address-table [{interface <интерфейс> | address <IP-адрес> | hwaddress <MAC-адрес> | vlan <интерфейс VLAN>}]
```

Параметры и ключевые слова

- `<интерфейс>` — фильтрация по имени сетевого интерфейса ViPNet Coordinator HW (физического или виртуального):
  - Если вы укажете физический сетевой интерфейс (например, `eth0`), для которого настроены виртуальные сетевые интерфейсы, то в выводе команды будут содержаться записи как для физического сетевого интерфейса, так и для всех виртуальных сетевых интерфейсов, настроенных на нем.
  - Если вы укажете виртуальный сетевой интерфейс (например, `eth0.1`), то в выводе команды будут содержаться записи только для указанного виртуального сетевого интерфейса
- `<IP-адрес>` — фильтрация по IP-адресу в формате X.X.X.X. В случае указания части IP-адреса будут выведены все записи, содержащие в подстроке указанную часть (октеты) IP-адреса.
- `<MAC-адрес>` — фильтрация по MAC-адресу в формате XX:XX:XX:XX:XX:XX. В случае указания только части MAC-адреса будут выведены все записи, содержащие в подстроке указанную часть MAC-адреса.
- `<интерфейс VLAN>` — фильтрация по номеру сетевого интерфейса VLAN ViPNet Coordinator HW (например, `vlan 1`).

Значения по умолчанию

Если параметр не указан, выводится вся ARP-таблица.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

- Просмотреть всю ARP-таблицу:

```
hostname> inet show mac-address-table
Address            HWtype     HWaddress           Flags Mask     Iface
---------------    ---------  ------------------  ------------   -------
172.16.5.1         ether      4c:02:89:0c:53:a2     C              eth3
172.23.221.11      ether      00:0c:29:09:1a:98     C              eth0
172.23.221.99      ether      54:04:a6:d0:f7:1a     C              eth0
172.16.5.3         ether      4c:02:89:08:ef:24     C              eth3
Found: 4
```

- Просмотреть ARP-таблицу с фильтрацией по сетевому интерфейсу `eth0`:

```
hostname> inet show mac-address-table interface eth0
Address            HWtype     HWaddress           Flags          Iface
---------------    ---------  ------------------  ------------   -------
81.30.192.131      ether      1c:74:0d:10:16:3d     C              eth0.1
81.30.192.132      ether      b4:b5:2f:89:bb:0d     C              eth0.1
81.30.192.129      ether      00:1f:ca:b3:6c:c0     C              eth0.2
81.30.192.133      ether      64:d1:54:14:c5:53     C              eth0.2
Found: 4
```

- Просмотреть записи ARP-таблицы, содержащие часть IP-адреса 30.192:

```
hostname> inet show mac-address-table address 30.192
Address            HWtype     HWaddress           Flags          Iface
---------------    ---------  ------------------  ------------   -------
81.30.192.131      ether      1c:74:0d:10:16:3d     C              eth0.1
86.30.192.132      ether      b4:b5:2f:89:bb:0d     C              eth0.1
218.15.30.192      ether      00:1f:ca:b3:6c:c0     C              eth0.2
81.30.192.133      ether      64:d1:54:14:c5:53     C              eth0.2
Found: 4
```

- Просмотреть записи ARP-таблицы, содержащие часть MAC-адреса `b4:b5:2f`:

```
hostname> inet show mac-address-table hwaddress b4:b5:2f
Address            HWtype     HWaddress           Flags          Iface
---------------    ---------  ------------------  ------------   -------
81.30.192.132      ether      b4:b5:2f:89:bb:0d     C              eth0.1
81.30.192.133      ether      14:c5:b4:b5:2f:53     C              eth0.2
10.0.0.1           ether      b4:b5:2f:b4:b5:2f     C              eth1.1
```

```
Found: 3
```

inet show ntp

Просмотреть настройки и состояние NTP-сервера.

Синтаксис

```
inet show ntp
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Возможны следующие состояния NTP-сервера:
  - `NTP server is INITIALIZING` — NTP-сервер в процессе запуска с проверкой доступности публичных или корпоративных NTP-серверов;
  - `NTP server is RUNNING` — NTP-сервер запущен, доступен хотя бы один NTP-сервер;
  - `NTP server is TERMINATING` — работа NTP-сервера в процессе завершения;
  - `NTP server is STOPPED` — NTP-сервер не запущен.
- Если NTP-сервер запущен, выводятся следующие параметры NTP-серверов, используемых для синхронизации:
  - `remote` — IP-адреса внешних NTP-серверов, с которыми синхронизируется время;
  - `refid` — сервер, с которым синхронизируется данный NTP-сервер;
  - `st` — уровень сервера, с которым синхронизируется данный NTP-сервер;
  - `t` — тип соединения, принимает следующие значения:
    - `u` — unicast или manycast;
    - `b` — broadcast или multicast;
    - `l` — local reference clock;
    - s — симметричный узел;
    - `A` — manycast NTP-сервер;
    - `B` — broadcast NTP-сервер;
    - `M` — multicast NTP-сервер.
  - `when` — время, соответствующее последнему ответу NTP-сервера;
  - `poll` — частота опроса;

- `reach` — восьмой бит октета, показывающий статус общения с внешним NTP-сервером;
- `delay` — время в миллисекундах между отправкой и получением ответа;
- `offset` — смещение в миллисекундах между ViPNet Coordinator HW и NTP-серверами;
- `jitter` — абсолютное значение в миллисекундах с указанием среднеквадратичного отклонения смещения относительно ViPNet Coordinator HW.

Пример использования

```
hostname> inet show ntp
NTP server autostart is off
NTP server is RUNNING
remote           refid       st   t   when   poll   reach   delay    offset   jitter
==============   ==========  ==   ==  =====  =====  =====   ======   =======  =======
10.0.2.1         10.0.2.4    5    u   36     64     1       3.893    0.708    0.000
10.0.2.1         10.0.6.100  4    u   35     64     1       0.702    25.706   0.000
194.149.67.129   .INIT.      16   u   -      64     0       0.000    0.000    0.000
```

inet show policy rule

Просмотреть правила политик маршрутизации.

Синтаксис

```
inet show policy rule {active | all | <имя политики>}
```

Параметры и ключевые слова

- `active` — правила для действующих политик маршрутизации;
- `all` — параметры всех политик маршрутизации;
- `<имя политики>` — уникальное текстовое имя политики маршрутизации. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Чтобы завершить просмотр, нажмите **Q**.
- В кластере команда выполняется на активном узле.

Пример использования

Чтобы просмотреть правила, заданные для активной политики маршрутизации:

```
hostname> inet show policy rule active

Policy default is active.

Policy rule(s) configured: 1

Rule(Policy) Name Priority

  Values

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

rule default

      table 254 (default)
```

inet show routing

Просмотреть таблицу маршрутизации по умолчанию, списки маршрутов от конкретного источника (Static, DHCP/PPP, OSPF, BGP) или пользовательскую таблицу маршрутизации.

Синтаксис

```
inet show routing [{static [table {<номер таблицы> | name <имя таблицы> | default}] | dhcp
| ospf [<фильтр>] | bgp}]
```

Параметры и ключевые слова

- `static` — просмотр статических маршрутов;
- `table` — просмотр таблицы маршрутизации:
  - `<номер таблицы>` — номер пользовательской таблицы маршрутизации;
  - `<имя таблицы>` — имя пользовательской таблицы маршрутизации;
  - `default` — таблица маршрутизации по умолчанию;
- `dhcp` — просмотр маршрутов, получаемых от DHCP/PPP-сервера;
- `ospf` — просмотр OSPF-маршрутов;
- `<фильтр>` — фильтр OSPF-маршрутов;
- `bgp` — просмотр BGP-маршрутов.

Значения по умолчанию

Если параметры не указаны, выводится список со всеми маршрутами, кроме маршрутов из пользовательских таблиц маршрутизации.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Маршруты в одну и ту же сеть, полученные от одного источника и с одинаковой метрикой (или административной дистанцией в случае статических маршрутов), отображаются в виде одного маршрута с несколькими шлюзами.
- Если маршрут по умолчанию не задан и отсутствует в таблице маршрутизации, выводится соответствующее предупреждение.
- Если указан параметр, для которого не существует маршрутов, вывод команды будет пустой.
- Параметр `<фильтр>` — строка текста; применяется только при просмотре OSPF-маршрутов:
  - Допустимые символы: `0-9`, `a-z`, `A-Z`, `/`, `.`, `:`, `[`, `]`.
  - Длина: 1–32 символа.
- Пояснения по атрибутам, которые выводятся перед списком маршрутов, приведены в документе «Настройка с помощью командного интерпретатора», в разделе «Просмотр таблицы маршрутизации».

Пример использования

- Чтобы просмотреть пользовательскую таблицу маршрутизации с номером 1234:

```
hostname> inet show routing static table 1234
Table 1234 (TABLE1)
Destination      Netmask          Next hop         Distance Weight
-----------      -------          --------         -------- ------
172.16.0.0       255.255.0.0      10.0.0.1         10       1
```

- Чтобы просмотреть список всех маршрутов, кроме маршрутов из пользовательских таблиц маршрутизации:

```
hostname> inet show routing
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup


VRF default table 254:
B>* 10.10.1.0/24 [20/0] via 192.168.1.1, enp0s3, weight 1, 00:00:03
C>* 10.10.2.0/24 is directly connected, enp0s8, 04:10:47
B   10.10.200.0/24 [200/0] via 172.16.1.2, enp0s9, weight 1, 04:10:30
```

```
S>* 10.10.200.0/24 [1/0] via 172.16.1.2, enp0s9, weight 1, 04:10:47
C>* 172.16.1.0/30 is directly connected, enp0s9, 04:10:47
C>* 192.168.1.0/30 is directly connected, enp0s3, 04:10:47
```

inet show traffic

Просмотреть статистику передачи данных по интерфейсам: текущее значение скорости и объёма трафика.

Синтаксис

```
inet show traffic [interface <интерфейс>][interval <интервал обновления>]
```

Параметры и ключевые слова

- `<интерфейс>` — интерфейс (физический, агрегированный, виртуальный).
- `<интервал обновления>` — интервал обновления статистики в секундах, целое число от 1 до 10.

Значения по умолчанию

Интервал обновления — 3 секунды.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Без указания интерфейса отображается статистика по всем физическим и агрегированным интерфейсам.
- Статистика включает:
  - имя интерфейса;
  - текущую входящую скорость интерфейс (RX speed);
  - текущую исходящую скорость интерфейс (TX speed);
  - объём входящего трафика с момента начала работы интерфейса (RX Total);
  - объём исходящего трафика с момента начала работы интерфейса (TX Total);
  - время, с которого ведется подсчет объёма трафика (время загрузки ViPNet Coordinator HW).
- Чтобы завершить выполнение команды, нажмите **Ctrl**+**C**.
- В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname> inet show traffic

Please wait for 3 sec. Gathering traffic....

Interface         RX speed           TX speed            RX Total        TX Total

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

eth0              10,24 Kbit/s       12,37 Kbit/s        456,12 KB       517,37 KB

eth1              999,99  bit/s      634,12  bit/s       12,31 KB        6,27 KB

bond0             1,00 Gbit/s        1000,00 Mbit/s      1,10 TB         1022,12 GB

eth2              512,00 Mbit/s      500,00 Mbit/s       563,20 GB       511,06 GB

eth3              512,00 Mbit/s      500,00 Mbit/s       563,20 GB       511,06 GB

Mon Feb 2 09:55:16 2024
```

inet show usb-modem

Просмотреть информацию о модеме и настройках подключения к сети текущего преператора.

Синтаксис

```
inet show usb-modem
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображается информация о модеме и настройках подключения к сети:

- Статус модема (найден или не найден).
- Имя текущего оператора.
- Состояние SIM-карты.
- ПИН SIM-карты.
- Статус подключения модема.
- Используется маршрут по умолчанию, полученный от оператора (см. inet usb-modem set route).
- Используется адрес DNS-сервера, полученный от оператора (см inet usb-modem set dns).

- Метрика маршрута по умолчанию, полученного от оператора (см. inet usb-modem set route-metric).

  Если метрика была удалена (`inet usb-modem set route-metric none`), используется метрика по умолчанию (см. inet dhcp client route-default-metric), которая отображается с префиксом `default`.

- Имя сетевого интерфейса модема.

Пример использования

```
hostname> inet show usb-modem

3G modem is found.

Cellular provider: MTS

SIM card: OK

PIN code is not set.

PIN verification: NA

3G connection is enabled

Use DHCP response information: gateway(yes) DNS(yes)

Route metric: default (70)

Connection interface: ppp0
```

inet show usb-modem chatscript

Просмотреть скрипт подключения к сети текущего оператора.

Синтаксис

```
inet show usb-modem chatscript
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet show usb-modem chatscript

ABORT "ERROR"

TIMEOUT 5

"" "ATE1"

ABORT "BUSY"
```

```
ABORT "NO ANSWER"
ABORT "NO CARRIER"
'' ATI
#'' AT&V
# Pass PIN-code (if defined)
#PIN#'OK' 'AT+CPIN?'
#PIN#'CPIN: READY-AT+CPIN="<pincode>"-OK' 'AT\d\d\d\d'
OK AT+CGDCONT=1,"IP","\U"
OK ATD\T
TIMEOUT 125
"CONNECT" "\c"
/etc/chatscripts/tele2-chat (END)
ABORT "ERROR"
TIMEOUT 5
"" "ATE1"
ABORT "BUSY"
ABORT "NO ANSWER"
ABORT "NO CARRIER"
'' ATI
#'' AT&V
# Pass PIN-code (if defined)
#PIN#'OK' 'AT+CPIN?'
#PIN#'CPIN: READY-AT+CPIN="<pincode>"-OK' 'AT\d\d\d\d'
OK AT+CGDCONT=1,"IP","\U"
OK ATD\T
TIMEOUT 125
"CONNECT" "\c"
~
...
~
(END)
```

inet show usb-modem config

Просмотреть конфигурацию текущего оператора.

Синтаксис

```
inet show usb-modem config
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet show usb-modem config
lcp-echo-failure 0
lcp-echo-interval 0
/dev/gsmmodem
connect '/usr/sbin/chat -v -T "*99***1#" -U "internet" -f /etc/chatscripts/tele2-chat'
crtscts
ipcp-accept-local
noauth
usepeerdns
defaultroute
persist
maxfail 99999
noipdefault
nodetach
user
password
/etc/ppp/peers/tele2 (END)
```

inet show usb-modem providers

Просмотреть список операторов.

Синтаксис

```
inet show usb-modem providers
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet show usb-modem providers
beeline
megafon
mts
skylink
```

inet show vlan

Просмотреть список виртуальных интерфейсов.

Синтаксис

```
inet show vlan
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Таблица со списком виртуальных интерфейсов содержит следующие столбцы:

- `Id` — номер виртуальной сети.
- `Name` — имя виртуального интерфейса.
- `IP` — IP-адрес виртуального интерфейса.
- `Parent` — имя родительского физического интерфейса.
- `Comment` — комментарий к виртуальной сети.

Пример использования

```
hostname> inet show vlan
```

```
VLAN interfaces
Id    | Name      | IP           | Parent| Comment
11    | eth2.11   | 172.16.11.2  | eth2  | VLAN11
12    | eth2.12   | 172.16.12.2  | eth2  | VLAN12
13    | eth2.13   | 172.16.13.2  | eth2  | VLAN13
14    | eth2.14   | 172.16.14.2  | eth2  | VLAN14
```

inet show wifi

Примечание. Команда доступна только на аппаратных платформах со встроенным адаптером Wi-Fi.

Просмотреть настройки адаптера Wi-Fi.

Синтаксис

```
inet show wifi
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet show wifi

WiFi service is enabled

The WiFi service role is client

ssid=TEST

wpa=2

wpa_key_mgt=WPA-PSK

wpa_passphrase=12345

wpa_pairwise=TKIP
```

inet snmp autostart

Включить или выключить автоматический запуск SNMP-агента при загрузке ViPNet Coordinator HW.

Синтаксис

```
inet snmp autostart {on | off}
```

Параметры и ключевые слова

- `on` — включить запуск SNMP-агента при загрузке ViPNet Coordinator HW.
- `off` — выключить запуск SNMP-агента при загрузке ViPNet Coordinator HW.

Значения по умолчанию

Запуск SNMP-агента при загрузке ViPNet Coordinator HW выключен (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

Чтобы включить запуск SNMP-агента при загрузке ViPNet Coordinator HW:

```
hostname# inet snmp autostart on
SNMP agent is enabled and will be activated on next reboot.
You need to start the SNMP agent server manually or reboot to start it.
```

inet snmp cluster node community

Задать community string, который используется для мониторинга узла кластера по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp cluster node <IP-адрес> community
```

Параметры и ключевые слова

`<IP-адрес>` — IP-адрес интерфейса синхронизации узла кластера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При выполнении команды требуется ввести community string.

- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.
- Команда доступна для выполнения только на активном узле кластера.

Пример использования

```
hostname# inet snmp cluster node 172.168.0.1 community

Type community for 172.168.0.1: public1

Restarting SNMP Agent

New community for 172.168.0.1: public1
```

inet snmp cluster node context

Изменить контекст, назначенный узлу кластера.

Синтаксис

```
inet snmp cluster node <IP-адрес> context <контекст>
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес интерфейса синхронизации узла кластера (без маски).
- `<контекст>` — новое значение контекста для узла кластера. Допустимая длина — от 1 до 32 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита и цифры.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда доступна для выполнения только на активном узле кластера.

Пример использования

```
hostname# inet snmp cluster node 172.168.0.1 context Node1

Restarting SNMP Agent

New context for 172.168.0.1: Node1
```

inet snmp cluster show

Просмотреть конфигурацию мониторинга кластера по протоколу SNMP.

Синтаксис

```
inet snmp cluster show [community]
```

Параметры и ключевые слова

`community` — показывать список community string для мониторинга кластера.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Режим просмотра — параметр `community` недоступен.
- По команде отображается следующая информация:
  - разрешено или запрещено чтение SNMP-параметров по протоколам SNMPv1 и SNMPv2c;
  - IP-адреса интерфейсов синхронизации узлов кластера;
  - контексты, назначенные узлам кластера;
  - community string, заданные на узлах кластера (если не задан, отображается `Not set`), если указан параметр `community`.
- Команда доступна для выполнения только в кластере.

Пример использования

```
hostname# inet snmp cluster show
RO communities for cluster nodes are OFF
IP-address      Context     Community
-----------     -------     ---------
172.168.0.1     Node1       Not set
172.168.0.2     Node2       public2
```

inet snmp cluster v2

Разрешить или запретить чтение SNMP-параметров узлов кластера по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp cluster v2 {on | off}
```

Параметры и ключевые слова

- `on` — разрешить.
- `off` — запретить.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если чтение параметров по протоколам SNMPv1 и SNMPv2c запрещено с помощью команды inet snmp v2, команда не выполняется.
- Если при включении мониторинга кластера хотя бы на одном из узлов кластера не задан community string, выводится соответствующее сообщение.
- Команда доступна для выполнения только на активном узле кластера.

Пример использования

```
hostname# inet snmp cluster v2 on
Restarting SNMP Agent
RO communities for cluster nodes is ON
```

inet snmp community add

Добавить community string (пароль) для чтения SNMP-параметров ViPNet Coordinator HW.

Синтаксис

```
inet snmp community add
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type new community string:` введите значение community string.
- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.
- Максимальное количество community string — 16.

Пример использования

Чтобы задать community string со значением `MyCommunity`:

```
hostname# inet snmp community add

Type new community string: MyCommunity

RO community MyCommunity created
```

inet snmp community change

Изменить community string для чтения SNMP-параметров ViPNet Coordinator HW.

Синтаксис

```
inet snmp community change
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- При выполнении команды требуется ввести текущий и новый community string.
- Допустимая длина community string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.

Пример использования

Чтобы изменить community string со значения `MyCommunity` на значение `MyCommunity1`:

```
hostname# inet snmp community change

Type current community string: MyCommunity
```

```
Type new community string: MyCommunity1
Restarting SNMP Agent
RO community MyCommunity changed to MyCommunity1
```

inet snmp community delete

Удалить community string, используемый для чтения SNMP-параметров ViPNet Coordinator HW.

Синтаксис

```
inet snmp community delete
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type community string to delete:` введите значение community string.
- При вводе команды не поддерживается контекстная подсказка.

Пример использования

Чтобы удалить community string со значением `MyCommunity`:

```
hostname# inet snmp community delete
Type community string to delete: MyCommunity
RO community MyCommunity deleted
```

inet snmp community list

Просмотреть список community string для чтения SNMP-параметров ViPNet Coordinator HW.

Синтаксис

```
inet snmp community list
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколах SNMPv1 и SNMPv2c.

Пример использования

```
hostname# inet snmp community list

community ro = private
```

inet snmp logging

Изменить уровень важности событий SNMP-агента, которые будут записываться в системный журнал ViPNet Coordinator HW.

Синтаксис

```
inet snmp logging <уровень важности>
```

Параметры и ключевые слова

`<уровень важности>` — может принимать одно из следующих значений:

- `off` — запись событий в журнал выключена.
- `critical` — в журнал записываются критические ошибки, после которых SNMP-агент не может продолжить работу.
- `error` — в журнал записываются ошибки, после которых SNMP-агент может продолжать работу.
- `info` — в журнал записывается полная информация о работе SNMP-агента.
- `debug` — в журнал записывается служебная информация, используемая при отладке.

Каждый последующий уровень включает в себя предыдущие.

Значения по умолчанию

В системный журнал записываются критические ошибки и ошибки, после которых SNMP-агент может продолжать работу (`error`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

- Чтобы выключить регистрацию событий SNMP-агента в системном журнале ViPNet Coordinator HW:

  ```
  hostname# inet snmp logging off
  SNMP Agent logging is off
  ```

- Чтобы протоколировать полную информацию о работе SNMP-агента:

  ```
  hostname# inet snmp logging info
  New SNMP Agent syslog level is info
  ```

inet snmp port

Задать UDP-порт, на котором SNMP-агент будет принимать запросы.

Синтаксис

```
inet snmp port <порт>
```

Параметры и ключевые слова

`<порт>` — номер UDP-порта.

Значения по умолчанию

По умолчанию SNMP-агент использует UDP-порт 161.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- Если UDP-порт используется другой службой ViPNet Coordinator HW — выводится сообщение `UDP port already in use. Please choose another port.`

Пример использования

Чтобы SNMP-агент принимал запросы на UDP-порт 5252:

```
hostname# inet snmp port 5252
SNMP agent port set to 5252 UDP
```

inet snmp reset-engineid

Сгенерировать новый идентификатор `engineID` SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp reset-engineid
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Команду рекомендуется использовать для устранения проблем, связанных с получением сообщений от SNMP-агентов ViPNet Coordinator HW по протоколу SNMPv3, одной из причин которых может быть одинаковый `engineID` у SNMP-агентов. Не следует генерировать новый идентификатор `engineID` при нормальной работе системы мониторинга SNMP-агентов.
- В кластере команда генерирует новый `engineID` только на том узле, на котором она вызвана.

Пример использования

Чтобы сгенерировать новый идентификатор `engineID`:

```
hostname# inet snmp reset-engineid
Reset successful
New EngineID = 0x80002A3C800D992556F6C6745E00000000
```

inet snmp show

Просмотреть информацию о текущем состоянии и настройках SNMP-агента.

Синтаксис

```
inet snmp show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname> inet snmp show

Net-SNMP agent is RUNNING.

ViPNet SNMP plugin is RUNNING.

SNMP agent autostart is ON.

Reading OIDs via SNMPv1 and SNMPv2c is OFF and sending traps is OFF

Reading OIDs via SNMPv3 is ON and sending traps is ON

Device info:

      Name = MyCoordinator

      Location = Branch_Office

      Contact = admin@infotecs.ru

      engineID = 0x80002A3C800D992556F6C6745E00000000


Current syslog level is error

SNMP agent use UDP port 161.
```

По команде выводится следующая информация:

- Статус SNMP-агента — запущен (`RUNNING`) или остановлен (`STOPPED`).
- Статус плагина ViPNet SNMP — запущен (`RUNNING`) или остановлен (`STOPPED`).
- Статус запуска SNMP-агента при перезагрузке ViPNet Coordinator HW — запуск включен (`ON`) или выключен (`OFF`).
- Статус работы по протоколам SNMPv1 и SNMPv2c и статус отправки SNMP-оповещений по протоколам SNMPv1 и SNMPv2c — разрешена (`ON`) или запрещена (`OFF`).
- Статус работы по протоколу SNMPv3 и статус отправки SNMP-оповещений по протоколу SNMPv3 — разрешена (`ON`) или запрещена (`OFF`).
- Информация о ViPNet Coordinator HW, доступная по SNMP: имя устройства, месторасположение, контактная информация, идентификатор устройства. Если имя устройства, месторасположение или контактная информация не заданы — выводится сообщение `Not set`.
- UDP-порт, используемый SNMP-агентом.

inet snmp start

Запустить встроенный SNMP-агент ViPNet Coordinator HW.

Синтаксис

```
inet snmp start
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname# inet snmp start
Starting SNMP agent... done.
```

inet snmp stop

Завершить работу встроенного SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp stop
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

Пример использования

```
hostname# inet snmp stop
Stopping SNMP agent... done.
```

inet snmp system contact

Задать параметр `mib-2.system.sysContact` («Контактное лицо») SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp system contact
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- На запрос `Type new syscontact:` введите значение параметра mib-2.system.sysContact.
- Допустимая длина строки параметра `mib-2.system.sysContact` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysContact` SNMP-агента ViPNet Coordinator HW сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.4.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysContact`).
- В кластере команда выполняется на активном узле.

Пример использования

Чтобы задать параметр `mib-2.system.sysContact`:

```
hostname# inet snmp system contact
Type new syscontact: admin@mycompany.ru
Syscontact set successfully. New syscontact = admin@mycompany.ru
```

inet snmp system location

Задать параметр `mib-2.system.sysLocation` («Местоположение») SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp system location
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.

- На запрос `Type new syslocation:` введите значение параметра `mib-2.system.sysLocation`.
- Допустимая длина строки параметра `mib-2.system.sysLocation` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysLocation` SNMP-агента ViPNet Coordinator HW сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.6.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysLocation`).
- В кластере команда задает параметр `mib-2.system.sysLocation` только на том узле, на котором она вызвана.

Пример использования

Чтобы задать параметр `mib-2.system.sysLocation` SNMP-агента ViPNet Coordinator HW:

```
hostname# inet snmp system location
Type new syslocation: Branch_Office
Syslocation set successfully. New syslocation = Branch_Office
```

inet snmp system name

Задать параметр `mib-2.system.sysName` («Имя устройства») SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp system name
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1, SNMPv2c и SNMPv3.
- На запрос `Type new sysname:` введите значение параметра `mib-2.system.sysName`.
- Допустимая длина строки параметра `mib-2.system.sysName` — от 1 до 256 символов. Разрешенные символы в строке — прописные и строчные буквы латинского алфавита, цифры, символ пробела и специальные символы: `. * / - : _ ? = @ , & < >`.
- Значение параметра `mib-2.system.sysName` SNMP-агента ViPNet Coordinator HW сохраняется в объекте MIB с идентификатором 1.3.6.1.2.1.1.5.0 (`iso.identified-organization.dod.internet.mgmt.mib-2.system.sysName`).
- В кластере команда задает параметр `mib-2.system.sysName` только на том узле, на котором она вызвана.

Пример использования

Чтобы задать параметр `mib-2.system.sysName` SNMP-агента ViPNet Coordinator HW:

```
hostname# inet snmp system name
Type new sysname: MyCoordinator
Sysname set successfully. New sysname = MyCoordinator
```

inet snmp trapsink add

Добавить адрес сетевого узла, на который SNMP-агент ViPNet Coordinator HW будет отправлять оповещения.

Синтаксис

```
inet snmp trapsink add <адрес> [port <номер>] [{v1 | inform}]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта, на который отправлять оповещения.
- `v1` — отправлять оповещения типа TRAP по протоколу SNMPv1.
- `inform` — отправлять оповещения типа INFORM по протоколу SNMPv2c.

Значения по умолчанию

- Если порт не задан, используется порт UDP 162.
- Если тип оповещений не задан, используется тип TRAP по протоколу SNMPv2c.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- На запрос `Type community string for sending traps:` введите community string, заданный на сетевом узле, получающем SNMP-оповещения (community-trap string).
- Максимальное количество сетевых узлов для SNMP-агента ViPNet Coordinator HW — 16.
- Допустимая длина community-trap string — от 6 до 18 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `. * / - : _ ? = @ , &`.
- При указании параметра `v1` отправка оповещений INFORM невозможна.

- Если вы хотите задать порт, отличный от UDP 162, перед выполнением команды добавьте сетевой фильтр, разрешающий передачу SNMP-оповещений на данный порт (firewall add).

Пример использования

Чтобы SNMP-агент ViPNet Coordinator HW отправлял оповещения INFORM на UDP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp trapsink add 10.0.0.1 port 162 inform

Type community string for sending traps: trapcommunity1

Inform -> 10.0.0.1:162 UDP Community = trapcommunity1 added
```

inet snmp trapsink delete

Удалить адрес сетевого узла, на который SNMP-агент ViPNet Coordinator HW отправляет оповещения.

Синтаксис

```
inet snmp trapsink delete <адрес> [port <номер>]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- Если на SNMP-агенте ViPNet Coordinator HW заданы сетевые узлы с одинаковым IP-адресом и портом, но с разными community-trap string — удаляются все такие сетевые узлы.

Пример использования

Чтобы удалить сетевой узел с IP-адресом 10.0.0.1, принимающий SNMP-оповещения на UDP-порт 162:

```
hostname# inet snmp trapsink delete 10.0.0.1 port 162

Trap -> 10.0.0.1:162 UDP Community = trapcommunity1 deleted
```

inet snmp trapsink list

Просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения.

Синтаксис

```
inet snmp trapsink list [secure]
```

Параметры и ключевые слова

`secure` — отображать community-trap string.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Режим просмотра — параметр `secure` недоступен.
- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.

Пример использования

- Чтобы просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения:

```
hostname> inet snmp trapsink list
Trap {v1|v2c} -> 101.101.101.211:162 UDP

Trap {v1|v2c} -> my-domain.org:162 UDP

Inform -> 10.10.10.3:162 UDP
```

- Чтобы просмотреть список сетевых узлов, на которые SNMP-агент отправляет оповещения, включая community-trap string:

```
hostname# inet snmp trapsink list secure
Trap {v1|v2c} -> 101.101.101.211:162 UDP
Community = trapcommunity2

Trap {v1|v2c} -> my-domain.org:162 UDP
Community = trapcommunity3

Inform -> 10.10.10.3:162 UDP
Community = trapcommunity2
```

inet snmp user add

Добавить пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user add <имя пользователя> [{md5 | sha}]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `md5` или `sha` — алгоритм хэширования пароля пользователя.

Значения по умолчанию

Алгоритм хэширования пароля пользователя — MD5.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Допустимая длина имени пользователя — от 1 до 32 символов. Разрешенные символы имени пользователя — прописные и строчные буквы латинского алфавита и цифры.
- При выполнении команды требуется дважды ввести пароль пользователя. При вводе паролей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина пароля — от 8 до 32 символов. Разрешенные символы пароля — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () – _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- Максимальное количество пользователей на SNMP-агенте ViPNet Coordinator HW — 32.
- Пользователь создается с правом на чтение SNMP-параметров.

Пример использования

Чтобы добавить нового пользователя `user1` и задать алгоритм хэширования пароля `sha`:

```
hostname# inet snmp user add user1 sha
Type the new user1 password:
Confirm the new user1 password:
User1 created
```

inet snmp user delete

Удалить пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user delete <имя пользователя>
```

Параметры и ключевые слова

`<имя пользователя>` — имя пользователя SNMP.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы удалить пользователя `user1`:

```
hostname# inet snmp user delete user1
user1 deleted
```

inet snmp user list

Просмотреть список пользователей SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

```
hostname> inet snmp user list

user1:

    hash=MD5 encryption=OFF

    read = ON

    trapsess = OFF

user2:

    hash=SHA encryption=off

    read = OFF

    trapsess = ON

    Trap -> 101.101.101.211:162 UDP

user3:

    hash=SHA encryption=AES

    read = ON view = all

    trapsess = ON

    Trap -> my-domain.org:162 UDP

    Inform -> 10.10.10.3:162 UDP

user4:

    certname=user4

    read = ON view = all
```

По команде выводится список пользователей и настройки каждого из них:

- имя пользователя;
- настройка хэширования пароля;
- настройка шифрования данных;
- право чтения SNMP-параметров;
- право отправки SNMP-оповещений;
- параметры отправки SNMP-оповещений.

Примечание. Если пользователь использует TLS, вместо информации о хэшировании и шифровании выводится имя используемого сертификата.

inet snmp user set key

Создать, изменить или удалить ключ шифрования пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user set <имя пользователя> key [off]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `off` — удалить ключ шифрования пользователя.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- При выполнении команды требуется дважды ввести ключ шифрования пользователя. При вводе ключей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина ключа шифрования — от 8 до 32 символов. Разрешенные символы ключа — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

Внимание! Не используйте повторяющиеся последовательности символов в ключе шифрования. Иначе его хэш может совпасть с хэшем другого ключа. Например, ключи AbcdAbcd и AbcdAbcdAbcd будут иметь одинаковые хэши. Подробнее см. RFC 3414.

- Для шифрования данных используется алгоритм AES-128.

Пример использования

- Чтобы создать ключ шифрования пользователя `user1`, для которого ключ не создавался или был удален:

```
hostname# inet snmp user set user1 key
Type the privacy key for user1:
Confirm the privacy key for user1:
Restarting SNMP Agent
Privacy key for User1 created
```

- Чтобы изменить ключ шифрования пользователя:

```
hostname# inet snmp user set user1 key
Type the privacy key for user1:
Confirm the privacy key for user1:
Restarting SNMP Agent
Privacy key for User1 changed
```

- Чтобы удалить ключ шифрования пользователя `user1`:

```
hostname# inet snmp user set user1 key off
Restarting SNMP Agent
Privacy key for User1 deleted
```

inet snmp user set name

Изменить имя пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user set <имя пользователя> name <новое имя пользователя>
```

Параметры и ключевые слова

- `<имя пользователя>` — текущее имя пользователя SNMP.
- `<новое имя пользователя>` — новое имя пользователя SNMP.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Допустимая длина имени пользователя — до 32 символов. Разрешенные символы имени пользователя — прописные и строчные буквы латинского алфавита и цифры.
- При успешном выполнении команды:
  - Пароль пользователя остается без изменений.
  - Если для пользователя настроено шифрование данных (см. inet snmp user set key), ключ шифрования остается без изменений.
  - Если для пользователя выполнены настройки отправки оповещений, имя пользователя в них будет изменено.

Пример использования

Чтобы изменить имя пользователя с `user1` на `user2`:

```
hostname# inet snmp user set user1 name user2

Username for user1 changed to user2
```

inet snmp user set passwd

Изменить пароль пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user set <имя пользователя> passwd [{md5 | sha}]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `md5` или `sha` — алгоритм хэширования пароля.

Значения по умолчанию

Алгоритм хэширования пароля пользователя — MD5.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- При выполнении команды требуется дважды ввести новый пароль пользователя. При вводе паролей символы не отображаются, введенные символы отредактировать нельзя.
- Допустимая длина пароля — от 8 до 32 символов. Разрешенные символы пароля — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

Внимание! Не используйте повторяющиеся последовательности символов в пароле. Иначе его хэш может совпасть с хэшем другого пароля. Например, пароли AbcdAbcd и AbcdAbcdAbcd будут иметь одинаковые хэши. Подробнее см. RFC 3414.

Пример использования

Чтобы изменить пароль пользователя `user1` и задать алгоритм хэширования пароля `sha`:

```
hostname# inet snmp user set user1 passwd sha

Type the new user1 password:

Confirm the new user1 password:
```

```
Password for user1 changed
```

inet snmp user set read

Разрешить или запретить чтение SNMP-параметров (OID) для пользователя SNMP-агента ViPNet Coordinator HW.

Синтаксис

```
inet snmp user set <имя пользователя> read {on | off}
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `on` — разрешить чтение.
- `off` — запретить чтение.

Значения по умолчанию

При добавлении пользователя (см. inet snmp user add) чтение по умолчанию разрешено.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы запретить пользователю `user1` чтение SNMP-параметров:

```
hostname# inet snmp user set user1 read off
Reading OID for user1 is off
```

inet snmp user set trapsess

Разрешить или запретить отправку SNMP-оповещений для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess {on | off}
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `on` — разрешить отправку.
- `off` — запретить отправку.

Значения по умолчанию

Отправка оповещений запрещена (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы разрешить отправку оповещений для пользователя `user1`:

```
hostname# inet snmp user set user1 trapsess on

Sending traps for user1 is on
```

inet snmp user set trapsess add

Добавить адрес сетевого узла, на который SNMP-агент ViPNet Coordinator HW будет отправлять оповещения для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess add <адрес> [port <номер>] [inform]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта, на который отправлять оповещения.
- `inform` — отправлять оповещения типа INFORM.

Значения по умолчанию

- Если порт не задан, используется порт UDP 162.

- Если лексема `inform` не указана, используется тип TRAP.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколе SNMPv3.
- Максимальное количество сетевых узлов для всех пользователей SNMP-агента ViPNet Coordinator HW — 16.
- Если вы хотите задать порт, отличный от UDP 162, перед выполнением команды добавьте сетевой фильтр, разрешающий передачу SNMP-оповещений на данный порт.

Пример использования

Чтобы SNMP-агент ViPNet Coordinator HW отправлял оповещения TRAP для пользователя `user1` на UDP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp user set user1 trapsess add 10.0.0.1
Trap -> 10.0.0.1:162 UDP for user1 added
```

inet snmp user set trapsess delete

Удалить адрес сетевого узла, на который SNMP-агент ViPNet Coordinator HW отправляет оповещения для пользователя.

Синтаксис

```
inet snmp user set <имя пользователя> trapsess delete <адрес> [port <номер>]
```

Параметры и ключевые слова

- `<имя пользователя>` — имя пользователя SNMP.
- `<адрес>` — IP-адрес или доменное имя сетевого узла.
- `<номер>` — номер UDP-порта.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы SNMP-агент ViPNet Coordinator HW перестал отправлять сообщения для пользователя `user1` на TCP-порт 162 сетевого узла с IP-адресом 10.0.0.1:

```
hostname# inet snmp user set user1 trapsess delete 10.0.0.1 port 162

Trap -> 10.0.0.1:162 UDP for user1 deleted
```

inet snmp v2

Разрешить или запретить чтение SNMP-параметров (OID) и отправку SNMP-оповещений по протоколам SNMPv1 и SNMPv2c.

Синтаксис

```
inet snmp v2 {ro | traps} {on | off}
```

Параметры и ключевые слова

- `ro` — чтение SNMP-параметров:
  - `on` — разрешить.
  - `off` — запретить.
- `traps` — отправка SNMP-оповещений:
  - `on` — разрешить.
  - `off` — запретить.

Значения по умолчанию

- Чтение SNMP-параметров запрещено (`off`).
- Отправка SNMP-оповещений запрещена (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

До выполнения команды `inet snmp v2 traps on`, которая разрешает отправку SNMP-оповещений, добавьте хотя бы один сетевой узел (см. inet snmp trapsink add).

Пример использования

- Чтобы разрешить чтение SNMP-параметров:

  ```
  hostname# inet snmp v2 ro on
  ```

```
Reading OIDs via SNMPv1 and SNMPv2c is ON
```

- Чтобы разрешить отправку SNMP-оповещений:

```
hostname# inet snmp v2 traps on
Sending traps via SNMPv1 and SNMPv2c is ON
```

inet snmp v3

Разрешить или запретить чтение SNMP-параметров (OID) и отправку SNMP-оповещений по протоколу SNMPv3.

Синтаксис

```
inet snmp v3 {ro | traps} {on | off}
```

Параметры и ключевые слова

- `ro` — чтение SNMP-параметров:
  - `on` — разрешить.
  - `off` — запретить.
- `traps` — отправка SNMP-оповещений:
  - `on` — разрешить.
  - `off` — запретить.

Значения по умолчанию

- Чтение SNMP-параметров запрещено (`off`).
- Отправка SNMP-оповещений запрещена (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

До выполнения команды `inet snmp v3 traps on`, которая разрешает отправку SNMP-оповещений, добавьте хотя бы один сетевой узел (см. inet snmp user set trapsess add).

Пример использования

- Чтобы разрешить чтение SNMP-параметров:

```
hostname# inet snmp v3 ro on
Reading OIDs via SNMPv3 is ON
```

- Чтобы разрешить отправку SNMP-оповещений:

```
hostname# inet snmp v3 traps on
Sending traps via SNMPv3 is ON
```

inet ssh

Подключиться к удаленному узлу по протоколу SSH.

Синтаксис

```
inet ssh {host <адрес> | id <идентификатор>} [user <пользователь>] [port <порт>]
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя удаленного узла.
- `<идентификатор>` — идентификатор сетевого узла ViPNet в шестнадцатеричном формате. Используется для доступа к защищенному узлу.
- `<пользователь>` — имя пользователя удаленного узла.
- `<порт>` — номер порта доступа.

Значения по умолчанию

- `<пользователь>` — `user`.
- `<порт>` — `22`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе идентификатора работают автодополнение и подсказка, данные для подсказки берутся из списка связей ViPNet Coordinator HW.
- На время установления соединения с удаленным компьютером блокируется доступ к консоли. Максимальное время ожидания — 90 секунд. По истечении этого времени удаленный компьютер считается недоступным и соединение разрывается.
- В ViPNet Coordinator HW поддерживается только кодировка KOI8-R. Поэтому при подключении к компьютеру, на котором используется другая кодировка, возможны проблемы при вводе с клавиатуры и отображении на консоли символов нелатинского алфавита.

Пример использования

Чтобы подключиться к узлу ViPNet с идентификатором `0x270e000a`:

```
hostname# inet ssh id 0x270e000a

user password:
```

inet usb-modem add provider

Добавить нового оператора в список доступных операторов.

Синтаксис

```
inet usb-modem add provider <оператор>
```

Параметры и ключевые слова

`<оператор>` — имя оператора.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet usb-modem add provider tele2

Provider 'tele2' config file (/etc/ppp/peers/tele2) and chat script
(/etc/chatscripts/tele2-chat) created.

The current cellular provider is tele2
```

inet usb-modem delete provider

Удалить оператора из списка доступных операторов.

Синтаксис

```
inet usb-modem delete provider <оператор>
```

Параметры и ключевые слова

`<оператор>` — имя оператора.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet usb-modem delete provider tele2

Provider 'tele2' config file (/etc/ppp/peers/tele2) and chat script
(/etc/chatscripts/tele2-chat) removed.

The current cellular provider is not specified.
```

inet usb-modem mode

Включить или выключить модем.

Синтаксис

```
inet usb-modem mode {on | off}
```

Параметры и ключевые слова

- `on` — включить модем;
- `off` — выключить модем.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию модем выключен (`off`).
- При выключении модема автоматически выполняется подключение к сети текущего оператора.
- После включения модема проверяется наличие и целостность SIM-карты и правильность ПИНа, что может занять некоторое время. Если сразу выполнить команду inet show usb-modem, статусы SIM-карты и ПИНа могут отображаться неверно.

Пример использования

Включить использование модема:

```
hostname# inet usb-modem mode on

3G/4G connection is enabled
```

inet usb-modem modify chatscript

Изменить скрипт подключения к сети текущего оператора.

Синтаксис

```
inet usb-modem modify chatscript
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Изменение скрипта может потребоваться, если модем имеет нестандартные команды управления, например, нестандартный способ задания ПИНа.

inet usb-modem modify config

Изменить конфигурацию текущего оператора.

Синтаксис

```
inet usb-modem modify config
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Изменение конфигурации может потребоваться, если стандартные настройки не позволяют подключиться к сети оператора.

inet usb-modem reset pin

Удалить ПИН SIM-карты текущего оператора.

Синтаксис

```
inet usb-modem reset pin
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet usb-modem reset pin
```

```
PIN code was reset
```

inet usb-modem set connection address

Задать адрес сервера доступа для подключения к сети текущего оператора.

Синтаксис

```
inet usb-modem set connection address {<IP-адрес> | <DNS-имя>}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес сервера.
- `<DNS-имя>` — доменное имя сервера.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Задать доменное имя static.beeline.ru:

```
hostname# inet usb-modem set connection address static.tele2.ru
Provider 'tele2' set connection address to static.tele2.ru
```

inet usb-modem set dns

Разрешить или запретить получение адреса DNS-сервера оператора.

Синтаксис

```
inet usb-modem set dns {on | off}
```

Параметры и ключевые слова

- `on` — разрешить получение адреса DNS-сервера;
- `off` — запретить получение адреса DNS-сервера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

По умолчанию получение адреса DNS-сервера разрешено (`on`).

Пример использования

Запретить получение адреса DNS-сервера:

```
hostname# inet usb-modem set dns off
```

```
inet usb-modem set dns off
```

inet usb-modem set password

Задать пароль пользователя, используемый при аутентификации во время подключения к сети текущего оператора.

Синтаксис

```
inet usb-modem set password <пароль>
```

Параметры и ключевые слова

`<пароль>` — пароль пользователя.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet usb-modem set password Aa123456
```

```
Provider 'tele2' set new password
```

inet usb-modem set phone

Задать номер доступа текущего оператора.

Синтаксис

```
inet usb-modem set phone <номер доступа>
```

Параметры и ключевые слова

`<номер доступа>` — номер доступа.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet usb-modem set phone *99***1#
Provider 'tele2' set phone to *99***1#
```

inet usb-modem set pin

Задать ПИН SIM-карты текущего оператора.

Синтаксис

```
inet usb-modem set pin <ПИН>
```

Параметры и ключевые слова

`<ПИН>` — ПИН.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# inet usb-modem set pin 1234
PIN code was set
```

inet usb-modem set provider

Выбрать текущего оператора из списка доступных.

Синтаксис

```
inet usb-modem set provider <оператор>
```

Параметры и ключевые слова

`<оператор>` — имя оператора.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Можно выбрать одно из предустановленных операторов: `beeline`, `megafon`, `mts`, `skylink`.
- Также можно указать другого оператора, добавленного с помощью команды inet usb-modem add provider.

Пример использования

Выбрать в качестве текущего оператора Мегафон:

```
hostname# inet usb-modem set provider megafon
Cellular provider is set to megafon
```

inet usb-modem set route

Разрешить или запретить получение маршрута по умолчанию от оператора при подключении к его сети.

Синтаксис

```
inet usb-modem set route {on | off}
```

Параметры и ключевые слова

- `on` — разрешить получение маршрута по умолчанию.
- `off` — запретить получение маршрута по умолчанию.

Значения по умолчанию

По умолчанию получение маршрута разрешено (`on`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Запретить получение получение маршрута по умолчанию:

```
hostname# inet usb-modem set route off
```

inet usb-modem set route-metric

Задать или удалить специфичную метрику маршрута по умолчанию, получаемого от оператора при подключении к его сети.

Синтаксис

```
inet usb-modem set route-metric {<1-255> | none}
```

Параметры и ключевые слова

- `<1–255>` — значение метрики.
- `none` — удалить метрику.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

После удаления метрики будет использоваться метрика по умолчанию (см. inet dhcp client route-default-metric).

Пример использования

- Задать метрику 40:

  ```
  hostname# inet usb-modem set route-metric 40
  Route metric for USB modem is set to 40
  ```

- Удалить метрику:

  ```
  hostname# inet usb-modem set route-metric none
  Route metric for USB modem is unset
  ```

inet usb-modem set user

Задать имя пользователя, используемое при аутентификации во время подключения к сети текущего оператора.

Синтаксис

```
inet usb-modem set user <имя>
```

Параметры и ключевые слова

`<имя>` — имя пользователя.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Задать имя пользователя Ivanov:

```
hostname# inet usb-modem set user Ivanov
Provider 'tele2' set username to "Ivanov"
```

inet vlan comment add

Добавить комментарий к виртуальной сети.

Синтаксис

```
inet vlan <номер> comment add <комментарий>
```

Параметры и ключевые слова

- `<номер>` — номер виртуальной сети.
- `<комментарий>` — комментарий. Комментарий, содержащий пробелы, должен быть указан в двойных кавычках.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы добавить комментарий «This is VLAN number 10» к виртуальной сети с номером 10:

```
hostname# inet vlan 10 comment add "This is VLAN number 10"
```

inet vlan comment delete

Удалить комментарий к виртуальной сети.

Синтаксис

```
inet vlan <номер> comment delete
```

Параметры и ключевые слова

`<номер>` — номер виртуальной сети.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы удалить комментарий к виртуальной сети с номером 10:

```
hostname# inet vlan 10 comment delete
```

inet wifi access-point channel

Задать номер канала Wi-Fi при работе ViPNet Coordinator HW в режиме точки доступа.

Синтаксис

```
inet wifi access-point channel <номер>
```

Параметры и ключевые слова

`<номер>` — номер канала Wi-Fi. Допустимый диапазон: 1–11.

Значения по умолчанию

По умолчанию задан канал 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.

Пример использования

Чтобы задать номер канала 10:

```
hostname# inet wifi access-point channel 10
```

inet wifi access-point hwmode

Выбрать стандарт сети Wi-Fi при работе ViPNet Coordinator HW в режиме точки доступа.

Синтаксис

```
inet wifi access-point hwmode {b | g}
```

Параметры и ключевые слова

- `b` — стандарт IEEE 802.11b.
- `g` — стандарт IEEE 802.11g.

Значения по умолчанию

Используется стандарт сети IEEE 802.11g.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.

Пример использования

Чтобы выбрать стандарт сети IEEE 802.11b:

```
hostname# inet wifi access-point hwmode b
Configured successfully.
```

inet wifi access-point show

Просмотреть список подключенных клиентов Wi-Fi к ViPNet Coordinator HW, при его работе в режиме точки доступа.

Синтаксис

```
inet wifi access-point show
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.

Пример использования

По команде выводится список подключенных клиентов Wi-Fi, для каждого клиента — MAC-адрес и уровень сигнала.

```
hostname# inet wifi access-point show

client: 38:aa:3c:bf:86:5a
  signal: -37 dBm
  signal avg: -36 dBm
```

inet wifi authentication

- Указать тип защиты сети Wi-Fi — при работе ViPNet Coordinator HW в режиме клиента Wi-Fi.
- Задать тип защиты сети Wi-Fi — при работе ViPNet Coordinator HW в режиме точки доступа Wi-Fi.

Синтаксис

```
inet wifi {client | access-point} authentication {open | wpa-psk | wpa2-psk}
```

Параметры и ключевые слова

- `client` — ViPNet Coordinator HW работает в режиме клиента Wi-Fi.
- `access-point` — ViPNet Coordinator HW работает в режиме точки доступа Wi-Fi.
- `wpa-psk` — защита с помощью WPA-PSK.
- `wpa2-psk` — защита с помощью WPA2-PSK.
- `open` — соединение не защищено.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.
- При выполнении команды с типом защиты `wpa-psk` или `wpa2-psk` по запросу введите имя сети (SSID) и пароль доступа к сети.
- При выполнении команды с типом защиты `open` по запросу введите только имя сети (SSID).

Пример использования

- Чтобы подключиться к сети Wi-Fi с именем `WLAN_1` и защитой соединений WPA2-PSK, для которой требуется аутентификация с использованием пароля `Aa12345678`:

  ```
  hostname# inet wifi client authentication wpa2-psk
  WiFi SSID: WLAN_1
  WiFi password: Aa12345678
  WiFi client has been configured successfully
  ```

- Чтобы задать параметры точки доступа Wi-Fi `WLAN_1` с защитой соединений WPA-PSK для подключения к которой клиентов Wi-Fi аутентификация не требуется:

  ```
  hostname# inet wifi access-point authentication open
  WiFi SSID: WLAN_1
  WiFi access point has been configured successfully
  ```

inet wifi mode

Включить или выключить интерфейс Wi-Fi.

Синтаксис

```
inet wifi mode {on | off}
```

Параметры и ключевые слова

- `on` — включить интерфейс.
- `off` — выключить интерфейс.

Значения по умолчанию

Сетевой интерфейс Wi-Fi выключен (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию сетевой интерфейс Wi-Fi выключен (`off`).
- Команда доступна для выполнения только на аппаратных платформах со встроенным модулем Wi-Fi.
- В кластере команда не поддерживается.

Пример использования

Чтобы включить сетевой интерфейс Wi-Fi:

```
hostname# inet wifi mode on
WiFi service has been enabled
WiFi service has been started
```

inet wifi role

Выбрать режим работы ViPNet Coordinator HW в сети Wi-Fi.

Синтаксис

```
inet wifi role {access-point | client}
```

Параметры и ключевые слова

- `access-point` — режим точки доступа Wi-Fi.
- `client` — режим клиента Wi-Fi.

Значения по умолчанию

Установлен режим клиента Wi-Fi (`client`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.
- При изменении режима сбрасываются настройки интерфейса `wlan0`.

Пример использования

Чтобы переключить ViPNet Coordinator HW в режим точки доступа Wi-Fi:

```
hostname# inet wifi role access-point
The WiFi service role has been set to access-point
```

inet wifi scan

Просмотреть доступные сети Wi-Fi.

Синтаксис

```
inet wifi scan
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.

Пример использования

```
hostname> inet wifi scan

Scanning...

bssid / frequency / signal level / flags / ssid

10:bf:48:e7:11:f8    2437  -50  [WPA2-PSK-CCMP][WPS][ESS] ASUS

00:3A:99:AA:25:30    2412  -60  [WPA2-EAP-CCMP][ESS] Infotecs
```

Команды группы iplir

Настройка параметров работы в защищенной сети ViPNet.

iplir adapter add

Добавить новый сетевой интерфейс.

Синтаксис

```
iplir adapter add <интерфейс> [traffic {on | off}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя добавляемого сетевого интерфейса.
- `traffic` — включение или выключение прохождения IP-трафика через добавляемый сетевой интерфейс (действие параметра аналогично команде iplir adapter traffic). Параметр может принимать следующие значения:
  - `on` — включить прохождение IP-трафика через добавляемый сетевой интерфейс;
  - `off` — выключить прохождение IP-трафика через добавляемый сетевой интерфейс.

Значения по умолчанию

Прохождение IP-трафика через добавляемый сетевой интерфейс выключено (`traffic off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Служба `iplircfg` должна быть запущена (iplir start).
- Добавляемый интерфейс должен быть заранее создан как VLAN (см. inet ifconfig vlan add) или агрегированный (см. inet ifconfig bonding add).

Пример использования

Добавить сетевой интерфейс `eth1.10` и не включать на нём прохождение IP-трафика:

```
hostname# iplir adapter add eth1.10
```

iplir adapter delete

Удалить сетевой интерфейс.

Синтаксис

```
iplir adapter delete <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Чтобы удалить сетевой интерфейс `eth1.10`:

```
hostname# iplir adapter delete eth1.10
```

iplir adapter traffic

Включить или выключить прохождение IP-трафика через сетевой интерфейс.

Синтаксис

```
iplir adapter traffic <интерфейс> {on | off}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `on` — включить прохождение IP-трафика через интерфейс.
- `off` — выключить прохождение IP-трафика через интерфейс.

Значения по умолчанию

- Для физических интерфейсов: включено (`on`).
- Для добавленных интерфейсов: выключено (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Служба `iplircfg` должна быть запущена (iplir start).
- После выполнения команды выводится предупреждение о необходимости проверить, соответствуют ли сетевые фильтры политике безопасности вашей организации.

Пример использования

Чтобы включить прохождение IP-трафика для интерфейса `eth2`:

```
hostname# iplir adapter traffic eth2 on

Set eth2 allowTraffic as on

Attention: Upon changing this parameter, make sure that firewall rules match your
organization's security policy.
```

iplir config

Редактировать один из файлов конфигурации: основной файл конфигурации, файл конфигурации заданного интерфейса или группы интерфейсов.

Синтаксис

```
iplir config [{<интерфейс> | <группа интерфейсов>}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя статического интерфейса, для которого требуется редактировать файл конфигурации.
- `<группа интерфейсов>` — имя группы динамических интерфейсов, для которой требуется редактировать файл конфигурации:
  - `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
  - `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если в команде не указан параметр, то будет запущен текстовый редактор с основным файлом конфигурации `iplir.conf`.

- Если в команде указан интерфейс или группа интерфейсов, то будет запущен текстовый редактор с файлом конфигурации этого интерфейса или группы интерфейсов `iplir.conf-<интерфейс или группа интерфейсов>`.
- Перед редактированием файла `iplir.conf` или файла `iplir.conf-<интерфейс или группа интерфейсов>` завершите работу службы `iplircfg`.

Пример использования

Чтобы отредактировать файл конфигурации интерфейса `eth0`:

```
hostname# iplir config eth0
```

iplir info

Просмотреть информацию о своем узле и количестве туннельных соединений, а также статистику фильтрации IP-пакетов по заданному интерфейсу или группе интерфейсов.

Синтаксис

```
iplir info [{<интерфейс> | <группа интерфейсов>}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя статического интерфейса, для которого требуется просмотреть статистику фильтрации IP-пакетов.
- `<группа интерфейсов>` — имя группы динамических интерфейсов, для которой требуется просмотреть статистику фильтрации IP-пакетов:
  - `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
  - `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Если параметр не указан, выводится информация об узле (имя узла, имя сети, версия установленного ПО, активные сетевые интерфейсы и другие параметры), количестве туннельных соединений и статистика фильтрации IP-пакетов по всем интерфейсам.
- Если указан интерфейс, выводится только статистика фильтрации IP-пакетов по этому интерфейсу.
- Если указана группа интерфейсов, выводится статистика фильтрации IP-пакетов по всем активным интерфейсам, входящим в эту группу.

- Для выполнения команды служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Чтобы просмотреть статистику по интерфейсу `eth0`:

```
hostname> iplir info eth0
Interface:              eth0

Category                                            Received            Sent

Non-encrypted packets dropped:                      0                   0
Non-encrypted bytes dropped:                        0                   0

Encrypted packets passed:                           0                   0
Encrypted packets dropped:                          0                   0
Encrypted bytes passed:                             0                   0
Encrypted bytes dropped:                            0                   0

Non-encrypted broadcast packets dropped:            2                   0
Non-encrypted broadcast bytes dropped:              271                 0

Encrypted broadcast packets passed:                 0                   2
Encrypted broadcast packets dropped:                0                   0
Encrypted broadcast bytes passed:                   0                   716
Encrypted broadcast bytes dropped:                  0                   0
```

Информация о количестве туннельных соединений выводится в следующем формате:

```
Tunnels statistics: License <лицензионное>, Current <текущее>, Peak <максимальное> –
<дата>
```

где:

- `<лицензионное>` — максимальное количество туннельных соединений, разрешенное для роли, которая назначена узлу ViPNet Coordinator HW.
- `<текущее>` — текущее количество туннельных соединений.
- `<максимальное>` — максимально зарегистрированное количество туннельных соединений с момента последнего старта драйвера сетевой защиты.
- `<дата>` — дата и время последнего старта драйвера сетевой защиты.

iplir option be-default-gateway

Включить или выключить обнаружение ViPNet Coordinator HW другими координаторами с версией ПО 5.3.0 и выше в качестве шлюза по умолчанию.

Синтаксис

```
iplir option be-default-gateway {on | off | auto}
```

Параметры и ключевые слова

- `on` — включить;
- `off` — выключить;
- `auto` — в соответствии с настройкой, заданной в ViPNet Prime.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# iplir option be-default-gateway on
```

iplir option connection-server

Задать или удалить сервер соединений.

Синтаксис

```
iplir option connection-server {<id_узла> | default}
```

Параметры и ключевые слова

- `<id_узла>` — идентификатор сервера соединений;
- `default` — удалить заданный сервер соединений.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда используется в режиме «С динамической трансляцией адресов» (см. iplir option mode).
- Сервер соединений должен быть доступен из внешней сети по публичному IP-адресу.

Пример использования

```
hostname# iplir option connection-server 0x034A234D
```

iplir option interface-timeout

Задать период опроса сетевых интерфейсов.

Синтаксис

```
iplir option interface-timeout <период>
```

Параметры и ключевые слова

`<период>` — период опроса сетевых интерфейсов в секундах; число из диапазона 1–255.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Период опроса сетевых интерфейсов по умолчанию — 30 секунд.

Пример использования

```
hostname# iplir option interface-timeout 10
```

iplir option ip-forwarding

Включить или выключить маршрутизацию транзитных IP-пакетов при запуске управляющей службы `iplircfg`.

Синтаксис

```
iplir option ip-forwarding {on | off | system}
```

Параметры и ключевые слова

- `on` — включить;
- `off` — выключить;
- `system` — не изменять текущую настройку.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Значение по умолчанию — `on`.
- Значения `off` и `system` рекомендуется использовать только при отладке.
- Если маршрутизация транзитных IP-пакетов выключена, не работают пересылка транзитных IP-пакетов и туннелирование.

Пример использования

```
hostname# iplir option ip-forwarding on
```

iplir option keepalive-timeout

Задать период отправки IP-пакетов серверу соединений для поддержания активности соединения и пропуска входящего трафика через межсетевой экран.

Синтаксис

```
iplir option keepalive-timeout <период>
```

Параметры и ключевые слова

`<период>` — период отправки IP-пакетов в секундах; число из диапазона 1–255.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Значение по умолчанию — 25.
- Значение по умолчанию обеспечивает связь с сервером соединений при работе через большинство внешних межсетевых экранов.

Пример использования

```
hostname# iplir option keepalive-timeout 20
```

iplir option maxtimediff

Задать допустимый интервал времени между отправкой и приемом IP-пакетов.

Синтаксис

```
iplir option maxtimediff <интервал>
```

Параметры и ключевые слова

`<интервал>` — интервал времени в секундах; число из диапазона 1—7200.

Значения по умолчанию

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Значение по умолчанию — 7200.
- IP-пакет блокируется, если превышен заданный интервал времени между отправкой и приемом IP-пакетов.

Пример использования

```
hostname# iplir option maxtimediff 7000
```

iplir option mode

Задать режим подключения ViPNet Coordinator HW к VPN-сети.

Синтаксис

```
iplir option mode {dynamic <id_узла> [always-use-server] | static}
```

Параметры и ключевые слова

- `dynamic` — режим с динамической трансляцией адресов:
  - `<id_узла>` — идентификатор сервера соединений;
  - `always-use-server` — перенаправлять трафик внешних узлов через сервер соединений;
- `static` — режим со статической трансляцией адресов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Порт режима со статической трансляцией адресов по умолчанию — 55777.

Пример использования

```
hostname# iplir option dynamic 0x034A234D

You may lose connection with remote management application by switching to this
connection-server.

Confirm switching [y/n]: y
```

iplir option mss-decrease

Задать количество байт, на которое будет уменьшен максимальный размер TCP-сегмента (MSS).

Синтаксис

```
iplir option mss-decrease <количество>
```

Параметры и ключевые слова

`<количество>` — количество байт; число из диапазона 0–200.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Рекомендуется уменьшать MSS, если между ViPNet Coordinator HW другими защищенными или туннелируемыми узлами успешно проходит проверка соединения (ping), но не устанавливается TCP-соединение. Причиной блокирования шифрованных IP-пакетов, передаваемых в рамках TCP-соединения, может быть фрагментация этих IP-пакетов на устройствах, стоящих на пути от отправителя к получателю.

- Чтобы избежать фрагментации, рекомендуется уменьшить размер IP-пакетов на величину от 20 до 40 байт.
- Чтобы уменьшить размер исходящих IP-пакетов узла, измените MSS на узле-получателе этих IP-пакетов.
- Для установления TCP-соединения достаточно изменить MSS на одном из взаимодействующих узлов.

Пример использования

```
hostname# iplir option mss-decrease 2
```

iplir option ping-timeout

Задать период опроса состояния ViPNet-клиентов со стороны ViPNet Coordinator HW для которых он — сервер IP-адресов.

Синтаксис

```
iplir option ping-timeout <период>
```

Параметры и ключевые слова

`<период>` — период опроса в секундах; число из диапазона 1–20000.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Период опроса по умолчанию — 300.
- Если от ViPNet-клиента, для которого ViPNet Coordinator HW — сервер IP-адресов, не было получено служебных пакетов в течение периода опроса, то такому клиенту посылается специальный пакет, на который должен прийти ответ. Если ответ не приходит, то узел клиента считается недоступным.

Пример использования

```
hostname# iplir option ping-timeout 60
```

iplir option show

Просмотреть текущие параметры работы управляющей службы `iplircfg`.

Синтаксис

```
iplir option show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются:

- `VPN connection mode` — режим подключения к VPN:
  - `dynamic` — с динамической трансляцией адресов без фиксации сервера соединений;
  - `dynamic (connection server – <ViPNet ID>)` — с динамической трансляцией адресов с фиксацией сервера соединений;
  - `static` — статический;
- `Forward all to server` — передача трафика внешних узлов через сервер соединений:
  - `on` — включена;
  - `off` — выключена;
- `Full iplir6 support` — полная поддержка iplir версии 6.1:
  - `Yes` — есть;
  - `No` — нет;
- `Addresses` — список IP-адресов доступа;
- `Syslog level` — уровень важности событий, регистрируемых в системном журнале:
  - `-1 (off)` — ведение системного журнала отключено;
  - `0 (critical)` — критические ошибки;
  - `1 (error)` — ошибки;
  - `2 (warning)` — предупреждения;
  - `3 (info)` — информационные;
  - `4 (debug)` — отладочные;
- `IP-forwarding` — маршрутизация транзитного трафика при запуске управляющей службы `iplircfg`:
  - `on` — включена;
  - `off` — выключена;
  - `system` — не изменять текущие настройки;
- `MSS decrease` — количество байт, на которое будет уменьшен максимальный размер TCP-сегмента;
- `Interface check timeout` — период опроса сетевых интерфейсов, секунды;
- `Sync time` — автоматическая синхронизация времени с сервером IP-адресов:
  - `on` — включена;
  - `off` — выключена;
- `Connection keepalive timeout` — период отправки IP-пакетов серверу соединений для поддержания активного соединения с ним и пропуска входящего трафика через межсетевой экран, секунды;
- `Tunnel local networks` — режим туннелирования IP-адресов узлов, входящих в локальную подсеть ViPNet Coordinator HW:

    - `on` — обращаться к туннелируемым узлам через ViPNet Coordinator HW;
    - `off` — обращаться к туннелируемым узлам напрямую, минуя ViPNet Coordinator HW;
- `Allow being default gateway` — обнаружение ViPNet Coordinator HW другими координаторами с версией ПО 5.3.0 и выше в качестве шлюза по умолчанию:
    - `on` — включено;
    - `off` — выключено;
    - `auto` — в соответствии с настройкой, заданной в ViPNet Prime;
- `UDP-ports count` — количество портов в диапазоне динамических портов UDP.

Пример использования

```
hostname# iplir option show

   VPN connection mode: dynamic (connection server – 0x034A234D)

   Forward all to server: off

   Addresses: <ip1>, <ipX>

   Syslog level: 2 — warning

   IP-forwarding: on

   MSS decrease: 0

   Interface check timeout: 30

   Connection keepalive timeout: 25

   Sync time: off

   Tunnel local networks: off

   Allow being default gateway: on

   UDP-ports count: 2
```

iplir option sync-time

Включить или выключить синхронизацию времени с сервером IP-адресов.

Синтаксис

```
iplir option sync-time {on | off}
```

Параметры и ключевые слова

- `on` — включить синхронизацию времени;
- `off` — выключить синхронизацию времени.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Значение по умолчанию — `off`.
- Изменять значение по умолчанию не рекомендуется.

Пример использования

```
hostname# iplir option sync-time on
```

iplir option syslog-level

Задать уровень важности событий, регистрируемых в системном журнале или отключить ведение системного журнала.

Синтаксис

```
iplir option syslog-level <уровень>
```

Параметры и ключевые слова

`<уровень>` — уровень важности событий:

- `-1 (off)` — отключить ведение системного журнала;
- `0 (critical)` — критические ошибки;
- `1 (error)` — ошибки;
- `2 (warning)` — предупреждения;
- `3 (info)` — информационные;
- `4 (debug)` — отладочные.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Регистрируются события заданного уровня важности и уровней выше. Например, если задать уровень 2, то в системном журнале будут регистрироваться события с уровнями 2, 3 и 4.
- Во всех исполнения, кроме ViPNet Coordinator HW50, уровень важности по умолчанию — 3.
- В исполнениях ViPNet Coordinator HW50 с одним дисковым накопителем:

- уровень важности по умолчанию — 1;
- при локальном протоколировании доступны уровни важности от -1 до 3.

Пример использования

```
hostname# iplir option syslog-level 2
```

iplir option udp-ports-count

Задать диапазон портов UDP.

Синтаксис

```
iplir option udp-ports-count <количество портов>
```

Параметры и ключевые слова

`<количество портов>` — количество портов в диапазоне; целое число от 1 до 255.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Начальный порт диапазона:
  - по умолчанию — 55777;
  - может быть изменен в ViPNet Prime или в файле `iplir.conf` (параметр `port` собственной секции `[id]`).
- Количество портов в диапазоне по умолчанию — 255.
- Количество портов, равное 1, задает диапазон, состоящий из одного порта.

Пример использования

Чтобы уменьшить диапазон портов UDP до одного порта:

```
hostname# iplir option udp-ports-count 1
```

iplir ping

Проверить соединение с сетевым узлом ViPNet.

Синтаксис

```
iplir ping <идентификатор>
```

Параметры и ключевые слова

`<идентификатор>` — шестнадцатеричный идентификатор сетевого узла ViPNet, соединение с которым необходимо проверить.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- При вводе идентификатора работают автодополнение и подсказка, данные для подсказки берутся из списка связей ViPNet Coordinator HW с другими узлами.
- Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Чтобы проверить связь ViPNet Coordinator HW с узлом, который имеет идентификатор `0x15ea000d`:

```
hostname> iplir ping 0x15ea000d

Check connection with 0x15ea000d...

Connection successful
```

iplir set l2overip interface

Задать рабочий интерфейс L2OverIP.

Синтаксис

```
iplir set l2overip interface <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса, к которому подключен локальный сегмент сети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- В качестве параметра можно указать физический или виртуальный сетевой интерфейс.
- При вводе имени интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка существующих интерфейсов.

Пример использования

Чтобы в качестве рабочего задать виртуальный интерфейс `eth0.2`:

```
hostname# iplir set l2overip interface eth0.2
```

iplir set l2overip local-port

Добавить параметры локального сегмента сети в настройках L2OverIP.

Синтаксис

```
iplir set l2overip local-port <порт> <IP-адрес>
```

Параметры и ключевые слова

- `<порт>` — номер порта. Допустимые значения: `1–31`.
- `<IP-адрес>` — IP-адрес внешнего интерфейса ViPNet Coordinator HW.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В качестве IP-адреса можно указать только статический адрес.

Пример использования

Чтобы добавить локальный сегмент сети с номером порта 1 и адресом 172.16.1.1:

```
hostname# iplir set l2overip local-port 1 172.16.1.1
```

iplir set l2overip mac-ttl

Задать время жизни MAC-адреса в таблице MAC-адресов виртуального коммутатора при отсутствии трафика, поступающего от этого адреса.

Синтаксис

```
iplir set l2overip mac-ttl <время>
```

Параметры и ключевые слова

`<время>` — время в секундах. Допустимые значения: `60–86400`.

Значения по умолчанию

Установлено время 300 секунд.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы задать время жизни адреса в таблице MAC-адресов виртуального коммутатора 10 минут:

```
hostname# iplir set l2overip mac-ttl 600
```

iplir set l2overip mode

Включить или выключить L2OverIP.

Синтаксис

```
iplir set l2overip mode {switch | none}
```

Параметры и ключевые слова

- `switch` — включить L2OverIP.
- `none` — выключить L2OverIP.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию L2OverIP выключен (`none`).
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Чтобы включить L2OverIP:

```
hostname# iplir set l2overip mode switch
```

iplir set l2overip remote-port

Добавить параметры удаленного сегмента сети в настройках L2OverIP.

Синтаксис

```
iplir set l2overip remote-port <порт> <IP-адрес>
```

Параметры и ключевые слова

- `<порт>` — номер порта удаленного сегмента.
- `<IP-адрес>` — актуальный IP-адрес видимости ViPNet Coordinator HW, к которому подключен удаленный сегмент сети (реальный или виртуальный адрес удаленного ViPNet Coordinator HW).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Указанный номер удаленного порта должен быть отличен от номера локального порта.
- Можно добавить не более 31 удаленного порта, так как число объединяемых сегментов сети не может быть больше 32.
- Можно указать номер порта, который уже был добавлен. В этом случае будет обновлен IP-адрес удаленного сегмента.

Пример использования

Чтобы добавить удаленный сегмент сети с номером порта 2 и адресом 172.16.2.2:

```
hostname# iplir set l2overip remote-port 2 172.16.2.2
```

iplir set l2overip remote-port delete

Удалить порт с заданным номером из настроек L2OverIP.

Синтаксис

```
iplir set l2overip remote-port <порт> delete
```

Параметры и ключевые слова

`<порт>` — номер порта, который требуется удалить.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед удалением порта выключите L2OverIP (iplir set l2overip mode).
- При выполнении команды запрашивается подтверждение.

Пример использования

Чтобы удалить порт с номером 2:

```
hostname# iplir set l2overip remote-port 2 delete
Do you want to delete remote port number 2 from L2OverIP configuration? [Yes/No]: y
```

iplir set l2overip unsolicited-frames

Задать режим обработки одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя.

Синтаксис

```
iplir set l2overip unsolicited-frames {drop | broadcast | smart-broadcast}
```

Параметры и ключевые слова

- `drop` — блокировать.
- `broadcast` — обрабатывать как многоадресные с рассылкой на несколько портов:
  - кадры, принятые от локального порта, пересылать на все удаленные порты и на порт с номером 0;
  - кадры, принятые от удаленного порта, пересылать на локальный порт и на порт с номером 0;
  - кадры, принятые от порта с номером 0, пересылать на все удаленные порты и на локальный порт.

- `smart-broadcast` — аналогично режиму `broadcast`, но без обработки кадров от порта с номером 0. В этом режиме кадры, принятые от порта с номером 0, блокируются. Рекомендуемый режим при использовании технологий агрегирования каналов.

Значения по умолчанию

Установлен режим `drop`.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы задать режим обработки `smart-broadcast`:

```
hostname# iplir set l2overip unsolicited-frames smart-broadcast
```

iplir node access-point

Добавить или удалить IP-адрес доступа к координатору.

Синтаксис

```
iplir node <id_узла> access-point {add | delete} <IP-адрес> [port <порт>] [metric
<метрика>]
```

Параметры и ключевые слова

- `<id_узла>` — идентификатор сетевого узла координатора;
- действие:
  - `add` — добавить;
  - `delete` — удалить.
- `<IP-адрес>` — IP-адрес доступа;
- `<порт>` — порт доступа; число из диапазона 1–65535;
- `<метрика>` — период отправки тестовых сообщений в миллисекундах при определении IP-адреса доступа узла; число из диапазона 0–9999.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Параметры `port` и `metric` можно указать только с действием `add`. Если значения не указаны:

- `<порт>` — 55777;
- `<метрика>` — назначается автоматически.

Пример использования

```
hostname# iplir node 0x50248525 access-point add 13.1.0.24 port 55888 metric 5
```

iplir node blockforward

Включить или выключить блокирование транзитных IP-пакетов, передаваемых через ViPNet Coordinator HW связанному с ним сетевому узлу ViPNet.

Синтаксис

```
iplir node <id_узла> blockforward {on | off}
```

Параметры и ключевые слова

- `<id_узла>` — идентификатор сетевого узла ViPNet;
- блокирование транзитных IP-пакетов:
  - `off` — выключено, транзитные IP-пакеты в направлении связанного узла пропускаются;
  - `on` — включено, транзитные IP-пакеты в направлении связанного узла блокируются с кодом 70.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

По умолчанию все транзитные IP-пакеты в направлении узла ViPNet блокируются с кодом 70.

Пример использования

```
hostname# iplir node 0x383d0002 blockforward on
```

iplir node domain-name

Добавить или удалить доменное имя узла ViPNet.

Синтаксис

```
iplir node <id_узла> {add | delete} domain-name {<имя> | all}
```

Параметры и ключевые слова

- `<id_узла>` — идентификатор сетевого узла ViPNet;
- действие:
  - `add` — добавить доменное имя;
  - `delete` — удалить доменное имя;
- `<имя>` — доменное имя;
- `all` — удалить все доменные имена сетевого узла ViPNet.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Узлу ViPNet можно добавить не более 5 доменных имен.

Пример использования

```
hostname# iplir node 0x383d0002 add domain-name hw5.vipnet
```

iplir node list

Просмотреть сведения об узлах ViPNet, связанных с ViPNet Coordinator HW.

Синтаксис

```
iplir node list [{clients | gateways}] [filter <фильтр>]
```

Параметры и ключевые слова

- `<фильтр>` — строка текста, состоящая из идентификатора узла ViPNet или сети, имени или части имени узла; может содержать до 50 символов: `A–z`, `0–9`, `.,()!№-=_@;` .
- тип связанного узла:
  - `clients` — клиенты (ViPNet Client 4, 4U for Linux, 4U for Android, Mobile 2);
  - `gateways` — шлюзы безопасности (ViPNet Coordinator HW, VA, KB, IG).

Значения по умолчанию

Отображается список всех узлов ViPNet, связанных с ViPNet Coordinator HW, и сведения о них.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Список связанных узлов ViPNet содержит:
  - `Node id` — идентификатор узла;
  - `Type` — тип узла:
    - `CL` — клиент;
    - `GW` — шлюз безопасности;
  - `Node name` — имя узла;
  - `Full iplir6 support` — полная поддержка iplir версии 6.1:
    - `Yes` — есть;
    - `No` — нет;
  - `Networks` — номера сетей ViPNet, для которых ViPNet Coordinator HW — шлюзовой координатор.
- Параметр `<фильтр>`, содержащий пробел, необходимо заключить в двойные кавычки (`""`).

Пример использования

```
hostname# iplir node list
Node id       Type    Node name                  Fil6s    Networks
------------------------------------------------------------------------
0x383d0002    CL      Control Center             Yes      -
0x383d0001    GW      main_coordinator           Yes      1, 2, 3
0x3307000e    CL      NCC                        Yes      -
0x3307000a    CL      C1                         No       -


hostname# iplir node list 3307
Node id       Type    Node name                  Fil6s    Networks
------------------------------------------------------------------------
0x3307000e    CL      NCC                        Yes      -
```

```
0x3307000a    CL      C1                          No       -
```

iplir node show

Просмотреть сведения об узле ViPNet.

Синтаксис

```
iplir node <id_узла> show
```

Параметры и ключевые слова

`<id_узла>` — идентификатор сетевого узла ViPNet.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются:

- `Node name` — имя узла;
- `Type` — тип узла:
  - `Client` — клиент (ViPNet Client 4, 4U for Linux, 4U for Android, Mobile 2);
  - `Gateway` — шлюз безопасности (ViPNet Coordinator HW, VA, KB, IG);
- `VPN connection mode` — режим режим подключения к VPN-сети, если известен:
  - `dynamic` — с динамической трансляцией адресов;
  - `static` — со статической трансляцией адресов;
- `Port for TCP-tunneling` — TCP-порт туннелирования всех соединений с узлом;
- `Full iplir6 support` — полная поддержка iplir версии 6.1:
  - `Yes` — есть;
  - `No` — нет;
- `Used cipher type` — используемый алгоритм шифрования:
  - `GOST-CFB: Cipher Feedback Mode`;
  - `AES: Advanced Encryption Standard Mode`;
  - `GOST-CTR: Counter Mode`;
  - `FIPS: Federal Information Processing Standards Mode Certified`;

    - FIPS: Federal Information Processing Standards Mode;
    - GOST 34.12-2015: Magma MGM;
    - GOST 34.12-2015: Kuznyechik CTR;
- Domain name — доменное имя узла;
- Visibility — видимость узла:
    - real — по реальным IP-адресам;
    - virtual — по виртуальным IP-адресам;
- Block forward — блокирование транзитных IP-пакетов:
    - off — транзитные пакеты в направлении узла пропускаются;
    - on — транзитные пакеты в направлении узла блокируются с кодом 70;
- Access-address table — таблица IP-адресов доступа к узлу:
    - IP-address — IP-адрес доступа к узлу;
    - Port — порт;
    - Metric — период отправки тестовых сообщений при определении IP-адреса доступа узла, миллисекунды;
    - Interface — интерфейс (IP-адрес интерфейса), через который IP-пакеты передаются на IP-адрес доступа;
    - Registration type — тип регистрации IP-адреса доступа узла:
        - mgmt-center — централизованная (адрес задан на ViPNet Prime);
        - manual — ручная (адрес задан администратором сети);
        - auto — автоматическая (адрес задан ViPNet Coordinator HW);
- Tunnel settings — настройки туннелирования:
    - Use tunnel — использование туннелей:
        - on — включено;
        - off — выключено;
    - Tunnel local networks — туннелирование локальных сетей:
        - on — включено;
        - off — выключено;
    - Tunnel visibility — видимость в туннеле:
        - real — по реальным IP-адресам;
        - virtual — по реальным IP-адресам;
- Tunnel ranges — диапазоны туннелируемых адресов и исключения.

Пример использования

```
hostname# iplir node 0x383d0002 show
  Node name: Control Center
  Type: Gateway
  Port for TCP-tunneling: 234
  Full iplir6 support: Yes
  Used cipher type: GOST 34.12-2015: Magma MGM
  Domain name: nodeX.vipnet
  Visibility: real
  Block forward: on
  Access-address table:
    IP-address        Port    Metric   Interface   Registration type
    ------------------------------------------------------------------
    176.12.13.14      333     80       eth3        auto
    222.222.222.222   34567   -        eth2.2      manual
  Tunnel settings:
    Use tunnel: on
    Tunnel local networks: off
    Tunnel visibility: virtual
    Tunnel ranges:
      176.1.1.1-176.1.1.10 to 11.1.1.1-11.1.1.10
      176.1.1.11-176.1.1.30 to 12.1.1.1-12.1.1.20
      192.1.1.100-192.1.1.130 to 12.1.1.21-12.1.1.51
      excluded 192.1.1.110-192.1.1.112
      excluded 176.1.1.15
```

iplir node show domain-names

Просмотреть список доменных имен сетевого узла ViPNet.

Синтаксис

```
iplir node <id_узла> show domain-names
```

Параметры и ключевые слова

`<id_узла>` — идентификатор сетевого узла ViPNet.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname# iplir node 0x383d0002 show domain-names
1. hw5.vipnet
2. other-domain.vipnet
```

iplir node update domain-name cache

Обновить DNS-кеш узла ViPNet.

Синтаксис

```
iplir node <id_узла> update domain-name cache
```

Параметры и ключевые слова

`<id_узла>` — идентификатор сетевого узла ViPNet.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# iplir node 0x383d0002 update domain-name cache
```

iplir set performance-mode

Выбрать профиль производительности обработки трафика сетевых соединений.

Синтаксис

```
iplir set performance-mode {single|multi}
```

Параметры и ключевые слова

- `single` — профиль высокой производительности для обработки трафика одного соединения.
- `multi` — профиль стандартного распределения ресурсов; обеспечивает быструю обработку трафика нескольких сетевых соединений.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда применима для исполнений ViPNet Coordinator HW на аппаратных платформах HW100 N1, N2, N3, Q1, Q2, HW2000 Q4, Q5, HW5000 Q1, Q2.
- По умолчанию установлен профиль стандартного распределения ресурсов.
- Выбранный профиль будет применен после перезагрузки ViPNet Coordinator HW.
- Команда устанавливает глобальную блокировку управляющих запросов; сессии всех пользователей завершаются, новые сессии не открываются.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Чтобы выбрать профиль высокой производительности для обработки трафика одного соединения:

```
hostname# iplir set performance-mode single
Are you sure you want to switch system performance in single connection mode? (Yes/No): Yes
A reboot is required to enable the function. You can reboot system now or later.
Do you want to reboot system now? (Yes/No): Yes
```

iplir show adapter

Просмотреть разрешение на прохождение IP-трафика через сетевой интерфейс.

Синтаксис

```
iplir show adapter <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Чтобы просмотреть параметры сетевого интерфейса `eth0`:

```
hostname> iplir show adapter eth0

Adapter eth0 single

Allow traffic = on

Type = internal
```

iplir show adapters

Просмотреть все активные статические и динамические сетевые интерфейсы ViPNet Coordinator HW. При просмотре для каждого интерфейса в списке указан параметр `allowtraffic`, который показывает, разрешено или заблокировано прохождения IP-трафика через интерфейс.

Синтаксис

```
iplir show adapters
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Чтобы просмотреть список активных сетевых интерфейсов:

```
hostname> iplir show adapters

Active interface    Allowtraffic

eth0                on

eth1                on

eth2                off

eth3                on
```

iplir show adapters groups

Просмотреть активные динамические сетевые интерфейсы ViPNet Coordinator HW.

Синтаксис

```
iplir show adapters groups
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> iplir show adapters groups
Interface group: Active interfaces
```

iplir show authentication-type

Просмотреть способ аутентификации пользователей.

Синтаксис

```
iplir show authentication-type
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# iplir show authentication-type
Current authentication mode: password
```

iplir show ciphertype

Просмотреть информацию о текущем режиме шифрования для сети или отдельного узла ViPNet.

Синтаксис

```
iplir show ciphertype [<nodeid>]
```

Параметры и ключевые слова

`<nodeid>` — идентификатор узла сети ViPNet в HEX-формате.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- При указании параметра `<nodeid>` выводятся параметры шифрования для указанного узла. В случае если алгоритм шифрования для узла не задан, выводятся параметры шифрования для сети.
- При вводе некорректного `<nodeid>` (некорректные символы, отсутствует в справочнике) отображается соответствующее предупреждение, после чего выводится список связанных узлов и выполнение команды прекращается.

Пример использования

```
hostname> iplir show ciphertype

Network ciphertype - GOST-CFB: Cipher Feedback Mode
```

iplir show config

Просмотреть один из файлов конфигурации: основной файл конфигурации или файл конфигурации заданного интерфейса.

Синтаксис

```
iplir show config [{<интерфейс> | <группа интерфейсов>}]
```

Параметры и ключевые слова

- `<интерфейс>` — имя статического интерфейса, файл конфигурации которого требуется просмотреть.
- `<группа интерфейсов>` — имя группы динамических интерфейсов, файл конфигурации которой требуется просмотреть:
  - `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
  - `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi.

Режимы командного интерпретатора

- Режим просмотра.

- Режим настройки.

Особенности использования

- Если параметр не указан, выводится основной файл конфигурации `iplir.conf`.
- Если указан интерфейс или группа интерфейсов, выводится файл конфигурации этого интерфейса или группы интерфейсов `iplir.conf-<интерфейс или группа интерфейсов>`.
- Чтобы завершить просмотр файла конфигурации, нажмите **Q**.

Пример использования

Чтобы просмотреть основной файл конфигурации:

```
hostname> iplir show config
[id]
id= 0x15ea000b
name= Coordinator 2
ip= 10.0.14.101
...
```

iplir show exchange-keys

Просмотреть сведения о ключах обмена.

Синтаксис

```
iplir show exchange-keys [{warning | peer <peer>}]
```

Параметры и ключевые слова

- `<warning>` — отображать сведения о ключах обмена, для которых:
  - срок действия ключа истек;
  - срок действия ключа истекает — разница в днях между датой окончания срока действия ключа и текущей датой меньше периода оповещения (см. iplir warning-threshold).
- `peer` — отображать сведения о ключах обмена со связанным узлом в сети ViPNet; `<peer>` — идентификатор связанного узла.

Значения по умолчанию

При выполнении команды без параметров отображаются сведения обо всех ключах обмена, в том числе срок действия которых истек или скоро истечет.

Режимы командного интерпретатора

- Режим просмотра.

- Режим настройки.

Особенности использования

- Отображаются следующие сведения о ключах обмена:
  - `Peer` — идентификатор связанного узла в сети ViPNet.
  - `Variant` — номер варианта ключей связанного узла.
  - `StartDate` — дата начала срока действия ключа.
  - `ExpiryDate` — дата окончания срока действия ключа.
  - `KeyID` — идентификатор ключа в ViPNet Prime.
- В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname# iplir show exchange-keys
 Peer      Variant     StartDate     ExpiryDate                  KeyID
------------------------------------------------------------------------------
231323E1     1        2020-11-08    2021-11-09 (6 days)  123-123-123-123-321
23132341     3        2020-02-05    2022-02-06 (6 days)  321-123-123-123-321
23132341     2        2020-10-06    2021-10-07 (6 days)  321-123-123-123-321
01234563     2        2020-09-30    2021-10-01 (6 days)  123-321-123-123-321
Warning starts displaying in 7 days before expiry date.
```

iplir show firewall status

Просмотреть статистику работы межсетевого экрана.

Синтаксис

```
iplir show firewall status
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде выводится следующая информация:

- `Max connections` — максимальное количество одновременно открытых соединений (транзитных, служебных и управляющих).
- `Connection ttl TCP` — таймаут разрыва TCP-соединения в секундах.
- `Connection ttl UDP` — время жизни UDP-соединения.
- `ICMP timeout` — время жизни ICMP-соединения.
- `Connection ttl IP` — время жизни соединения для протоколов, отличных от TCP, UDP, ICMP.
- `Total connections count` — текущее количество открытых, защищенных и туннелируемых соединений по всем протоколам.
- `Local connections count` — текущее количество локальных открытых соединений по всем протоколам.
- `VPN connections count` — текущее количество защищенных (зашифрованных) соединений по всем протоколам.
- `Forward connections count` — текущее количество транзитных открытых соединений по всем протоколам.
- `Tunnel connections count` — текущее количество туннелируемых соединений по всем протоколам.

Пример использования

```
hostname> iplir show firewall status
Max connections           150000
TCP SYN timeout           120
Connection ttl TCP        1800
Connection ttl UDP        300
ICMP timeout              30
Connection ttl IP         300
Total connections count   17
Local connections count   15
VPN connections count     2
Forward connections count 10
Tunnel connections count  5
```

iplir show key-info

Получить информацию о ключе защиты узла ViPNet Coordinator HW.

Синтаксис

```
iplir show key-info
```

Режимы командного интерпретатора

- Режим просмотра.

- Режим настройки.

Особенности использования

По команде на экран выводится следующая информация:

- о ключе защиты узла:
  - `Uid` — идентификатор;
  - атрибуты ключа:
    - `Software-specified key ID` — идентификатор ключа, задаваемый приложением;
    - `Key algorithm` — алгоритм шифрования;
    - `Key expiration date` — дата окончания периода действия ключа;
    - `Key effective date` — дата начала периода действия ключа;
    - `My network ID` — идентификатор собственной сети;
    - `My host ID` — идентификатор собственного узла;
    - `My host name` — имя собственного узла;
    - `My host variant` — вариант собственного узла;
    - `Message count on NSK` — порядковый номер сообщения на ключе.
- о криптодрайвере:
  - поддерживаемые системы и их статус;
  - поддерживаемые алгоритмы шифрования.

Пример использования

```
hostname# iplir show key-info

NSK information:

       Uid: 34543dfg-dfg4-fbg2-ds54-dsfg45fdgb63

                  Software-specified key ID: bc5c9cef-47c9-4b31-a51c-93548e5d092f

                Key algorithm: The Magma key algorithm

                Key expiration date: 2023-04-15

                Key effective date: 2022-01-20

                My network ID: 383d

                My host ID: 110

                My host name: IG100-2c6700b7

                My host variant: 0

                Message count on NSK: 36

Driver information:
```

```
Support system:
          ItcsCdCryptSystemGost | status: ItcsCdCryptSystemReady
          ItcsCdCryptSystemFips | status: ItcsCdCryptSystemUnavailable
Support crypto suites:
          G28147_CFB_WITH_IMIT
         G28147_CTR_WITH_IMIT_CMACKDF
         ITCS_AES256_CFB_WITH_IMIT
         G28147_CTR_WITH_IMIT (for IPLir 4.1)
         G3412_MAGMA_AEAD
         G3412_KUZNYECHIK_CTR_WITH_CMAC ( CTR + CMAC)
         AES128_GCM_CMACKDF ( IPLir 6.1)
         AES128_CTR_WITH_CMAC_CMACKDF ( CTR + CMAC for IPLir 6.1)
         AES128_CFB_WITH_CMAC_CMACKDF ( CFB + CMAC for IPLir 6.1)
```

iplir show l2overip

Просмотреть состояние или настройки L2OverIP.

Синтаксис

```
iplir show l2overip <опция>
```

Параметры и ключевые слова

`<опция>` — параметр, который может принимать одно из значений:

- `clone-fabric-stats` — просмотр статистики «фабрики клонов», которая выполняет обработку широковещательного и многоадресного трафика. Информация предназначена для тестирования и локализации ошибок.
- `config` — просмотр текущих настроек L2OverIP.
- `mac-address-table` — просмотр таблицы MAC-адресов, используемой L2OverIP.
- `mac-hash-stats` — просмотр статистики хэш-таблицы MAC-адресов, используемой L2OverIP. Информация предназначена для тестирования и локализации ошибок.
- `port-table` — просмотр таблицы портов, используемых L2OverIP.
- `status` — просмотр текущего состояния L2OverIP: `switch` — включена, `none` — выключена.
- `virtual-switch-stats` — просмотр статистики по обработке Ethernet-кадров: общее количество обработанных и заблокированных кадров, а также количество обработанных и заблокированных одноадресных кадров с неизвестным MAC-адресом получателя.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

Чтобы просмотреть текущие настройки:

```
hostname> iplir show l2overip config
mode = switch
mac_ttl = 300
device = eth0
local_port = 12, 172.16.12.123
remote_port = 13, 172.16.12.124
unsolicited-frames = drop
```

iplir show performance-mode

Просмотреть текущий профиль производительности обработки трафика сетевых соединений.

Синтаксис

```
iplir show performance-mode
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Команда применима для исполнений ViPNet Coordinator HW на аппаратных платформах HW100 N1, N2, N3, Q1, Q2, HW2000 Q4, Q5, HW5000 Q1, Q2.
- Если профиль производительности был изменен, но перезагрузка ViPNet Coordinator HW не выполнена, отображается текущий и выбранный профили.

Пример использования

```
hostname# iplir show performance-mode
Current performance mode: single connection
After system reboot performance mode will be switched to: multi connection
```

iplir show tcptunnel-info

Просмотреть настройки TCP-туннеля на ViPNet Coordinator HW.

Синтаксис

```
iplir show tcptunnel-info
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> iplir show tcptunnel-info
TCP-tunnel server is running
TCP server port: 80
Max TCP-tunnels: 100
Current TCP-tunnels: 0
```

В результате выполнения команды будет выведена следующая информация:

- включен или выключен TCP-туннель;
- номер порта для входящих TCP-соединений;
- возможное количество TCP-соединений;

Примечание. ViPNet Coordinator HW текущей версии может поддерживать не более 100 соединений через TCP-туннель.

- количество текущих TCP-соединений.

iplir start

Запустить управляющую службу `iplircfg`.

Синтаксис

```
iplir start
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# iplir start
Loading IpLir
```

iplir stop

Завершить работу управляющей службы `iplircfg`.

Синтаксис

```
iplir stop
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# iplir stop
Shutting down IpLir
```

iplir warning-threshold

Задать период оповещения о скором истечении срока действия:

- ключей обмена;
- ключа защиты узла;
- сертификата пользователя.

Синтаксис

```
iplir warning-threshold <период оповещения>
```

Параметры и ключевые слова

`<период оповещения>` — количество дней в интервале 7–365.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Период оповещения по умолчанию — 30 дней.
- В кластере команда выполняется на активном узле.

Пример использования

```
hostname# iplir warning-threshold 14
```

```
Key warnings will start displaying in 14 days before expiry date.
```

iplir tcptunnel server

Включить или выключить сервер TCP-туннелей.

Синтаксис

```
iplir tcptunnel server {on | off}
```

Параметры и ключевые слова

- `on` — включить сервер TCP туннелей;
- `off` — выключить сервер TCP туннелей.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# iplir tcptunnel server on
TCP-tunnel server is enabled
TCP-tunnel server is running
```

Команды группы machine

Выключение и перезагрузка ViPNet Coordinator HW, установка имени компьютера и системного времени, работа с системным журналом, а также регламентное тестирование ViPNet Coordinator HW.

machine backup

Включить или выключить резервное копирование индивидуальной конфигурации ViPNet Coordinator HW по расписанию.

Синтаксис

```
machine backup {on | off}
```

Параметры и ключевые слова

- `on` — включить резервное копирование;
- `off` — выключить резервное копирование.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию резервное копирование включено (`on`) и запускается в случайное время из интервала 21:00–23:00.
- Если выключить резервное копирование, то ранее созданное расписание будет удалено.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# machine backup on

Backup scheduled at 22:23.

Note: ViPNet services will be stopped for the time of export
```

machine backup export

Экспортировать индивидуальную конфигурацию ViPNet Coordinator HW на сервер ViPNet Prime или USB-носитель вручную.

Синтаксис

```
machine backup export {server | usb}
```

Параметры и ключевые слова

- `server` — экспортировать на сервер ViPNet Prime.
- `usb` — экспортировать на USB-носитель.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Шаблон имени файла индивидуальной конфигурации `<имя узла>-<время создания файла>.ecf`; формат времени создания файла `YYYYMMDDTHHMMSSZ`, где `YYYY` — год, `MM` — месяц, `DD` — день, `HH` — час, `MM` — минуты, `SS` — секунды.
- Файл индивидуальной конфигурации зашифровывается на ключе обмена.
- Выполнение команды не зависит от настройки резервного копирования индивидуальной конфигурации по расписанию (см. machine backup).
- Команда устанавливает глобальную блокировку управляющих запросов; текущие сессии пользователей сохраняются, новые сессии не открываются.
- В кластере команда выполняется на активном узле.

Пример использования

Чтобы экспортировать индивидуальную конфигурацию на сервер ViPNet Prime:

```
hostname# machine backup export server
Checking settings integrity...done
Creating settings backup...done
Uploading backup...done
```

Чтобы экспортировать индивидуальную конфигурацию на USB-носитель:

```
hostname# machine backup export usb
Checking settings integrity...done
Creating settings backup...done
```

```
Insert USB drive and press Enter with at least 3.0MB free space and press Enter
Generic Flash Disk successfully mounted.
Copying hw1000-20210719T105451Z.ecf to USB drive. Press ^ + C to abort.
File successfully copied.
You may remove the USB drive.
```

machine backup schedule

Задать расписание резервного копирования индивидуальной конфигурации ViPNet Coordinator HW на сервер ViPNet Prime.

Синтаксис

```
machine backup schedule <начало интервала>[-<конец интервала>]
```

Параметры и ключевые слова

`<начало интервала>` и `<конец интервала>` — время начала и время окончания интервала времени в формате `HH:MM`, где `HH` — часы (24-часовой формат), `MM` — минуты.

Значения по умолчанию

По умолчанию используется интервал времени 21:00–23:00.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если указан интервал времени, то точное время резервного копирования выбирается из этого интервала случайным образом при создании первой резервной копии и используется далее.
- `<конец интервала>` может быть меньше, чем `<начало интервала>` — в этом случае `<конец интервала>` интерпретируется как время следующего дня.
- Чтобы задать точное время резервного копирования, укажите только `<начало интервала>`.
- В кластере команда выполняется на активном узле.

Примеры использования

Чтобы задать расписание резервного копирования с указанием временного интервала:

```
hostname# machine backup schedule 22:00-01:00
Backup scheduled at 22:23.
```

```
Note: ViPNet services will be stopped for the time of export
```

Чтобы задать расписание резервного копирования с указанием точного времени:

```
hostname# machine backup schedule 02:13

Backup scheduled at 02:13.

Use different backup time across network to balance the backup server load.

Note: ViPNet services will be stopped for the time of export
```

machine config export usb

Экспортировать универсальную конфигурацию ViPNet Coordinator HW на USB-носитель.

Синтаксис

```
machine config export usb
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Шаблон имени файла универсальной конфигурации `<имя сетевого узла>-<время создания файла>.vbe`; формат времени создания файла `YYYYMMDDTHHMMSSZ`, где `YYYY` — год, `MM` — месяц, `DD` — день, `HH` — час, `MM` — минуты, `SS` — секунды.
- В процессе выполнения команды вы можете задать текстовое описание конфигурации. Допустимая длина поля описания конфигурации `Description` — до 512 символов кодировки UTF-8.
- Файл универсальной конфигурации зашифровывается на пароле. Допустимая длина пароля — от 8 до 32 символов. Разрешенные символы — прописные и строчные буквы латинского алфавита, цифры, специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- Команда устанавливает глобальную блокировку управляющих запросов; текущие сессии пользователей сохраняются, новые сессии не открываются.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# machine config export usb

Checking settings integrity...done

Do you want to add configuration description [Yes/No]: y

Description: universal configuration
```

```
Enter password for encryption:
Creating configuration file...done
Insert USB drive with at least 3.0MB free space and press Enter
General USB Flash Disk successfully mounted.
Copying HW1000-15ea000b-20220220T152132Z.vbe to USB drive. Press ^+C to abort.
File successfully copied.
You may remove the USB drive.
```

machine config import

Импортировать настройки универсальной конфигурации или индивидуальную конфигурацию ViPNet Coordinator HW с USB-носителя.

Синтаксис

```
machine config import
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Файл универсальной конфигурации имеет расширение `vbe` и зашифрован на пароле. Импорт универсальной конфигурации можно выполнить на любом ViPNet Coordinator HW версий 5.1 и выше. При этом необходимо:
  - Указать пароль, на котором зашифрован файл конфигурации.
  - Выбрать настройки по группам и способ импорта:
    - `Firewall` — пользовательские настройки межсетевого экрана (сетевые фильтры, правила трансляции адресов (NAT), группы объектов): с добавлением к текущим настройкам (`append`) или с заменой текущих настроек (`replace`).
    - `Network-interface settings` — настройки сетевых интерфейсов.
    - `Routing settings` — таблицы и политики статической маршрутизации: `append` или `replace`.
- Файл индивидуальной конфигурации имеет расширение `ecf` и зашифрован на ключе обмена. Импортировать индивидуальную конфигурацию можно только на тот ViPNet Coordinator HW, на котором она была создана ранее.
- По завершении импорта конфигурации отображаются статические IP-адреса сетевых интерфейсов. Возможность подключения к ViPNet Coordinator HW по этим интерфейсам определяется сетевыми фильтрами.

- Команда устанавливает глобальную блокировку управляющих запросов; текущие сессии пользователей сохраняются, новые сессии не открываются.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Импорт настроек универсальной конфигурации:

```
hostname# machine config import
Insert USB drive and press Enter


Found va-20210220T152132Z.vbe.
Product: ViPNet Coordinator VA
Platform: VA VMWARE
Software version: 5.1.0-2799
Description: universal configuration.


Enter configuration password:
Loading settings...


Select which settings you want to import:
Firewall [y/n] : y
Append firewall settings or replace them? [a/r] : a
Network-interface settings [y/n] : y
Routing settings [y/n] : y
Append routing settings or replace them? [a/r] : r


After the import the device should be available with following parameters:
Web-interface port: 8080
SSH-port: 22
Static interface addresses:
   12.11.2.33
   175.165.73.2
Obtained DHCP-addresses.
```

```
Importing settings...done
Settings successfully imported. You may remove the USB drive.
```

Импорт индивидуальной конфигурации ViPNet Coordinator HW:

```
hostname# machine config import
Insert USB drive and press Enter

Found va-20210220T152132Z.ecf.

After the import the device should be available with following parameters:
Web-interface port: 8080
SSH-port: 22
Obtained DHCP-addresses.

Importing settings...done
Settings successfully imported. You may remove the USB drive.
```

machine halt

Завершить работу ViPNet Coordinator HW.

Синтаксис

```
machine halt
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# machine halt
Shutting down failover daemon
Shutting down MFTP daemon
Shutting down IpLir
hostname# The session has been forced to close.
```

machine hosts add

Добавить запись о соответствии IP-адреса доменному имени в файл hosts ViPNet Coordinator HW.

Синтаксис

```
machine hosts add <IP-адрес> <доменное имя>
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес сетевого узла.
- `<доменное имя>` — доменное имя сетевого узла.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Добавляются только уникальные записи.
- Одному IP-адресу может соответствовать несколько доменных имён, и наоборот — одному доменному имени может соответствовать несколько IP-адресов.
- В кластере файл hosts не синхронизируется, поэтому команду необходимо выполнить на обоих узлах.

Пример использования

Чтобы добавить запись о соответствии IP-адреса `12.0.11.23` доменному имени `prime.vipnet` в файл hosts:

```
hostname# machine hosts add 12.0.11.23 prime.vipnet
```

machine hosts remove

Удалить запись о соответствии IP-адреса доменному имени в файле hosts ViPNet Coordinator HW.

Синтаксис

```
machine hosts remove {<IP-адрес> | <доменное имя>}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес сетевого узла.
- `<доменное имя>` — доменное имя сетевого узла.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию файл hosts содержит запись `127.0.0.1 <имя узла> localhost localhost.localdomain`, которую невозможно удалить.
- В кластере файл hosts не синхронизируется, поэтому команду необходимо выполнить на обоих узлах.

Пример использования

Чтобы удалить все записи файла hosts, в которых указан IP-адрес `12.0.11.23`:

```
hostname# machine hosts remove 12.0.11.23
```

machine hosts show

Просмотреть файл hosts ViPNet Coordinator HW.

Синтаксис

```
machine hosts show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Для завершения просмотра нажмите **Q** или **Ctrl+C**.

Пример использования

Чтобы просмотреть файл hosts ViPNet Coordinator HW с именем hw1000:

```
hostname> machine hosts show
127.0.0.1 hw1000 localhost localhost.localdomain
11.1.0.23 nvs.prime
12.0.11.23 nsms.vipnet
```

machine logs clear dns

Очистить журнал DNS-запросов.

Синтаксис

```
machine logs clear dns
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# machine logs clear dns
This will clear log files. Are you sure? [Yes/No]: Yes
Removing DNS request log... Done
```

machine logs export usb

Экспортировать архив файлов журналов на USB-носитель.

Синтаксис

```
machine logs export usb
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Имя архива файлов журналов — `logs-<платформа>-<идентификатор узла>-%Y-%M-%D-%H-%M-%S.tar.gz`.
- Файлы журналов в архиве:
  - журнал аудита — `/var/log/audit_user.tar.gz`;
  - журнал СКЗИ — `/var/log/audit_crypto.tar.gz`;
  - журнал MFTP — `/var/log/mftpenv.log`;
  - журнал DNS-запросов — `/var/log/namedlog`;
  - системный журнал — `var/log/everything.log` и ротированные архивы.

- При просмотре архива в Windows время его создания может отличаться от реального времени, но время событий будет указано правильно. Это связано с особенностями работы с системным временем в Linux и Windows.

Пример использования

```
hostname# machine logs export usb

archiving user in progress, wait please...

.

archiving user complete


copying in progress, wait please...

.

archiving crypto in progress, wait please...

.

archiving crypto complete


copying in progress, wait please...

.prepare audit export files complete

Stopping system log daemon: syslogd.

tar: Removing leading `/' from member names

/var/log/alert

/var/log/audit/

/var/log/audit/hw_management_1.dblite

/var/log/audit/hw_crypto_1.dblite-shm

/var/log/audit/hw_management_1.dblite-shm

/var/log/audit/hw_management_1.dblite-wal

/var/log/audit/hw_crypto_1.dblite

/var/log/audit/hw_crypto_1.dblite-wal

/var/log/audit_crypto.tar.gz

/var/log/audit_user.tar.gz

/var/log/dmesg.boot

/var/log/everything.log

/var/log/integrity.log

/var/log/iphook.log
```

```
/var/log/iptables_new_ruleset.log

/var/log/iptables_new_tree.log

/var/log/iptables_old_ruleset.log

/var/log/iptables_old_tree.log

/var/log/lastlog

/var/log/snort/

/var/log/startboot.log

/var/log/vmware-vmsvc.log

/var/log/webgui-fcgi-server.log

/var/log/wtmp

/mnt/main/etc/probed_hw.txt

Starting system log daemon: syslogd.

Insert USB drive with at least 4.4MB free space and press Enter

Generic Flash Disk successfully mounted.


Copying logs_va_3e1303d1_va1000_2023_01_24_12_59_09.tar.gz to USB drive. Press ^+C to
abort.

File successfully copied. Unmounting USB drive...

You may remove the USB drive.
```

machine logs export-and-clear usb

Экспортировать архив файлов журналов на USB-носитель с последующим удалением файлов журналов на ViPNet Coordinator HW.

Синтаксис

```
machine logs export-and-clear usb
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Имя архива файлов журналов — `logs-<платформа>-<идентификатор узла>-%Y-%M-%D-%H-%M-%S.tar.gz`.
- Файлы журналов в архиве:

- журнал аудита — `/var/log/audit_user.tar.gz`;
- журнал СКЗИ — `/var/log/audit_crypto.tar.gz`;
- журнал MFTP — `/var/log/mftpenv.log`;
- журнал DNS-запросов — `/var/log/namedlog`;
- системный журнал — `var/log/everything.log` и ротированные архивы.

- При просмотре архива в Windows время его создания может отличаться от реального времени, но время событий будет указано правильно. Это связано с особенностями работы с системным временем в Linux и Windows.

Пример использования

```
hostname# machine logs export-and-clear usb
Are you sure to export and remove logs? [Yes/No]: Yes
.
Insert USB drive with at least 16KB free space and press Enter
Generic Flash Disk successfully mounted.


Copying logs_va_VMWARE_5.2.0-5133_3e1303d1_va1000_2023_02_20_15_06_33.tar.gz to USB
drive. Press ^+C to abort.
File successfully copied. Unmounting USB drive...
Logs archive file integrity check successful.
You may remove the USB drive.
Logs exported and removed from ViPNet Coordinator VA successfully.
```

machine logs export network-traffic usb

Экспортировать журнал IP-пакетов на USB-носитель.

Синтаксис

```
machine logs export network-traffic usb <имя>
```

Параметры и ключевые слова

`<имя>` — имя файла экспорта.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда недоступна при работе в удаленной SSH-сессии.
- До выполнения команды сформируйте файл экспорта журнала IP-пакетов с помощью команды `machine logs show network-traffic` (ddd).

- При вводе имени файла работает автодополнение и подсказка, данные для подсказки берутся из списка существующих файлов экспорта.

Пример использования

Чтобы экспортировать журнал IP-пакетов в файл с именем `ippacket`:

```
hostname# machine logs export network-traffic usb ippacket
Put ippacket.tar.gz file onto USB drive.
Insert USB drive and press Enter
1) JetFlash Transcend 4GB partition 3825Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc as is
Partition /dev/sdc was successfully mounted on /usb.
File ippacket.tar.gz to be copied onto the USB drive.
File ippacket.tar.gz was successfully copied onto the USB drive.
You may remove the USB drive.
```

machine logs settings

Задать максимальный размер журнала аудита или журнала СКЗИ.

Синтаксис

```
machine logs settings {user-audit | crypto-audit} size <размер>
```

Параметры и ключевые слова

- Тип журнала:
  - `user-audit` — журнал аудита.
  - `crypto-audit` — журнал СКЗИ.
- `<размер>` — максимальный размер выбранного журнала в Мбайт. Минимальное значение — 10 Мбайт, максимальное — зависит от объёма свободной дисковой памяти.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Если текущий размер журнала превышает задаваемое значение `<размер>`, то выводится уведомление `To perform the operation, you must export the log. Continue?`; при подтверждении запускается команда `machine logs export usb`.

Пример использования

Чтобы задать максимальный размер журнала СКЗИ 100 Мбайт, выполните:

```
hostname# machine logs settings crypto-audit size 100
```

machine logs settings cef

Задать для сетевого интерфейса исключения из списка событий журнала IP-пакетов, экспортируемых в формате CEF.

Синтаксис

```
machine logs settings cef <интерфейс> {include | exclude} {<события> | none}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса;
- действие:
  - `include` — включить в список событий;
  - `exclude` — исключить из списка событий;
- `<события>` — номера событий, разделенные запятой;
- `none` — удалить исключения.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Если экспорт сообщений CEF настроен в режиме `ips`, исключения, заданные командой, игнорируются.

Пример использования

```
hostname# machine logs settings cef eth0 exclude 2,121,33
```

```
hostname# machine logs settings cef eth0 exclude none
```

machine logs settings cef event-type

Задать тип событий журнала IP-пакетов, экспортируемых в формате CEF.

Синтаксис

```
machine logs settings cef event-type {all | blocked} [<интерфейс>]
```

Параметры и ключевые слова

- Тип событий:
  - `all` — все события журнала IP-пакетов;
  - `blocked` — события о блокированных IP-пакетах или с предупреждением IPS о вторжении;
- `<интерфейс>` — имя сетевого интерфейса.

Значения по умолчанию

Если сетевой интерфейс не указан, тип событий задается для всех интерфейсов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Тип событий по умолчанию — `blocked`.

Пример использования

```
hostname# machine logs settings cef event-type all
```

```
hostname# machine logs settings cef event-type blocked eth2
```

machine logs settings network-traffic maxsize

Задать максимальный размер журнала IP-пакетов для выбранного сетевого интерфейса.

Синтаксис

```
machine logs settings network-traffic <интерфейс> maxsize <размер>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса;
- `<размер>` — размер журнала IP-пакетов интерфейса, Мбайт.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Значение размера журнала по умолчанию и его максимальный размер зависят от исполнения ViPNet Coordinator HW:

Таблица 5. Размер по умолчанию и максимальный размер журнала IP-пакетов, Мбайт

Исполнение	Размер по умолчанию	Макс. размер для физических интерфейсов	Макс. размер для виртуальных интерфейсов
HW50	10	10	
HW100	50	50	
HW1000	50	1800	200
HW2000	50	1800	200
HW5000	50	1800	200
ViPNet Coordinator VA	50	1800	200

Пример использования

```
hostname# machine logs settings network-traffic eth0 maxsize 40
```

machine logs settings network-traffic omit-client-port

Включить или выключить регистрацию порта TCP-соединения на сетевом интерфейсе.

Синтаксис

```
machine logs settings network-traffic <интерфейс> omit-client-port {on | off}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса;
- `on` — включите регистрацию;
- `off` — выключить регистрацию.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Значение по умолчанию — `off`. В этом случае, если с сетевого узла выполняется попытка подключения к порту ViPNet Coordinator HW, и соединение не устанавливается, то при следующей попытке с того же узла может быть использован другой порт. При сканировании портов число таких попыток может достигать нескольких сотен в секунду. Поскольку каждый раз используется другой порт, то для каждого IP-пакета создается запись в журнале IP-пакетов.
- Если `omittcpclientport` установлен в `on`, порт TCP-соединении не регистрируется, в журнале IP-пакетов номера порта указывается равным нулю, что позволяет объединить события о попытках подключения к какому-либо порту ViPNet Coordinator HW с определенного узла в одну запись.

Пример использования

```
hostname# machine logs settings network-traffic eth1.2 omit-client-port on
```

machine logs settings network-traffic register

Включить или выключить регистрацию IP-пакетов определенного типа, проходящих через сетевой интерфейс, в журнале IP-пакетов.

Синтаксис

```
machine logs settings network-traffic <интерфейс> register {passed | broadcast | service}
{on | off}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса;
- тип IP-пакетов:
  - `passed` — пропущенные;
  - `broadcast` — широковещательные;
  - `service` — служебные;
- регистрация IP-пакетов:
  - `on` — включить;
  - `off` — выключить.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Регистрация IP-пакетов по умолчанию:
  - пропущенные — `off` (при этом регистрируются события о блокированных IP-пакетах и изменении IP-адресов сетевых узлов);
  - широковещательные — `off`;
  - служебные — `on`.

Пример использования

```
hostname# machine logs settings network-traffic eth1 register passed on
```

machine logs settings network-traffic timediff

Задать интервал времени, в течение которого связанные события регистрации IP-пакетов, проходящих через сетевой интерфейс, объединяются в одну запись журнала IP-пакетов.

Синтаксис

```
machine logs settings network-traffic <интерфейс> timediff <интервал>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса;
- `<интервал>` — интервал времени, секунды.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Значение интервала времени по умолчанию — 60 секунд.

Пример использования

```
hostname# machine logs settings network-traffic eth1.2 timediff 10
```

machine logs settings show

Просмотреть размер и процент заполнения журналов аудита и СКЗИ, а также настройки экспорта журнала IP-пакетов в формате CEF.

Синтаксис

```
machine logs settings show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются:

- Размер и процент заполнения журналов аудита и СКЗИ.
- Настройки экспорта журнала IP-пакетов в формате CEF:
  - статус экспорта:
    - `enabled` — включен;
    - `disabled` — выключен;
  - режим формирования сообщений CEF:
    - `hw` — полные сообщения;
    - `ips` — по событиям IPS 67 и 142;
  - IP-адрес и порт сервера для приема сообщений CEF.
- Настройки журнала IP-пакетов по сетевым интерфейсам:
  - `Interface` — имя интерфейса;
  - `Max size` — максимальный размер журнала, Мбайт;
  - `Timediff` — интервал объединения связанных IP-пакетов в одну запись журнала, секунды;
  - `Flags` — флаги регистрации IP-пакетов по типам в порядке `PBSO`:
    - `P` — регистрировать пропущенные IP-пакеты;
    - `B` — регистрировать широковещательные IP-пакеты;
    - `S` — регистрировать служебные VPN-события;
    - `O` — регистрировать порт TCP-соединений;
    - `-` — не регистрировать IP-пакеты по соответствующему флагу.
  - `CEF type` — типы событий в сообщении CEF:
    - `all` — все события журнала IP-пакетов;
    - `blocked` — события о блокированных IP-пакетах или с предупреждением IPS о вторжении.
  - `Excluded events (CEF)` — исключать из сообщений CEF события с заданными номерами.

Пример использования

```
hostname#  machine logs settings show

Journal size limit:

  User-audit: 50 Mb (56% free)

  Crypto-audit: 50 Mb (74% free)


CEF export enabled (hw)

Server address and port: 192.168.1.1 : 514


Interface  Max size  Timediff  Flags   CEF type  Excluded events (CEF)

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

eth0             50         5  PBSO    blocked   5,6,7,8

eth1             50         5  PBS-    all       -

eth2             50         5  --S-    all       1,3,14,15,16,17,18,19,44,45,46,

                                                  47,48,57,59

eth3             50         5  --S-    all
```

machine logs show crypto-audit

Просмотреть журнал СКЗИ.

Синтаксис

```
machine logs show crypto-audit [reversed] [result {success | failed}] [from <время>] [to <время>] [user <имя>] [text <строка>]
```

Параметры и ключевые слова

- `reversed` — вывод записей в обратном хронологическом порядке.
- `result` — вывод записей в зависимости от результата выполнения запроса:
  - `success` — успех.
  - `failed` — ошибка.
- `from <время>` — вывод записей, начиная с указанного времени.
- `to <время>` — вывод записей до указанного времени включительно.
- `user <имя>` — вывод записей, связанных с пользователем.
- `text <строка>` — вывод записей, содержащих строку текста.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Для завершения просмотра нажмите клавишу **Q**.
- Параметр `<время>` задается в формате `YYYY-MM-DD hh:mm:ss`.
- В параметре `<строка>` разрешены символы `A-Z`, `a-z`, `0-9`, а также: `!# $ % & () * + , - . / : ; < = > @ [ ] _ { | } ~`.

  Параметр `<строка>`, в котором есть пробелы или `$`, необходимо заключать в двойные кавычки.
- Формат записи журнала:
  - Дата и время события в формате `YYYY-MM-DD hh:mm:ss`.
  - Имя узла ViPNet, например `hostname`.
  - Режим системы защиты от сбоев:
    - `single mode` — одиночный режим.
    - `active` — активный узел кластера.
    - `passive` — пассивный узел кластера.
  - Текст события.
  - Статус запроса: `success` или `failed`.
  - Инициатор запроса:
    - Имя учетной записи — `admin`, `user`, централизованные пользователи.
    - `System` — служебный запрос.
    - `System.Prime` — запрос ViPNet Prime.
  - Подробности события.

Пример использования

Просмотреть все записи журнала СКЗИ:

```
hostname# machine logs show crypto-audit
2024 12:37:33 [hostname] [Single Mode] backup_dump [success] [System]
Details: finish
2024 12:37:38 [hostname] [Single Mode] CheckIntegrity [success] [System]
Details: failoverd: initializing (single)
2024 12:37:39 [hostname] [Single Mode] CheckIntegrity [success] [System]
Details: iplircfg: initializing
```

```
2024 12:37:42 [hostname] [Single Mode] backup_dump [success] [System]
Details: finish
2024 12:38:04 [hostname] [Single Mode] StartSession [failed] [System]
Details: userid:admin ticket:
2024 12:38:14 [hostname] [Single Mode] StartSession [success] [System]
Details: userid:admin ticket:AAA__17c91f_bd5b57_1c936a_9eb8e0
2024 12:38:52 [hostname] [Single Mode] Lock [success] [System]
...
```

Просмотреть записи журнала, в которых встречается строка `9eb8e0`:

```
hostname# machine logs show crypto-audit text ca7776b9
2024 12:38:14 [hostname] [Single Mode] StartSession [success] [System]
Details: userid:admin ticket:AAA__17c91f_bd5b57_1c936a_9eb8e0
```

machine logs show mftp

Просмотреть журнал MFTP.

Синтаксис

```
machine logs show mftp
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Формат записи журнала MFTP:
  - `Envelope filename, Personal envelope name` — имя конверта.
  - `Sender` — имя узла-отправителя конверта.
  - `Receiver` — имя узла-получателя конверта.
  - `Date-Time` — дата и время события.
  - `Event` — статус конверта:
    - `Received` — принят;
    - `Sent` — отправлен;
    - `Deleted` — удален;

- `Size` — размер конверта в килобайтах.
- `Description` — описание конверта.
- `Task` — прикладная задача, в которой создан конверт.

- Если имеется несколько файлов журнала, то они выводятся по порядку, начиная с последней даты. Чтобы после просмотра одного файла журнала открыть следующий, нажмите клавишу `q` и на запрос `Do you want to view the next mftp log file?` ответьте `Yes`.
- При выполнении команды на одном из узлов кластера отображается только информация о конвертах, обработанных за периоды, когда этот узел был активным.

Пример использования

```
hostname# machine logs show mftp
=== MFTP envelopes journal dump at Tue Feb 11 16:45:48 2024
-------------------------------------------------------------------------------
-------------------------------------------------------------
| Envelope filename | Personal envelope name | Sender| Receiver            |Date-Time
 |     Event         |      Size   |      Description   |      Task          |
-------------------------------------------------------------
| ~OJ)(#(A.RJ9      | ~OJ)(#(A.RJ9               | Admin    | xfva | 11.02.2024 16:45:48
 |     Received      |      19090  |                    | File exchange      |
-------------------------------------------------------------------------------
-------------------------------------------------------------
```

machine logs show network-traffic

Просмотреть журнал IP-пакетов.

Синтаксис

```
machine logs show network-traffic
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Служба `iplircfg` должна быть запущена.
- После запуска команды задайте параметры поиска записей в журнале IP-пакетов и нажмите **Find**.
- В кластере команда выполняется только на активном узле.

Пример использования

```
hostname# machine logs show network-traffic
```

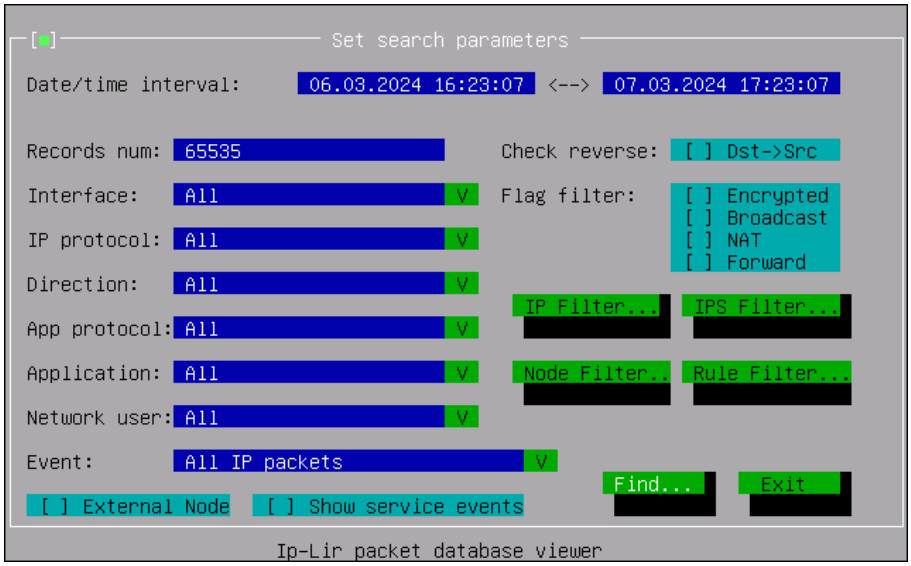

Рисунок 1. Параметры поиска записей в журнале IP-пакетов

machine logs show syslog

Просмотреть системный журнал.

Синтаксис

```
machine logs show syslog [reversed] [{since <время> | filtered {<служба> | string <строка>}
}]
```

Параметры и ключевые слова

- `reversed` — вывод записей в обратном хронологическом порядке.
- `since <время>` — вывод записей, начиная с указанного времени.
- `<служба>` — вывод записей системного журнала для указанной службы ПО ViPNet Coordinator HW.
- `string <строка>` — вывод записей, содержащих строку текста.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Для завершения просмотра нажмите клавишу **Q**.
- Параметр `<время>` задаётся в формате `YYYY-MM-DD hh:mm:ss`.
- В параметре `<служба>` можно указать одну из служб ПО ViPNet Coordinator HW. Полный список служб см. в документе «Настройка с помощью командного интерпретатора», разделе «Список служб ПО ViPNet Coordinator HW».
- В параметре `<строка>` можно использовать символы `A-Z, a-z, 0-9`, а также `!# $ % & () * + , - . / : ; < = > @ [ ] _ { | } ~`.

  Параметр `<строка>`, в котором есть пробелы или `$`, необходимо заключать в двойные кавычки.

Пример использования

Просмотр всех записей системного журнала за все время и для всех служб:

```
hostname# machine logs show syslog
```

Просмотр записей системного журнала, начиная с 14:50 22 февраля 2024 года, выводимых в обратном порядке:

```
hostname# machine logs show syslog reversed since 2024-02-22 14:50:00
```

Просмотр записей системного журнала для службы `vmunix`:

```
hostname# machine logs show syslog filtered vmunix
```

Просмотр записей системного журнала за всё время его ведения, в которых встречается строка `command 3001`:

```
hostname# machine logs show syslog filtered string "command 3001"
```

machine logs show user-audit

Просмотреть журнал аудита.

Синтаксис

```
machine logs show user-audit [reversed] [result {success | failed}] [from <время>] [to <время>] [user <имя>] [text <строка>]
```

Параметры и ключевые слова

- `reversed` — вывод записей в обратном хронологическом порядке.
- `result` — вывод записей в зависимости от результата выполнения запроса:
  - `success` — успех.
  - `failed` — ошибка.

- `from <время>` — вывод записей, начиная с указанного времени.
- `to <время>` — вывод записей до указанного времени включительно.
- `user <имя>` — вывод записей, связанных с пользователем.
- `text <строка>` — вывод записей, содержащих строку текста.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Для завершения просмотра нажмите клавишу **Q**.
- Параметр `<время>` задаётся в формате `YYYY-MM-DD hh:mm:ss`.
- В параметре `<строка>` разрешены символы `A-Z`, `a-z`, `0-9`, а также: `!# $ % & () * + , - . / : ; < = > @ [ ] _ { | } ~`.

  Параметр `<строка>`, в котором есть пробелы или `$`, необходимо заключать в двойные кавычки.
- Формат записи журнала:
  - Дата и время события в формате `YYYY-MM-DD hh:mm:ss`.
  - Имя узла, например `hostname`.
  - Режим системы защиты от сбоев:
    - `single mode` — одиночный режим.
    - `active` — активный узел кластера.
    - `passive` — пассивный узел кластера.
  - Текст события.
  - Статус запроса: `success` или `failed`.
  - Инициатор запроса:
    - Имя учётной записи — `admin`, `user`, централизованные пользователи.
    - `System` — служебный запрос.
    - `System.Prime` — запрос ViPNet Prime.
  - Подробности события.

Пример использования

Просмотреть все записи журнала аудита:

```
hostname# machine logs show user-audit
2024 12:38:14 [hostname] [Single Mode] VPN:ViPNet:ShowWarningThreshold [success] [admin]
```

```
Details: Command:'certificate or keys expiration request '

2024 12:38:14 [hostname] [Single Mode] View the password protectioncounter [success]
[admin]

Details: Command:'Recorded failed authentication request '

2024 12:38:53 [hostname] [Single Mode] Edit firewall filters via Web Access [success]
[admin]

Details: Command:'firewall local add 'src' '@any' 'dst' '@any' 'pass' '

2024 12:38:53 [hostname] [Single Mode] Add firewall filter [success] [admin]

Details: Command:'firewall local add 'src' '@any' 'dst' '@any' 'pass' '

2024 12:39:05 [hostname] [Single Mode] Show network interface parameters [success] [admin]

Details: Command:'inet show interface eth0'

2024 12:39:58 [hostname] [Single Mode] Show idle session time-out [success] [admin]

Details:

2024 12:39:58 [hostname] [Single Mode] Show appliance info [success] [admin]

Details:

2024 12:39:58 [hostname] [Single Mode] Viewing license information[success] [admin]

Details:

...
```

Просмотреть записи журнала, начиная с 14:50 22 ноября 2024 года, выводимые в обратном порядке:

```
hostname# machine logs show user-audit reversed from 2024-11-22 14:50:00
```

Просмотреть записи журнала с 14:50 по 17:50 22 ноября 2024 года пользователя `admin` с неуспешным результатом выполнения запроса:

```
hostname# machine logs show user-audit result failed from 2018-11-22 14:50:00 to 2024-11-22
17:50:00 user admin
```

machine reboot

Перезагрузить ViPNet Coordinator HW.

Синтаксис

```
machine reboot
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# machine reboot
reboot in progress
...
hostname> login:
```

machine reboot-schedule

Включить или выключить перезагрузку ViPNet Coordinator HW по расписанию.

Синтаксис

```
machine reboot-schedule {on | off}
```

Параметры и ключевые слова

- `on` — включить перезагрузку по расписанию.
- `off` — выключить перезагрузку по расписанию.

Значения по умолчанию

Перезагрузка по расписанию выключена (`off`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# machine reboot-schedule on
Automatic reboot is scheduled at 23:00 on saturdays
```

machine reboot-schedule show

Просмотреть настройку перезагрузки ViPNet Coordinator HW по расписанию.

Синтаксис

```
machine reboot-schedule show
```

Режимы командного интерпретатора

- Режим просмотра.

- Режим настройки.

Пример использования

```
hostname> machine reboot-schedule show
Automatic reboot is scheduled at 23:00 on saturdays
```

machine reboot-schedule time

Задать расписание перезагрузки ViPNet Coordinator HW.

Синтаксис

```
machine reboot-schedule time <время> [day <день>]
```

Параметры и ключевые слова

- `<время>` — время перезагрузки. Указывается в формате `hh:mm`, где `hh` — часы (24-часовой формат), `mm` — минуты;
- `<день>` — день недели перезагрузки. Указываются английские полные названия без учета регистра — `Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday`.

Значения по умолчанию

Расписание перезагрузки по умолчанию — `02:00 on mondays`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если день недели не указан, выполняется ежедневная перезагрузка ViPNet Coordinator HW в указанное время.
- В кластере выполните команду на обоих узлах. Рекомендуется устанавливать время перезагрузки узлов, различающееся не менее чем на 30 минут.

Пример использования

Чтобы настроить перезагрузку в субботу в 06.00 часов утра:

```
hostname# machine reboot-schedule time 06:00 day Saturday

Automatic reboot is scheduled at 06:00 on saturdays
```

machine self-test

Запустить регламентное тестирование ViPNet Coordinator HW.

Синтаксис

```
machine self-test
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команду нельзя выполнить при удаленном подключении по SSH.
- До начала тестирования работа всех служб будет автоматически завершена, а после успешного окончания тестирования — автоматически восстановлена.
- В процессе регламентного тестирования проводятся:
  - Проверка файловых систем на первом и втором разделах загрузочного носителя.
  - Проверка контрольных сумм исполняемых и конфигурационных файлов ПО ViPNet Coordinator HW.
  - Статистический контроль последовательностей случайных чисел, генерируемых программным датчиком случайных чисел (ПДСЧ).
- При успешной проверке на экран выводятся имена проверенных файлов и шестнадцатеричные значения их контрольных сумм.
- После успешной проверки в исполнениях ViPNet Coordinator HW с двумя накопителями (все исполнения, кроме ViPNet Coordinator HW50) автоматически создается резервная копия конфигурационных и исполняемых файлов ПО, а также справочников.
- При обнаружении ошибок контрольных сумм файлов предпринимается попытка их восстановления из резервной копии с последующей перезагрузкой ViPNet Coordinator HW. При этом, если восстановление поврежденного конфигурационного файла было неуспешным, то ViPNet Coordinator HW перезагружается в режим ограниченной функциональности (подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Контроль целостности файлов ПО»).
- При обнаружении ошибки статистического контроля ПДСЧ ViPNet Coordinator HW перезагружается.
- Команда устанавливает глобальную блокировку управляющих запросов; текущие сессии пользователей сохраняются, новые сессии не открываются.

Пример использования

```
hostname# machine self-test
```

```
If you run a self-test, then all daemons will be stopped. Continue? [Yes/No]: Yes
Operation may take a long time. Please wait...
>> Self test successfully passed.
>> Imito-protective inserts for modules:
iplircfg >> AEC2F1B4
failoverd >> E29353AE
webgui-fcgi-server >> E2SAS945
webgui-http-server >> 0E64E6FA
vpncrnd >> 35DA5FFC
rvpn_shell >> B77EDA20
vipnetsnrnp >> S133F97C
snort >> F3E93096
libidents.so >> 729DEEB0
libpasswd.so >> 415AS0S9
libpwdgen.so >> CE3FF31D
libroulett2.so >> C888289E
libstoredev.so >> D1192E5B
```

machine session-inactivity-timeout set

Установить допустимое время неактивности сессий пользователей.

Синтаксис

```
machine session-inactivity-timeout set <время>
```

Параметры и ключевые слова

`<время>` — время неактивности сессии в интервале 60–54000 секунд.

Значения по умолчанию

600 секунд.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Допустимое время неактивности устанавливается одинаковым для всех сессий пользователей.
- Сессия будет завершена через время неактивности, заданное в параметре `<время>`. В некоторых случаях, например при низкой скорости удаленного подключения, фактическое время завершения сессии может увеличится не более чем на 180 секунд.

Пример использования

Чтобы установить допустимое время неактивности сессии 600 секунд:

```
hostname# machine session-inactivity-timeout set 600
```

machine session-inactivity-timeout show

Просмотреть текущее допустимое время неактивности сессий пользователей.

Синтаксис

```
machine session-inactivity-timeout show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> machine session-inactivity-timeout show
Current session inactivity time is 600 sec (10 min)
```

machine set date

Изменить дату и время.

Синтаксис

```
machine set date <дата> <время>
```

Параметры и ключевые слова

- `<дата>` — дата. Указывается в формате `YYYY-MM-DD`, где `YYYY` — год, `MM` — месяц, `DD` — день.
- `<время>` — время. Указывается в формате `hh:mm:ss`, где `hh` — часы, `mm` — минуты, `ss` — секунды.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- После ввода даты и времени необходимо подтвердить действие — ввести `Yes` и нажать **Enter**.
- Дата и время на ViPNet Coordinator HW не должны отличаться от даты и времени узлов сети ViPNet более чем на величину `timediff`. Иначе текущие управляющие соединения с ViPNet Coordinator HW будут разорваны, а новые управляющие соединения невозможно будет установить.
- В кластере команда выполняется только на активном узле. Дата и время на пассивном узле синхронизируются с датой и временем на активном узле. Подробнее см. описание параметра `syncdatetime` секции `[misc]` конфигурационного файла `failover.ini`.

Пример использования

Чтобы установить дату 22 февраля 2024 года и время, равное 12 часам:

```
hostname# machine set date 2024-02-22 12:00:00
Do you really wish to change the date?
Continue? [Yes/No]: Yes
```

machine set hostname

Изменить имя компьютера.

Синтаксис

```
machine set hostname <имя>
```

Параметры и ключевые слова

`<имя>` — имя компьютера.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При инициализации ViPNet Coordinator HW имя компьютера формируется по шаблону `<название>-<идентификатор>`:

- `название` — наименование аппаратной платформы ViPNet Coordinator HW без последних двух символов;
- `идентификатор` — идентификатор сетевого узла.

Например: `HW1000-270E033A`, `HW100-2A15000D`.

Пример использования

Чтобы установить имя компьютера HW1000:

```
hostname# machine set hostname HW1000
```

machine set loghost

Задать место хранения системного журнала. С помощью этой команды также можно выключить запись событий в журнал.

Синтаксис

```
machine set loghost {<адрес> | local | null}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес или доменное имя сетевого узла, на котором будет храниться системный журнал (удалённое ведение журнала).
- `local` — хранить системный журнал на ViPNet Coordinator HW (локальное ведение журнала).
- `null` — выключить ведение журнала.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию системный журнал хранится на ViPNet Coordinator HW (`local`).
- Если системный журнал будет храниться на удалённом узле, этот узел должен быть доступен для ViPNet Coordinator HW. Если узел является открытым, то на ViPNet Coordinator HW создайте фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на 514-й порт этого узла.
- Для настройки удалённого ведения журнала в кластере задайте место хранения журнала как на активном, так и на пассивном узле кластера, так как эти настройки не синхронизируются.
- Не рекомендуется настраивать удалённое ведение журнала в кластере, так как на удалённый узел не будут передаваться события с пассивного узла.

Пример использования

Чтобы отправить системный журнал на узел с адресом 192.168.10.10:

```
hostname# machine set loghost 192.168.10.10
```

machine set log invalid-packet

Включить и отключить запись нарушений параметров таблицы соединений в системный журнал.

Синтаксис

```
machine set log invalid-packet {on | off}
```

Параметры и ключевые слова

- `on` — нарушения параметров таблицы соединений записываются в журнал;
- `off` — нарушения параметров таблицы соединений не записываются в журнал.

Значения по умолчанию

Нарушения параметров таблицы соединений записываются в журнал (`on`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Для включения записи нарушений параметров таблицы соединений в системный журнал:

```
hostname# machine set log invalid-packet on
```

machine set log queue

Включить или выключить запись в системный журнал событий о входящих IP-пакетах, обработка которых была отклонена в рамках приоритетной обработки трафика.

Синтаксис

```
machine set log queue {on | off}
```

Параметры и ключевые слова

- `on` — записывать события об отклоненных IP-пакетах в журнал;

- `off` — не записывать события об отклоненных IP-пакетах в журнал.

Значения по умолчанию

События об отклоненных IP-пакетах записываются в журнал (`on`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Для включения записи в системный журнал событий об отклоненных IP-пакетах:

```
hostname# machine set log queue on
```

machine set timezone

Задать временную зону (часовой пояс).

Синтаксис

```
machine set timezone <временная зона>
```

Параметры и ключевые слова

`<временная зона>` — временная зона, заданная в формате `Континент/Зона`, или значение `UTC` для установки времени UTC.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Название континента и зоны должны начинаться с прописной буквы.
- При вводе континента или зоны работает подсказка.
- Если временная зона не указана, выводится список всех существующих временных зон.
- В кластере команда выполняется только на активном узле. Временная зона на пассивном узле синхронизируются с временной зоной на активном узле кластера. Подробнее см. описание параметра `syncdatetime` секции `[misc]` конфигурационного файла `failover.ini`.

Примеры использования

- Чтобы просмотреть список временных зон в Антарктике:

```
hostname# machine set timezone Antarc?
Antarctica/Casey
Antarctica/Davis
...
```

- Чтобы установить часовой пояс Москвы:

```
hostname# machine set timezone Europe/Moscow
```

machine show backup

Просмотреть состояние резервного копирования индивидуальной конфигурации ViPNet Coordinator HW.

Синтаксис

```
machine show backup
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По команде отображаются:
  - Состояние резервного копирования индивидуальной конфигурации по расписанию:
    - `ON` — включено;
    - `OFF` — выключено;
    - `unavailable` — недоступно.
  - Статус завершения последнего резервного копирования, если включено резервное копирование по расписанию или конфигурация была экспортирована вручную (см. machine backup export):
    - `Last successful remote backup: <дата и время>` — закончилось успешно или не проводилось.
    - `Last remote backup failed (previous successful backup: <дата и время>)` — ошибка (предпоследнее резервное копирование закончилось успешно или не проводилось).
  - дата и время создания следующей резервной копии по расписанию или индикация процесса резервного копирования (`Currently backing-up...`), если резервное копирование по расписанию включено.
- В кластере команда доступна для выполнения на обоих узлах.

Примеры использования

```
hostname> machine show backup

Remote backup is ON

Last successful remote backup: 2019-12-15 22:18

Backup scheduled at 22:23.

Note: ViPNet services will be stopped for the time of export


hostname> machine show backup

Remote backup is OFF.

Last backup failed (previous successful backup: never)

Backup scheduled at 22:23.


hostname> machine show backup

Remote backup is unavailable.
```

machine show date

Просмотреть дату и время, установленные на ViPNet Coordinator HW.

Синтаксис

```
machine show date
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> machine show date
Thu Jan 27 19:11:56 MSK +7 2024
```

machine show hostname

Просмотреть имя ViPNet Coordinator HW.

Синтаксис

```
machine show hostname
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> machine show hostname
hostname
```

machine show loghost

Просмотреть настройки хранения системного журнала.

Синтаксис

```
machine show loghost
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде выводится одно из следующих значений:

- `null` — ведение журнала выключено.
- `local` — системный журнал хранится локально на ViPNet Coordinator HW.
- IP-адрес удаленного сетевого узла, заданный с помощью `machine set loghost`.

Пример использования

```
hostname> machine show loghost
The loghost set to `local`
```

machine show log invalid-packet

Просмотреть настройку записи нарушений параметров таблицы соединений в системный журнал (см. machine set log invalid-packet).

Синтаксис

```
machine show log invalid-packet
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> machine show log invalid-packet
Invalid-packet option is ON
```

machine show log queue

Просмотреть настройку записи событий об отклоненных IP-пакетах в системный журнал (см. machine set log queue).

Синтаксис

```
machine show log queue
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> machine show log queue
Option is: ON
```

machine show memory

Просмотреть информацию об использовании оперативной памяти и дискового пространства.

Синтаксис

```
machine show memory
```

Режимы командного интерпретатора

- Режим просмотра.

- Режим настройки.

Особенности использования

- Информация об использовании оперативной памяти выводится в виде таблицы:
  - `Mem` — оперативная память;
  - `Swap` — файл подкачки (не поддерживается в ViPNet Coordinator HW).
  - `total` — суммарный объем памяти;
  - `used` — объем используемой памяти: `used = total - free - buff/cache`;
  - `free` — объем неиспользуемой памяти;
  - `shared` — объем разделяемой памяти
  - `buff/cache` — суммарное количество памяти, занятое Linux под буферы ядра и под страничный кеш;
  - `available` — объем памяти, доступный приложениям.
- Информация об использовании дискового пространства выводится в виде таблицы:
  - подключенные разделы файловой системы ViPNet Coordinator HW:
    - `root` — корневой раздел Linux;
    - `tmpfs` — раздел файла подкачки;
    - `overlay` — объединенная файловая система ViPNet Coordinator HW.
  - `Filesystem` — имя раздела файловой системы;
  - `Size` — размер раздела файловой системы;
  - `Used` — объем использованного пространства;
  - `Avail` — объем доступного пространства;
  - `Use%` — процент использования раздела файловой системы;
  - `Mounted on` — точка монтирования раздела файловой системы.

Пример использования

```
hostname> machine show memory
               total        used        free      shared  buff/cache   available
Mem:            2005         436         278         342        1290         800
Swap:              0           0           0

Filesystem      Size  Used Avail Use% Mounted on
root           1003M  118M  886M  12% /mnt/root
tmpfs          1003M  3.4M 1000M   1% /run
tmpfs          1003M   36K 1003M   1% /tmp
udev             10M     0   10M   0% /dev
/dev/sda2       3.8G  250M  3.5G   7% /mnt/main
/dev/sdb2        78G  137M   78G   1% /additional
```

```
tmpfs           224M  223M  1.9M 100% /cache
overlay        1003M  118M  886M  12% /
```

machine show timezone

Просмотреть информацию о временной зоне (часовом поясе), настроенной на ViPNet Coordinator HW.

Синтаксис

```
machine show timezone
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> machine show timezone
Europe/Samara
```

machine show uptime

Просмотреть время работы ViPNet Coordinator HW после загрузки, а также среднее число процессов в очереди за ближайшее время.

Синтаксис

```
machine show uptime
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображается следующая информация:

- текущее время;
- время работы ViPNet Coordinator HW после загрузки;
- текущее количество пользователей;

- среднее количество процессов в очереди ожидания процессора за последние 1, 5 и 15 минут. Выводимые значения следует интерпретировать в зависимости от количества процессорных ядер исполнения ViPNet Coordinator HW. Для исполнений с многоядерными процессорами (в том числе с двумя процессорами) критическими являются значения, превышающие общее количество ядер. Например, для исполнений с 4-мя процессорными ядрами значения не должны превышать 4.00 — такие значения говорят о том, что ViPNet Coordinator HW перегружен.

Внимание! Для исполнений с одноядерными процессорами не стоит ориентироваться на эти значения, так как количество запущенных процессов на ViPNet Coordinator HW многократно больше 1. Вместо этого используйте значение `total cpu` в выводе команды `failover show info`.

Пример использования

```
hostname> machine show uptime
 18:04:29 up 44 min, 1 user, load average: 2.19, 2.18, 2.06
```

machine update-queue

Просмотреть очередь отложенных обновлений компонентов и настроек ViPNet Coordinator HW, отправленных из ViPNet Prime.

Синтаксис

```
machine update-queue
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображается текущее состояние очереди отложенных обновлений:

- `Update type` — тип обновления:
  - `Software` — ПО ViPNet Coordinator HW.
  - `License` — лицензия.
  - `Firewall` — политики безопасности.
  - `VPN node info` — справочники и ключи.
  - `DPI` — подсистема DPI.
  - `Services` — настройки прикладных служб.
- `Sent` — время отправки обновления из ViPNet Prime.

- `Application time` — плановое время применения обновления на ViPNet Coordinator HW.

Пример использования

Чтобы просмотреть очередь отложенных обновлений ViPNet Coordinator HW:

```
hostname> machine update-queue
Update type     Sent                  Application time
-----------------------------------------------------------
Software        2021-05-22 11:44:22   2021-05-30 07:30:00
VPN node info   2021-05-21 16:34:11   2021-05-30 07:30:00
```

Команды группы mftp

Настройка параметров транспортного сервера MFTP и каналов обмена ViPNet Coordinator HW с другими узлами сети ViPNet.

mftp config

Редактировать конфигурационный файл службы `mftpd`.

Синтаксис

```
mftp config
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед редактированием конфигурационного файла завершите работу службы `mftpd` (mftp stop).
- При выполнении команды запускается текстовый редактор, в который загружается файл `mftp.conf`.
- При сохранении файла происходит проверка его корректности. В случае ошибки предлагается отказаться от изменений или продолжить редактирование. Если проверка прошла успешно, файл применяется для работы службы `mftpd`, а информация об изменении конфигурации сохраняется в системный журнал.

Пример использования

Чтобы включить режим немедленной передачи конвертов по каналу обмена с узлом `0x270e000a`:

```
hostname# mftp config
```

В открывшемся файле в секции `[channel]` для узла `0x270e000a` присвойте параметру `call_flag` значение `yes`:

```
[channel]
id = 0x270e000a
name = Client-1

type = mftp
off_flag = no
call_flag = yes
...
```

mftp info

Просмотреть очередь исходящих транспортных конвертов MFTP.

Синтаксис

```
mftp info
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- При выполнении команды в одном из исполнений ViPNet Coordinator HW50 или HW100 на консоль выводится не более 10000 записей о конвертах. При выполнении команды в остальных исполнениях число выводимых записей о конвертах ограничено временем ожидания ответа (30 секунд), но не превышает 400000 записей.
- Для просмотра очереди исходящих конвертов используйте навигационные клавиши.
- Чтобы завершить просмотр нажмите **Q**.

Пример использования

```
hostname# mftp info
Name   Size   Type   Date         Time       Sender Id    Sender Name
@M1~   1390   Mail   15-10-2014   10:40:05   0x1639001b   Client-11
0x1639001a    Client-10
@M2~   3639   Mail   15-10-2014   10:42:50   0x1639001b   Client-11
0x1639001c    Client-12
...
hostname#
```

Очередь исходящих конвертов отображается в следующем формате:

```
Name  Size  Type  Date  Time  Sender ID  Sender Name

Receiver ID  Receiver Name
```

где:

- `Name` — имя конверта.
- `Size` — размер конверта в килобайтах.
- `Type` — тип конверта:
  - `Mail` — прикладной конверт;
  - `Control request` — управляющий запрос;
  - `Control request answer` — ответ на управляющий запрос;

    - `Task receipt` — прикладная квитанция;
    - `Transport receipt` — транспортная квитанция.
- `Date`, `Time` — дата и время создания конверта (первого его появления в очереди).
- `Sender ID` — идентификатор узла-отправителя конверта.
- `Sender Name` — имя узла-отправителя конверта.
- `Receiver ID` — идентификатор узла-получателя конверта.
- `Receiver Name` — имя узла-получателя конверта.

В случае отсутствия конвертов в очереди выводится сообщение `queue is empty`.

mftp show config

Просмотреть конфигурационный файл транспортного сервера MFTP.

Синтаксис

```
mftp show config
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Чтобы завершить просмотр конфигурационного файла, нажмите **Q**.

Пример использования

```
hostname> mftp show config
[channel]
id = 0x15ea0011
name = Client-1
off_flag = no
call_flag = no
type = MFTP
...
```

mftp start

Запустить службу `mftpd` (транспортный сервер MFTP).

Синтаксис

```
mftp start
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# mftp start
Loading MFTP daemon
..
```

mftp stop

Завершить работу службы `mftpd` (транспортный сервер MFTP).

Синтаксис

```
mftp stop
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# mftp stop
Shutting down MFTP daemon
```

Команды группы service

Настройка и управление прокси-сервером.

service cert delete

Удалить сертификат, список аннулированных сертификатов (CRL) или закрытый ключ.

Синтаксис

```
service cert delete {cert | crl | private} <pem>
```

Параметры и ключевые слова

- Тип удаляемого объекта:
  - `cert` — сертификат.
  - `crl` — список аннулированных сертификатов.
  - `private` — закрытый ключ.
- `<pem>` — имя файла сертификата, CRL или закрытого ключа соответственно.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При удалении из хранилища сертификата протокола HTTPS, который используется для доступа к ViPNet Coordinator HW с помощью веб-интерфейса, выводится предупреждение `After the command is executed, the HTTPS certificate will be deleted. WebUI will be switched to HTTP mode. Continue? Yes/No`. После подтверждения сертификат будет удален, протокол доступа к ViPNet Coordinator HW изменен на HTTP и выведено сообщение `Certificate for HTTPS deleted. The WebUI protocol is switched to HTTP`.
- Признак типов в PEM-файле:
  - Сертификат: `-----BEGIN CERTIFICATE-----`
  - CRL: `-----BEGIN X509 CRL-----`
  - Закрытый ключ: `-----BEGIN PRIVATE KEY-----`

Пример использования

- Чтобы удалить сертификат с именем `Cert1.pem`:

  ```
  hostname# service cert delete cert Cert1.pem
  ```

```
Certificate Cert1.pem is deleted
```

- Чтобы удалить CRL с именем `CRL1.pem`:

  ```
  hostname# service cert delete crl CRL1.pem
  CRL CRL1.pem is deleted
  ```

- Чтобы удалить закрытый ключ с именем файла `Cert1_key.pem`:

  ```
  hostname# service cert delete private Cert1_key.pem
  Private key Cert1_key.pem is deleted
  ```

service cert import

Импортировать в локальное хранилище ViPNet Coordinator HW закрытый ключ сертификата, сертификат или список аннулированных сертификатов (CRL) с USB-накопителя.

Синтаксис

```
service cert import
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Поддерживает импорт только сертификатов, подписанных с использованием алгоритма RSA.
- Поддерживает импорт сертификатов в кодировке DER и Base64.
- В контейнере PEM (`.pem`) используется стандарт PKCS#12 (`.p12`).
- По команде выполняется поиск на USB-накопителе файлов с расширениями `*.pem`, `*.cer` и `*.crl` и предлагается выбрать нужный сертификат, закрытый ключ сертификата или CRL.
- При импорте файлов с расширением `*.cer` и `*.crl` выполняется их конвертация в формат PEM.
- При импорте проверяется уникальность сертификата по содержимому и по имени:
  - Если имя и содержимое уникальны — сертификат импортируется, имя остается без изменения.
  - Если содержимое уникально, а имя нет — сертификат импортируется, к имени добавляется уникальный индекс (`<filename>_yyyy-mm-dd-hhmmss.<ext>`), об изменении имени файла выводится сообщение.
  - Если содержимое сертификата дублируется — сертификат не импортируется, выводится предупреждение о дублировании.

Пример использования

```
hostname# service cert import

Insert USB flash drive into empty USB slot and press <Enter>

Try to mount /dev/sdc1 as vfat

/dev/sdc1 mounted

1 - /usb/Cert1.cer

2 - /usb/CRL1.crl

Enter file number [1-2] or [q] to cancel: 1

Certificate /usb/Cert1.cer will be converted to PEM

Certificate:

...

/usb/Cert1.cer was imported as certnew.pem
```

service cert list

Просмотреть установленные закрытые ключи, сертификаты и списки аннулированных сертификатов (CRL).

Синтаксис

```
service cert list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service cert list

Certificates:

...

Certificate revocation list:

...

Private keys:

...
```

service cert request create

Создать закрытый ключ и запрос на сертификат в формате PKCS#12.

Синтаксис

```
service cert request create name <имя> bits <длина ключа> digest {sha256 | sha384 | sha512}
[subj <subj>]
```

Параметры и ключевые слова

- `<имя>` — имя сертификата;
- `<длина ключа>` — размер создаваемого RSA-ключа в битах, можно задавать следующие значения: 2048, 3072, 4096;
- `sha256` — алгоритм хэширования SHA-256;
- `sha384` — алгоритм хэширования SHA-384;
- `sha512` — алгоритм хэширования SHA-512;
- `subj` — дополнительные параметры запроса:
  - `/C` — страна;
  - `/ST` — область;
  - `/L` — город;
  - `/O` — организация;
  - `/OU` — отдел организации;
  - `/CN` — доменное имя сайта;
  - `/emailAddress` — электронный адрес;
  - `/subjectAltName` — альтернативные адреса ресурса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При выполнении команды в стандартном режиме необходимо следовать правилам заполнения параметров запроса:
  - Параметры запроса `subj` записываются единой строкой в двойных кавычках.
  - Названия полей параметров запроса отделяются от значений знаком `=`.
  - Пробелы между параметрами запроса не ставятся.
- Дополнительные параметры `subj` можно задавать в интерактивном режиме.

В процессе выполнения команды у вас будут запрошены личные данные, необходимые для создания сертификата. Не все поля обязательны к заполнению. Чтобы отказаться от заполнения тех или иных сведений, нажмите клавишу **Enter**.

- В контейнере PEM (`.pem`) используется стандарт PKCS#12 (`.p12`).
- По команде создается файл запроса на сертификат с именем `<имя сертификата>_req.pem` и файл с закрытым ключом с именем `<имя сертификата>_key.pem`.

Пример использования

Чтобы создать запрос на сертификат с длиной ключа 2048 бита, используя алгоритм шифрования SHA-256:

```
hostname# service cert request create name Cert1 bits 2048 digest sha256

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For same fields there will be a default value

If you enter '.', the field will be left blank.

If you want to create a certificate for the VPN network, fill in the CommonName and
AlternativeNames parameters.

Country Name (2 letter code) [AU]:DE

State or Province Name (full name) [Some-State]:

Locality Name (eg, city) []:Berlin

Organization Name (eg, company) [Internet Widgets Pty Ltd]:Company

Organizational Unit Name (eg, section) []:IT

Common Name (e.g. server FQDN or IP-address or domain name, one value) []:Company.de

Email Address []:post@co.de

Please enter the following 'extra' attributes

to be sent with your certificate request

An optional company name (e.g. server FQDN or IP-address or domain name, several value)
[]:Company.de

Generating a RSA private key

.....................................................................................
.................. ....+++++

.................................................+++++

writing new private key to '/etc/cert/Cert1_key.pem'

-----
```

```
Creating request Cert1_req.pem is completed
```

Чтобы создать запрос на сертификат с длиной ключа 2048 бита, используя алгоритм шифрования SHA-256 и дополнительные параметры запроса:

```
hostname# service cert request create name Cert1 bits 2048 digest sha256 subj
"/C=RU/ST=Moscow/L=Moscow/O=Infotecs/OU=IT/CN=infotecs.ru/emailAddress=post@infotecs.r
u/subjectAltName=DNS:infotecs.biz,IP:127.50.50.50"

Generating a RSA private key

...............................+++++

........+++++

writing new private key to '/etc/cert/Cert1_key.pem'

-----

Creating request Cert1_req.pem is completed
```

service cert request delete

Удалить запрос на сертификат.

Синтаксис

```
service cert request delete <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Признак запроса на сертификат в PEM файле: `-----BEGIN CERTIFICATE REQUEST-----`.

Пример использования

Чтобы удалить запрос на сертификат с именем `Cert1_req.pem`:

```
hostname# service cert request delete Cert1_req.pem

Certificate request Cert1_req.pem is deleted
```

service cert request export

Экспортировать запрос на сертификат на USB-накопитель.

Синтаксис

```
service cert request export <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Признак запроса на сертификат в PEM файле: `-----BEGIN CERTIFICATE REQUEST-----`.

Пример использования

Чтобы экспортировать запрос на сертификат с именем `Cert1_req.pem`:

```
hostname# service cert request export Cert1_req.pem
Insert USB flash drive into empty USB slot and press <Enter>
Try to mount /dev/sdc1 as vfat
/dev/sdc1 mounted
Cert1_req.pem was exported
```

service cert request list

Просмотреть список созданных запросов на сертификат.

Синтаксис

```
service cert request list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service cert request list

Cert1_req.pem
```

service cert request show

Просмотреть содержимое запроса на сертификат с заданным именем или всех запросов на сертификаты, созданных в ViPNet Coordinator HW.

Синтаксис

```
service cert request show <запрос>
```

Параметры и ключевые слова

`<запрос>` — имя файла запроса на сертификат. Если вместо имени указать `all`, будет отображено содержимое всех запросов на сертификаты, созданных в ViPNet Coordinator HW.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

Чтобы просмотреть содержимое файла запроса на сертификат с именем `Cert1_req.pem`:

```
hostname> service cert request show Cert1_req.pem

Certificate request:

    Data:

        ..

    Signature algorithm: md5WithRSAEncryption

        ..

...

(END)
```

service cert show cert

Просмотреть содержимое сертификата с заданным именем или всех сертификатов, установленных в локальное хранилище ViPNet Coordinator HW.

Синтаксис

```
service cert show cert <сертификат>
```

Параметры и ключевые слова

`<сертификат>` — имя файла сертификата. Если вместо имени сертификата указать `all`, то будет отображено содержимое всех сертификатов, установленных в локальное хранилище ViPNet Coordinator HW.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

Чтобы просмотреть содержимое сертификата с именем `Cert1.pem`:

```
hostname> service cert show cert Cert1.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            8c:93:38:27:1b:36:9c:be
    Signature Algorithm: sha256WithRSAEncryption
```

service cert show crl

Просмотреть содержимое списка аннулированных сертификатов (CRL) с заданным именем или всех списков аннулированных сертификатов, установленных в локальное хранилище ViPNet Coordinator HW.

Синтаксис

```
service cert show crl <CRL>
```

Параметры и ключевые слова

`<CRL>` — имя файла списка аннулированных сертификатов CRL. Если вместо имени CRL указать `all`, то будет отображено содержимое всех списков аннулированных сертификатов, установленных в локальное хранилище ViPNet Coordinator HW.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

Чтобы просмотреть содержимое списка аннулированных сертификатов с именем `CRL.pem`:

```
hostname> service cert show cert CRL.pem
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
```

service dpi mode

Включить или выключить автозапуск подсистемы DPI при перезагрузке ViPNet Coordinator HW.

Синтаксис

```
service dpi mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автозапуск.
- `off` — отключить автозапуск.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию автозапуск подсистемы DPI включен.
- После изменения текущего режима автозапуска необходимо перезагрузить ViPNet Coordinator HW.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Чтобы включать автозапуск подсистемы DPI:

```
hostname# service dpi mode on
```

```
The settings are saved. System must be restarted for the changes to take effect. Restart
now Y/N Y

reboot in progress
```

service dpi show status

Просмотреть текущие параметры подсистемы DPI.

Синтаксис

```
service dpi show status
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

При выполнении команды отображаются:

- состояние подсистемы DPI:
  - `DPI subsystem is on` — запущена;
  - `DPI subsystem is off` — остановлена;
  - `DPI subsystem is in service mode` — технологический режим;
- режим автозапуска подсистемы DPI:
  - `DPI subsystem autostart is on` — автозапуск включен;
  - `DPI subsystem autostart is off` — автозапуск отключен;
- версия подсистемы DPI в формате `YY.MM.DD`.

Пример использования

Чтобы просмотреть текущие параметры подсистемы DPI:

```
hostname> service dpi show status

DPI subsystem is on

DPI subsystem autostart is on

DPI version: 21.02.26
```

service dpi start

Запустить подсистему DPI.

Синтаксис

```
service dpi start
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию подсистема DPI запущена и выполняет классификацию протоколов, приложений и их групп.
- После выполнения команды ранее деактивированные сетевые фильтры, в параметрах которых указаны протоколы, приложения и их группы, будут активированы.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

Чтобы запустить подсистему DPI:

```
hostname# service dpi start
```

service dpi stop

Остановить работу подсистемы DPI.

Синтаксис

```
service dpi stop
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию подсистема DPI запущена и выполняет классификацию протоколов, приложений и их групп.
- После выполнения команды сетевые фильтры, в параметрах которых указаны протоколы, приложения и их группы, будут деактивированы.

- Команда не используется на пассивном узле кластера.

Пример использования

Чтобы остановить работу подсистемы DPI:

```
hostname# service dpi stop
```

service dpi update usb

Обновить подсистему DPI с USB-носителя.

Синтаксис

```
service dpi update usb
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Для обновления подсистемы DPI необходимо подключиться к ViPNet Coordinator HW с помощью консоли локально. Выполнить обновление в удаленной SSH-сессии невозможно.
- Для обновления подсистемы DPI необходим файл обновления: `<платформа ViPNet Coordinator HW>_vipnet_base_x86_64_<версия ViPNet Coordinator HW>_<версия DPI>_dpi.zip`, например, `hw1000_vipnet_base_x86_64_5.0_21.02.26_dpi.zip`.
- Файл обновления подсистемы DPI и файл ЭП обновления должны находиться в одном каталоге USB-носителя.
- Команда устанавливает глобальную блокировку управляющих запросов; сессии всех пользователей завершаются.
- После обновления подсистемы DPI необходимо перезагрузить ViPNet Coordinator HW.

Пример использования

```
hostname# service dpi update usb

During update, firewall will be stopped and all connections will be blocked. Are you sure
you want to continue? [Yes/No]: Y
Insert USB flash drive into empty USB slot and press <Enter>
Checking integrity of 'hw1000_vipnet_base_x86_64_5.0_21.02.26_dpi.zip'...
Select file to use for DPI update:
1 — /mnt/tmp/sdb1/hw1000_vipnet_base_x86_64_5.0_21.02.26_dpi.zip
Enter file number [1-1] or [q] to cancel: 1
Check file dpiimg.dat successfully
Check for enough main disk size
```

```
DPI is upgrading and system will be rebooted in progress.
```

service http-proxy antivirus bypass

Включить или выключить блокировку трафика, проходящего через прокси-сервер при недоступности ICAP-сервера внешнего антивируса.

Синтаксис

```
service http-proxy antivirus bypass {on | off}
```

Параметры и ключевые слова

- `on` — при недоступности ICAP-сервера внешнего антивируса прокси-сервер разрешает проходящий через него трафик.
- `off` — при недоступности ICAP-сервера внешнего антивируса прокси-сервер блокирует проходящий через него трафик.

Значения по умолчанию

`on`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды:
  - выключите антивирусную проверку (см. service http-proxy antivirus mode);
  - остановите прокси-сервер (см. service http-proxy stop).
- Команду нельзя выполнить, пока не задан адрес и метод подключения к ICAP-серверу.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# service http-proxy antivirus bypass on

HTTP proxy antivirus set bypass option: on
```

service http-proxy antivirus mode

Включить или выключить антивирусную проверку трафика, проходящего через прокси-сервер.

Синтаксис

```
service http-proxy antivirus mode {on | off}
```

Параметры и ключевые слова

- `on` — антивирусная проверка трафика включена.
- `off` — антивирусная проверка трафика выключена.

Значения по умолчанию

`off`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- Команду можно выполнить, если заданы параметры ICAP-сервера. После выполнения команды проверяются настроенные URL для ICAP-сервера (URL, порт, метод).

Пример использования

```
hostname# service http-proxy antivirus mode off

HTTP proxy antivirus mode is disabled
```

service http-proxy antivirus server-url add

Задать адрес и метод подключения к ICAP-серверу внешнего антивируса.

Синтаксис

```
service http-proxy antivirus server-url add {reqmod | respmod} <URL>
```

Параметры и ключевые слова

- `reqmod` — проверяется исходящий трафик (запросы от пользователей сети к прокси-серверу);
- `respmod` — проверяется входящий трафик (ответы прокси-сервера на запросы пользователей);
- `<URL>` — адрес ICAP-сервера антивируса в формате `icap://адрес[:порт]/<путь>`.

Значения по умолчанию

Если в адресе ICAP-сервера не указан порт, будет использоваться порт по умолчанию 1344.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# service http-proxy antivirus server-url add respmod icap://192.168.1.45/respmod
HTTP proxy antivirus add respmod service success
```

service http-proxy antivirus server-url delete

Удалить параметры подключения к ICAP-серверу внешнего антивируса.

Синтаксис

```
service http-proxy antivirus server-url delete {reqmod | respmod}
```

Параметры и ключевые слова

- `reqmod` — будет удален адрес доступа к ICAP-серверу для проверки исходящего трафика (запросы от пользователей сети к прокси-серверу);
- `respmod` — будет удален адрес доступа к ICAP-серверу для проверки входящего трафика (ответы прокси-сервера на запросы пользователей).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды:
  - выключите антивирусную проверку (см. service http-proxy antivirus mode);
  - остановите прокси-сервер (см. service http-proxy stop).
- Команду нельзя выполнить, пока не задан адрес и метод подключения к ICAP-серверу.
- В кластере команда доступна для выполнения на активном узле.

Пример использования

```
hostname# service http-proxy antivirus server-url delete respmod
```

```
HTTP proxy antivirus delete respmod service success
```

service http-proxy antivirus server-url list

Просмотреть текущие настройки доступа к ICAP-серверу антивируса.

Синтаксис

```
service http-proxy antivirus server-url list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service http-proxy antivirus server-url list
HTTP proxy antivirus server-url address: icap://192.168.1.45:1344/reqmod, method reqmod
HTTP proxy antivirus server-url address: icap://192.168.1.45:1344/respmod, method respmod
```

service http-proxy antivirus show-status

Просмотреть текущие настройки и состояние антивирусной защиты.

Синтаксис

```
service http-proxy antivirus show-status
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В кластере команда доступна для выполнения на обоих узлах.

Пример использования

```
hostname> service http-proxy antivirus show-status
Probing connection with I-CAP server, please be patient...
HTTP proxy antivirus mode is disabled
```

```
HTTP proxy antivirus bypass is on
HTTP proxy antivirus reqmod server-url: icap://192.168.1.45:1344/reqmod is offline
HTTP proxy antivirus respmod server-url: icap://192.168.1.45:1344/respmod is offline
```

service http-proxy cache

Задать размер кеша прокси-сервера.

Синтаксис

```
service http-proxy cache <размер>
```

Параметры и ключевые слова

`<размер>` — размер кеша в мегабайтах.

Значения по умолчанию

- для однодисковых платформ — 100 Мбайт;
- для остальных платформ — 256 Мбайт.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Кеш используется для хранения копии данных, к которым часто обращаются пользователи.
- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- Для однодисковых платформ размер кеша не может превышать 100 Мбайт.
- Невозможно задать размер кеша, превышающий 80% от объема свободного места на диске.

Пример использования

Чтобы задать размер кеша 512 мегабайт:

```
hostname# service http-proxy cache 512
```

service http-proxy content-filter add

Добавить правило контент-фильтрации.

Синтаксис

```
service http-proxy content-filter add [num <номер>] [rule <имя>] src <адрес отправителя>
dst <адрес получателя> {command <HTTP-метод> | mime-type <mime-тип>} <действие>
```

Параметры и ключевые слова

- `<номер>` — порядковый номер правила в таблице, определяющий его приоритет.
- `<имя>` — имя правила.
- `<адрес отправителя>` — адрес отправителя IP-пакетов.
- `<адрес получателя>` — адрес получателя IP-пакетов.
- `<HTTP-метод>` — метод протокола HTTP. Значение необходимо вводить в верхнем регистре, например `GET`.
- `<mime-тип>` — MIME-тип.
- `<действие>` — действие с HTTP-трафиком, соответствующим условиям правила контент-фильтрации:
  - `pass` — пропускать HTTP-трафик;
  - `drop` — блокировать HTTP-трафик.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- В качестве адреса отправителя задавайте адрес клиента прокси-сервера, в качестве получателя — адрес удаленного HTTP-сервера.
- Если номер не указан, правило добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика в последнюю очередь.
- Если указанный номер правила меньше последнего номера в таблице, нумерация правил, следующих после нового правила, будет автоматически изменена (их номера будут увеличены на 1). Например: последний номер правила в таблице — 5, вы добавили правило с номером 3. Правило добавится с указанным номером, при этом правило с номером 3, которое было создано ранее добавленного вами, получит номер 4. Правила с номерами 4 и 5, соответственно, получат номер 5 и 6.
- Если указанный номер правила больше последнего номера в таблице, то правило будет добавлено с номером на 1 больше последнего номера в таблице. Например: последний номер правила в таблице — 5, вы добавили правило с номером 8. В этом случае правило добавится с номером 6.
- Если имя правила не задано, будет создано правило без имени.

- В качестве адреса отправителя можно задать IP-адрес узла, маску адресов подсети, системную группу объектов `any`.
- В качестве адреса получателя можно задать IP-адрес или доменное имя узла, системную группу объектов `any`.

  Правило контент-фильтрации работает на прикладном уровне модели OSI. Поэтому при использовании в качестве адреса назначения доменного имени узла фильтрация будет осуществляться только по доменному имени, а при использовании IP-адреса узла — только по IP-адресу (без взаимного разрешения доменное имя — IP-адрес).
- Можно задать только один из параметров: `<HTTP-метод>` или `<mime-тип>`. При указании HTTP-метода нельзя указать MIME-тип, и наоборот.
- При неверном указании значения параметра `<mime-тип>` выводится полный список поддерживаемых значений.
- Для блокировки сайта задайте HTTP-метод `GET`.

Пример использования

- Чтобы заблокировать просмотр видео на сайте youtube.com для сети 192.168.1.1/24:

  ```
  hostname# service http-proxy content-filter add rule deny_youtube src 192.168.1.1/24 dst youtube.com mime-type video/mp4 drop
  ```
- Чтобы заблокировать использование поисковой формы на сайте yandex.ru для всех пользователей:

  ```
  hostname# service http-proxy content-filter add rule deny_post_yandex src @any dst yandex.ru command POST drop
  ```
- Чтобы полностью заблокировать доступ к сайту yandex.ru:

  ```
  hostname# service http-proxy content-filter add rule deny_yandex src @any dst yandex.ru command GET drop
  ```

service http-proxy content-filter change num

Редактировать правило контент-фильтрации.

Синтаксис

```
service http-proxy content-filter change num <номер правила> [rule <имя правила>] src <адрес отправителя> dst <адрес получателя> {command <HTTP-метод> | mime-type <mime-тип>} <действие>
```

Параметры и ключевые слова

- `<номер правила>` — номер редактируемого правила в таблице;
- `<имя правила>` — имя редактируемого правила фильтрации трафика;
- `<адрес отправителя>` — адрес отправителя IP-пакетов;

- `<адрес отправителя>` — адрес получателя IP-пакетов;
- `<HTTP-метод>` — метод протокола HTTP;
- `<mime-тип>` — MIME-тип;
- `<действие>` — действие с HTTP-трафиком, соответствующим условиям правила контент-фильтрации:
  - `pass` — пропускать HTTP-трафик;
  - `drop` — блокировать HTTP-трафик.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- В качестве адреса отправителя задайте адрес клиента прокси-сервера, в качестве получателя — адрес удаленного HTTP-сервера.
- Если номер не указан, правило добавляется в конец соответствующей таблицы и будет применяться при анализе IP-трафика в последнюю очередь.
- Если указанный номер правила меньше последнего номера в таблице, нумерация правил, следующих после нового правила, будет автоматически изменена (их номера будут увеличены на 1). Например: последний номер правила в таблице — 5, вы добавили правило с номером 3. Правило добавится с указанным номером, при этом правило с номером 3, которое было создано ранее добавленного вами, получит номер 4. Правила с номерами 4 и 5, соответственно, получат номер 5 и 6.
- Если указанный номер правила больше последнего номера в таблице, то правило будет добавлено с номером на 1 больше последнего номера в таблице. Например: последний номер правила в таблице — 5, вы добавили правило с номером 8. В этом случае правило добавится с номером 6.
- Если имя правила не задано, будет создано правило без имени.
- В качестве адреса отправителя можно задать IP-адрес узла, маску адресов подсети, системную группу объектов `any`.
- В качестве адреса получателя можно задать IP-адрес или доменное имя узла, системную группу объектов `any`.

  Правило контент-фильтрации прокси-сервера работает на прикладном уровне модели OSI. Поэтому при использовании в качестве адреса назначения доменного имени узла фильтрация будет осуществляться только по доменному имени, а при использовании IP-адреса узла, только по IP-адресу, без взаимного разрешения доменное имя — IP-адрес.
- Можно задать только один из параметров: `<HTTP-метод>` или `<mime-тип>`. При указании HTTP-метода нельзя указать MIME-тип, и наоборот.

- При неверном указании значения параметра `<mime-тип>` выводится полный список поддерживаемых значений.
- Для блокировки сайта задайте HTTP-метод `GET`.

Пример использования

Предположим, в таблице существует правило без имени с номером 15, которое полностью блокирует доступ к сайту yandex.ru для всех пользователей сети. Вы можете изменить имя блокируемого ресурса, например на google.com, выполнив команду:

```
hostname# service http-proxy content-filter change num 15 src @any dst google.com command GET drop
```

service http-proxy content-filter default-reply-action

Задать действие по умолчанию для ответов от HTTP-ресурсов, которые не подошли под условия других правил контент-фильтрации.

Синтаксис

```
service http-proxy content-filter default-reply-action <действие>
```

Параметры и ключевые слова

`<действие>` — действие с ответами от HTTP-ресурсов:

- `pass` — пропускать;
- `drop` — блокировать.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию ответы от HTTP-ресурсов пропускаются.
- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).

Пример использования

```
hostname# service http-proxy content-filter default-reply-action drop

Set default-reply-action to drop
```

service http-proxy content-filter default-request-action

Задать действие по умолчанию для запросов к HTTP-ресурсам, которые не подошли под условия других правил контент-фильтрации.

Синтаксис

```
service http-proxy content-filter default-request-action <действие>
```

Параметры и ключевые слова

`<действие>` — действие с запросами к HTTP-ресурсам:

- `pass` — пропускать;
- `drop` — блокировать.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию запросы к HTTP-ресурсам пропускаются.
- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).

Пример использования

```
hostname# service http-proxy content-filter default-request-action drop
Set default-request-action to drop
```

service http-proxy content-filter delete

Удалить правило контент-фильтрации.

Синтаксис

```
service http-proxy content-filter delete {num <номер> | rule <имя>}
```

Параметры и ключевые слова

- `<номер>` — порядковый номер правила в таблице.
- `<имя>` — имя правила.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).

Пример использования

- Чтобы удалить правило с именем `deny_youtube`:

  ```
  hostname# service http-proxy content-filter delete rule deny_youtube
  ```

- Чтобы удалить правило с порядковым номером 5:

  ```
  hostname# service http-proxy content-filter delete num 5
  ```

service http-proxy content-filter list

Просмотреть список правил контент-фильтрации.

Синтаксис

```
service http-proxy content-filter list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service http-proxy content-filter list
Content filter rules
============================
       num          1
       act          drop
       name         rule1
       src          @any
       dst          @any
       mime-type    image/jpeg
       num          2
       act          drop
```

```
name          rule2
src           @any
dst           @any
mime-type     image/png
```

service http-proxy content-filter mode

Включить или выключить контент-фильтрацию HTTP-трафика.

Синтаксис

```
service http-proxy content-filter mode {on | off}
```

Параметры и ключевые слова

- `on` — включить контент-фильтрацию.
- `off` — выключить контент-фильтрацию.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию контент-фильтрация включена.
- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- Контент-фильтрация трафика работает при запущенном прокси-сервере (см. service http-proxy start).

Пример использования

Чтобы включить контент-фильтрацию трафика:

```
hostname# service http-proxy content-filter mode on
```

service http-proxy content-filter move

Изменить порядковый номер правила контент-фильтрации.

Синтаксис

```
service http-proxy content-filter move {num <номер> | rule <имя>} to <новый номер>
```

Параметры и ключевые слова

- `<номер>` — порядковый номер правила в таблице.
- `<имя>` — имя правила.
- `<новый номер>` — новый порядковый номер правила.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).

Пример использования

- Чтобы назначить новый порядковый номер правилу с именем `deny_youtube`:

  ```
  hostname# service http-proxy content-filter move rule deny_youtube to 7
  ```

- Чтобы назначить новый порядковый номер правилу с порядковым номером 5:

  ```
  hostname# service http-proxy content-filter move num 5 to 7
  ```

service http-proxy content-filter show-status

Просмотреть информацию о статусе контент-фильтрации трафика.

Синтаксис

```
service http-proxy content-filter show-status
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service http-proxy content-filter show-status
HTTP-proxy content-filter is enabled with 4 rules
HTTP-proxy content-filter default-request-action is pass
HTTP-proxy content-filter default-reply-action is pass
HTTP-proxy service is stopped
```

service http-proxy external-address set

Задать внешний IP-адрес прокси-сервера.

Синтаксис

```
service http-proxy external-address set <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса, подключенного к интернету.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- При вводе интерфейса работает подсказка. Данные для нее берутся из списка интерфейсов в системе (включая виртуальные интерфейсы, созданные при назначении дополнительных IP-адресов основным интерфейсам).
- На указанном интерфейсе должен быть задан IP-адрес.

Пример использования

Чтобы задать IP-адрес интерфейса `eth1` в качестве внешнего адреса прокси-сервера:

```
hostname# service http-proxy external-address set eth1
```

service http-proxy external-address show

Просмотреть внешний IP-адрес прокси-сервера.

Синтаксис

```
service http-proxy external-address show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service http-proxy external-address show

External address: 10.0.14.110 (eth0)
```

service http-proxy fw-rules apply

Сгенерировать сетевые фильтры и правила трансляции адресов, соответствующие текущим настройкам прокси-сервера.

Синтаксис

```
service http-proxy fw-rules apply
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Невозможно создать сетевые фильтры и правила трансляции, если заданы не все параметры прокси-сервера.
- Автоматически созданные фильтры и правила трансляции добавляются в конец соответствующих таблиц и имеют зарезервированное название HTTP-Proxy auto.
- Редактировать созданные сетевые фильтры и правила трансляции не рекомендуется.
- Предыдущие сетевые фильтры и правила трансляции, соответствующие измененным настройкам прокси-сервера, будут удалены.

Пример использования

Чтобы после настройки прокси-сервера создать необходимые сетевые фильтры и правила трансляции:

```
hostname# service http-proxy fw-rules apply
```

service http-proxy fw-rules delete

Удалить сетевые фильтры и правила трансляции адресов, необходимые для работы прокси-сервера.

Синтаксис

```
service http-proxy fw-rules delete
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

По команде из соответствующих таблиц будут удалены сетевые фильтры и правила трансляции с названием HTTP-Proxy auto, автоматически созданные с помощью команды service http-proxy fw-rules apply.

Пример использования

Чтобы удалить имеющиеся сетевые фильтры и правила трансляции, автоматически созданные для работы прокси-сервера:

```
hostname# service http-proxy fw-rules delete
```

service http-proxy fw-rules show

Просмотреть существующие сетевые фильтры и правила трансляции адресов, необходимые для работы прокси-сервера.

Синтаксис

```
service http-proxy fw-rules show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service http-proxy fw-rules show
Local:
================================================================================
Num   Name                                          Option        Schedule
Act   Protocol                 Source               > Destination
================================================================================
11    HTTP-Proxy auto                                 User
pass  tcp:                     @HttpProxyUsers      > 169.254.241.1
       to 1024
--------------------------------------------------------------------------------
12    HTTP-Proxy auto                                 User
pass  tcp:                     192.168.1.1        > @InternetIP
       to 80,
      tcp:
```

```
       to 21,
      tcp:
       to 443
--------------------------------------------------------------------------------
```

service http-proxy listen-address add

Добавить интерфейс и порт, через которые будут приниматься запросы от клиентов прокси-сервера.

Синтаксис

```
service http-proxy listen-address add <интерфейс> <порт>
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `<порт>` — номер порта.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- При вводе интерфейса работает подсказка, данные для подсказки берутся из списка интерфейсов в системе (включая виртуальные интерфейсы, созданные при назначении дополнительных IP-адресов основным интерфейсам).
- На указанном интерфейсе должен быть задан IP-адрес.
- Разрешено задавать номер порта, который не используется другими службами.

Пример использования

Чтобы указать интерфейс `eth1` и номер порта 6789 для приема запросов от клиентов прокси-сервера:

```
hostname# service http-proxy listen-address add eth1 6789
```

service http-proxy listen-address delete

Удалить интерфейс из списка слушающих интерфейсов прокси-сервера.

Синтаксис

```
service http-proxy listen-address delete <интерфейс>
```

Параметры и ключевые слова

`<интерфейс>` — имя интерфейса.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из текущего списка прослушивания.

Пример использования

Чтобы удалить интерфейс `eth1` из списка интерфейсов, по которым принимаются запросы от клиентов прокси-сервера:

```
hostname# service http-proxy listen-address delete eth1
```

service http-proxy listen-address list

Просмотреть текущий список адресов интерфейсов и портов, через которые принимаются запросы от клиентов прокси-сервера.

Синтаксис

```
service http-proxy listen-address list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service http-proxy listen-address list
Listen:
10.0.14.110:6789 (eth0)
```

service http-proxy mode

Включить или выключить автоматический запуск прокси-сервера при загрузке ViPNet Coordinator HW.

Синтаксис

```
service http-proxy mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматический запуск.
- `off` — выключить автоматический запуск.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию автоматический запуск прокси-сервера выключен.
- По команде изменяется только настройка автоматического запуска прокси-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск, если заданы не все параметры, необходимые для работы прокси-сервера.

Пример использования

Чтобы выключить автоматический запуск прокси-сервера:

```
hostname# service http-proxy mode off
```

service http-proxy reset

Сбросить текущие настройки прокси-сервера.

Синтаксис

```
service http-proxy reset
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При выполнении команды запрашивается подтверждение очистки всех настроек прокси-сервера.
- При выполнении команды не удаляются сетевые фильтры и правила трансляции адресов, если такие создавались в соответствии с текущими настройками прокси-сервера с помощью команды service http-proxy fw-rules apply. После очистки настроек прокси-сервера данные фильтры и правила трансляции можно удалить вручную с помощью команды service http-proxy fw-rules delete.

Пример использования

Чтобы очистить настройки прокси-сервера:

```
hostname# service http-proxy reset
```

service http-proxy show

Просмотреть состояние и настройки прокси-сервера.

Синтаксис

```
service http-proxy show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service http-proxy show
HTTP Proxy autostart is on
Service is running
Transparent: on
Cache size: 256
Listen:
169.254.241.1:6789 (eth1)
External address: 10.0.14.110 (eth0)
```

service http-proxy start

Запустить прокси-сервер.

Синтаксис

```
service http-proxy start
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Невозможно запустить прокси-сервер, если заданы не все параметры, необходимые для его работы.

Пример использования

```
hostname# service http-proxy start
HTTP Proxy started
```

service http-proxy stop

Завершить работу прокси-сервера.

Синтаксис

```
service http-proxy stop
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service http-proxy stop
HTTP Proxy stopped
```

service http-proxy transparent-mode

Включить или выключить «прозрачный» режим работы прокси-сервера.

Синтаксис

```
service http-proxy transparent-mode {on | off}
```

Параметры и ключевые слова

- `on` — включить прозрачный режим.

- `off` — выключить прозрачный режим.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию «прозрачный» режим выключен.
- Перед выполнением команды завершите работу прокси-сервера (см. service http-proxy stop).
- Невозможно включить «прозрачный» режим, если заданы не все параметры, необходимые для работы прокси-сервера.
- При работе прокси-сервера в «прозрачном» режиме настройка на рабочих местах пользователей не требуется.

Пример использования

Чтобы включить «прозрачный» режим работы прокси-сервера:

```
hostname# service http-proxy transparent-mode on
```

service ips start

Включить предотвращение вторжений (IPS).

Синтаксис

```
service ips start
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

На время выполнения команды трафик блокируется межсетевым экраном ViPNet Coordinator HW, активные соединения принудительно закрываются.

Пример использования

Чтобы включить предотвращение вторжений:

```
hostname# service ips start
```

service ips stop

Выключить предотвращение вторжений (IPS).

Синтаксис

```
service ips stop
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- На время выполнения команды трафик блокируется межсетевым экраном ViPNet Coordinator HW, активные соединения принудительно закрываются.
- После выполнения команды ранее настроенные параметры предотвращения вторжений (IPS) сохраняются и будут применены при повторном включении предотвращения вторжений.

Пример использования

Чтобы выключить предотвращение вторжений:

```
hostname# service ips stop
```

service ips mode

Включить или выключить автоматический запуск предотвращения вторжений (IPS) при загрузке ViPNet Coordinator HW.

Синтаксис

```
service ips mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматический запуск IPS.
- `off` — выключить автоматический запуск IPS.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию автоматический запуск IPS включен (`on`).

- Чтобы применить изменение, перезагрузите ViPNet Coordinator HW.

Пример использования

Чтобы включить автоматический запуск IPS при загрузке ViPNet Coordinator HW:

```
hostname# service ips mode on

The settings are saved. System must be restarted for the changes to take effect. Restart now? Y/N
```

service ips rule restore-default

Восстановить базу правил IPS до версии, поставляемой в составе дистрибутива ViPNet Coordinator HW.

Синтаксис

```
service ips rule restore-default
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При выполнении команды запрашивается подтверждение восстановления базы правил IPS.
- После выполнения команды:
  - Будут сохранены ранее сделанные настройки обновления с сервера (адрес сервера обновлений, имя и пароль пользователя, расписание).
  - Автоматическое обновление базы правил IPS с сервера будет выключено.
  - Ранее сделанные настройки правил IPS (действие правила, комментарии и параметры правил) устанавливаются в состояние по умолчанию.

Пример использования

Чтобы восстановить базу правил IPS до версии, поставляемой в составе дистрибутива ViPNet Coordinator HW:

```
hostname# service ips rule restore-default

All IPS settings will be reset. Continue? [Yes,No]:Y

Restoring default rules...done.
```

service ips rule update

Включить или выключить автоматическое обновление базы правил предотвращения вторжения (правил IPS) по расписанию.

Синтаксис

```
service ips rule update {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматическое обновление базы правил IPS.
- `off` — выключить автоматическое обновление базы правил IPS.

Значения по умолчанию

Автоматическое обновление базы правил IPS выключено (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- До включения автоматического обновления базы правил IPS необходимо настроить имя пользователя (см. service ips rule update server login) и пароль пользователя (см. service ips rule update server password) для доступа на сервер обновлений. В случае, если имя пользователя и пароль пользователя не заданы, выводится сообщение о невозможности включить автоматическое обновление правил IPS.
- При обновлении базы правил IPS обработка трафика не прерывается.

Пример использования

Чтобы включить автоматическое обновление базы правил IPS по расписанию:

```
hostname# service ips rule update on
```

service ips rule update fetch

Обновить вручную базу правил предотвращения вторжений (правил IPS) с сервера обновлений.

Синтаксис

```
service ips rule update fetch
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- До выполнения обновления базы правил IPS необходимо настроить имя пользователя (см. service ips rule update server login) и пароль пользователя (см. service ips rule update server password) для доступа к серверу обновлений и проверить доступность сервера обновлений. В случае, если имя пользователя и пароль пользователя не заданы или сервер обновлений недоступен, выводится сообщение о невозможности выполнить обновление базы правил IPS.
- При обновлении базы правил IPS обработка трафика не прерывается.

Пример использования

Чтобы обновить базу правил IPS, не дожидаясь обновления по расписанию:

```
hostname# service ips rule update fetch
```

service ips rule update server proxy address

Задать адрес прокси-сервера, используемого при подключении к серверу обновлений базы правил IPS.

Синтаксис

```
service ips rule update server proxy address {<адрес прокси-сервера> | none}
```

Параметры и ключевые слова

- `<адрес прокси-сервера>` — IP-адрес или доменное имя прокси-сервера.
- `none` — не использовать прокси-сервер.

Значения по умолчанию

Прокси-сервер не используется (`none`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Для связи с прокси-сервером необходимо добавить разрешающее правило межсетевого экрана.

Пример использования

Чтобы использовать прокси-сервер `proxy.company.org`:

```
hostname# service ips rule update server proxy address proxy.company.org
```

service ips rule update server proxy port

Задать TCP-порт прокси-сервера, используемого при подключении к серверу обновлений базы правил IPS.

Синтаксис

```
service ips rule update server proxy port <порт>
```

Параметры и ключевые слова

`<порт>` — TCP-порт прокси-сервера.

Значения по умолчанию

Используется TCP-порт 3128.

Режимы командного интерпретатора

Режим настройки

Пример использования

Чтобы задать TCP-порт 8000:

```
hostname# service ips rule update server proxy port 8000
```

service ips rule update schedule

Настроить расписание автоматического обновления базы правил предотвращения вторжений (правил IPS).

Синтаксис

```
service ips rule update schedule {daily at <время> | weekly on <день> at <время>}
```

Параметры и ключевые слова

- `daily at <время>` — ежедневное обновление в указанное время. Параметр `<время>` задается в формате `hh:mm`, где `hh` — часы (24-часовой формат), `mm` — минуты.

- `weekly on <день> at <время>` — еженедельное обновление в указанные день и время. Параметры `<день>` и `<время>` задаются в форматах:
  - `<день>`: `sunday`, `monday`, `tuesday`, `wednesday`, `thursday`, `friday`, `saturday`.
  - `<время>`: `hh:mm`, где `hh` — часы (24-часовой формат), `mm` — минуты.

Значения по умолчанию

Периодичность обновления базы правил IPS — ежедневно, время обновления выбирается случайным образом.

Режимы командного интерпретатора

Режим настройки.

Примеры использования

Чтобы настроить ежедневное обновление базы правил IPS в 8 часов 15 минут:

```
hostname# service ips rule update schedule daily at 8:15
```

Чтобы настроить еженедельное обновление базы правил IPS по понедельникам, в 8 часов 15 минут:

```
hostname# service ips rule update schedule weekly on monday at 8:15
```

service ips rule update server address

Задать адрес сервера обновлений базы правил IPS.

Синтаксис

```
service ips rule update server address <адрес сервера>
```

Параметры и ключевые слова

`<адрес сервера>` — IP-адрес или доменное имя сервера обновлений базы правил IPS.

Значения по умолчанию

DNS-имя

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В доменном имени сервера обновлений разрешено использовать только символы латинского алфавита.

Пример использования

Чтобы использовать для обновления базы правил IPS сервер `10.0.7.72`:

```
hostname# service ips rule update proxy address 10.0.7.72
```

service ips rule update server login

Задать имя пользователя для доступа к серверу обновлений базы правил предотвращения вторжений (правил IPS).

Синтаксис

```
service ips rule update server login <имя пользователя>
```

Параметры и ключевые слова

`<имя пользователя>` — имя пользователя для доступа к серверу обновлений базы правил IPS. Файл с именем и паролем пользователя для доступа к серверу обновлений входит в комплект поставки ViPNet Coordinator HW.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы задать имя пользователя `User2019` для доступа к серверу обновлений базы правил IPS:

```
hostname# service ips rule update server login User2019
```

service ips rule update server password

Задать пароль пользователя для доступа к серверу обновлений базы правил предотвращения вторжений (правил IPS).

Синтаксис

```
service ips rule update server password
```

Параметры и ключевые слова

`<пароль>` — пароль пользователя для доступа к серверу обновлений базы правил IPS. Файл с именем и паролем пользователя для доступа к серверу обновлений входит в комплект поставки ViPNet Coordinator HW.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Пароль задается в интерактивном режиме, символы при вводе не отображаются.

Пример использования

Чтобы задать пароль пользователя для доступа к серверу обновлений базы правил IPS:

```
hostname# service ips rule update server password
Enter password for ips remote server:
```

service ips rule update usb

Обновить базу правил IPS с USB-носителя.

Синтаксис

```
hostname# service ips rule update usb
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Для обновления подсистемы IPS необходимы:
  - файл обновления базы правил IPS, например `rules.20210618-104906_eac_ver.hw-5.0.tgz`;
  - файл ЭП обновления `rules.20210618-104906_eac_ver.hw-5.0.tgz.sig`.
- Файл обновления базы правил IPS и файл ЭП обновления должны находиться в одном каталоге USB-носителя.
- При обновлении базы правил IPS обработка трафика не прерывается.

Пример использования

```
hostname# service ips rule update usb
```

```
Insert USB flash drive into empty USB slot and press <Enter>


Select file to use for updating IPS rules:
1 - /sdc1/rules.20210618-104906_eac_ver.hw-5.0.tgz
Enter file number [1-1] or [q] to cancel: 1
IPS updated successfully.
```

service ips show status

Просмотреть параметры системы предотвращения вторжений IPS.

Синтаксис

```
service ips show status
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

При выполнении команды отображается следующая информация:

- состояние системы предотвращения вторжений:
  - `IPS subsystem is in service mode` — технологический режим;
  - `IPS subsystem is off` — выключено;
  - `IPS subsystem is on` — включено;
  - `IPS subsystem is on and updating` — включено и выполняется обновление базы правил IPS;
- автоматический запуск системы предотвращения вторжений при перезапуске ViPNet Coordinator HW:
  - `autostart is on` — разрешено;
  - `autostart is off` — запрещено;
- ошибки системы предотвращения вторжений (строка выводится, если есть ошибки в работе предотвращения вторжений);
- уровень важности событий предотвращения вторжений, регистрируемых в системном журнале ViPNet Coordinator HW;
- дата и время создания текущей базы правил IPS;

- статус (успешно или не успешно), дата и время последнего обновления текущей базы правил IPS.

Пример использования

Чтобы просмотреть параметры предотвращения вторжений:

```
hostname> service ips show status

IPS subsystem is on

IPS subsystem autostart is on

Current syslog level is 3-info and higher

Current IPS rules database 2024-02-10 16:35:22

IPS rules database updated 2024-02-25 13:13:47
```

service ips show update-settings

Просмотр текущих параметров обновления базы правил IPS.

Синтаксис

```
service ips show update-settings
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

При выполнении команды отображается следующая информация:

- автоматическое обновление базы правил IPS (включено или выключено);
- расписание обновления базы правил IPS (периодичность и время обновления);
- адрес сервера обновлений базы правил IPS (DNS-имя или IP-адрес);
- имя пользователя для доступа к серверу обновлений базы правил IPS;
- статус пароля пользователя (установлен или не установлен);
- при подключении к серверу обновлений через прокси-сервер:
  - адрес прокси-сервера (IP-адрес или DNS-имя);
  - порт прокси-сервера;
  - статус подключения к прокси-серверу;
- срок истечения лицензии обновления базы правил IPS;

- идентификатор лицензии IPS.

Пример использования

```
hostname> service ips show update-settings

IPS rules database remote update: on

Database updates daily at 01:01

Update server:

  Address: updateids.infotecs.ru

  Login: user2021

  Password: specified

Update proxy-server:

  Address: proxy.gov.ru

  Port: 3128

   Status: unavailable

IPS rules update license expiration date: 2024-10-14 13:12:11

IPS license ID: 746k-l3s2
```

service ips syslog-level

Задать уровень важности событий предотвращения вторжений (IPS), записываемых в системный журнал ViPNet Coordinator HW.

Синтаксис

```
service ips syslog-level <уровень важности>
```

Параметры и ключевые слова

`<уровень важности>` — число от 0 до 5 по убыванию степени важности, соответствующее уровням событий:

- 0 — критические события;
- 1 — ошибки;
- 2 — предупреждения;
- 3 — информационные события;
- 4 — отладочные события;
- 5 — детализированные отладочные события.

Значения по умолчанию

Задан уровень событий — 3. При этом в системном журнале ViPNet Coordinator HW регистрируются:

- 0 — критические события;
- 1 — ошибки;
- 2 — предупреждения;
- 3 — информационные события.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Уровни важности событий IPS, записываемых в системный журнал ViPNet Coordinator HW, входят в три группы, включающие следующие уровни важности:

- 0, 1, 2;
- 3;
- 4, 5.

Если уровень изменяется на значение из другой группы событий, необходимо перезапустить IPS. При этом будет выведено сообщение с предложением немедленного перезапуска IPS:

```
IPS logging level will change upon IPS restart. IPS will restart now. [y/n]
```

- `y` — выполняется немедленный перезапуск IPS, устанавливается новый уровень важности;
- `n` — текущий уровень важности сохраняется до перезапуска IPS, после которого будет установлен новый уровень важности.

При изменении уровня важности на значение из той же группы, перезапуск IPS не требуется.

Пример использования

Предположим, что в ViPNet Coordinator HW установлен уровень важности событий IPS по умолчанию (`3`). Чтобы в системный журнал ViPNet Coordinator HW записывались события до 4-го уровня включительно (критические, ошибки, предупреждения, информационные и отладочные), установите уровень важности `4` и выполните немедленный перезапуск IPS:

```
hostname# service ips syslog-level 4
IPS logging level will change upon IPS restart. IPS will restart now. Continue? [y/n]: y
```

service user-control

Запустить или остановить работу службы управления пользователями (`uc`).

Синтаксис

```
service user-control {start | stop}
```

Параметры и ключевые слова

- `start` — запустить службу `uc`.
- `stop` — остановить работу службы `uc`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию работа службы `uc` остановлена.
- После запуска службы `uc` все сетевые пакеты неавторизованных пользователей будут блокироваться, даже если созданы разрешающие сетевые фильтры.

Пример использования

```
hostname# service user-control start
Starting uc.sh: uc.
```

service user-control active-users

Просмотреть информацию о текущих сессиях пользователей Active Directory и Captive portal.

Синтаксис

```
service user-control active-users
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В результате выполнения команды отображается список пользователей в формате:

<имя пользователя> <ip-адрес> {<метка времени>| 0}, где:

- <имя пользователя> — имя зарегистрированного пользователя Active Directory и Captive portal.
- <ip-адрес> — IP-адрес зарегистрированного пользователя Active Directory и Captive portal.
- <метка времени> — метка времени последнего IP-пакета от пользователя, если в Captive portal включены ограничения продолжительности сессии для IP-адресов пользователей. Если в Captive portal ограничения не включены, то вместо метки времени будет выводиться значение «0».

Примечание. ViPNet Coordinator HW не отслеживает выход пользователей из сети (logout). Например, если пользователь Active Directory вышел из сети, то он будет отображаться в списке пользователей до тех пор, пока не истечет время жизни кеша пользовательских сессий (см. service user-control ad set connection-timeout) или пока с этого IP-адреса в сеть не войдет другой пользователь.

Пример использования

```
hostname# service user-control active-users

 5 active network user session(s)

 User name             Session IP-address   Source        Start time  Lifetime left
 /AD Domain Controller                      AD Group Name

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

 Smith.John            13.34.152.12         AD            10:11:42
 /dc1.infotecs.int
 BrownPaul             78.54.24.16          CP            12:24:45    15m
 NelsonNeil            12.34.154.12         AD            10:04:23
 /Longdomaincontrollername.infotecs.int      Administrators
 superadmin            12.34.154.68         AD            10:22:57
 /dc2.infotecs.int
 superadmin            82.12.33.212         CP            11:03:36    1h 3m
```

service user-control ad reset

Удалить параметры соединения ViPNet Coordinator HW с контроллером домена Active Directory.

Синтаксис

```
service user-control ad reset [controller <адрес контроллера домена>]
```

Параметры и ключевые слова

`<адрес контроллера домена>` — IP-адрес или доменное имя узла контроллера домена.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если параметр `<адрес контроллера домена>` не задан, то сбрасываются настройки для всех настроенных контроллеров домена.
- Команда выполняется только при включенной службе UC.

Пример использования

Чтобы сбросить настройки параметров соединения контроллера домена `domain.local`:

```
hostname# service user-control ad reset controller domain.local

User-authentication service is stopped and mode is switched to off, as no authentication
method is currently configured.
```

service user-control ad show

Просмотреть информацию о параметрах аутентификации с помощью Active Directory.

Синтаксис

```
service user-control ad show [controller <адрес>]
```

Параметры и ключевые слова

`<адрес>` — IP-адрес или имя контроллера домена.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В результате выполнения команды выводится следующая информация о параметрах аутентификации с помощью Active Directory:

- Адрес и доступность контроллера домена (или сообщение об отсутствии этого параметра).
- Версия операционной системы и локализация контроллера домена.

- Имя пользователя, используемое для соединения с контроллером домена.
- Время задержки до следующего обновления статуса соединения.
- Допустимое время отсутствия связи (время до очистки кеша пользовательских сессий).

Если адрес или имя контроллера не задано, то выводится информация по всем настроенным контроллерам.

Пример использования

Выполнение команды при настроенном подключении к Active Directory имеет следующий вывод:

```
hostname# service user-control ad show

Active Directory authentication information:

     Domain Controller domain.local is available

               OS version: Microsoft Windows Server 2008 R2 Enterprise  Locale: English - United States

               Domain user: admin

               DC synchronization delay: 100 sec

               Allowed connection timeout: 1800 sec

               Log-file name: syslog.log

     Domain Controller secondary.local is available

               OS version: Microsoft Windows Server 2008 R2 Enterprise  Locale: English - United States

               Domain user: Administrator

               DC synchronization delay: 100 sec

               Allowed connection timeout: 1800 sec

               Log-file name: syslog.log
```

service user-control ad set controller

Настроить соединение с контроллером домена Active Directory.

Синтаксис

```
service user-control ad set controller <адрес контроллера домена> user <имя пользователя>
```

Параметры и ключевые слова

- `<адрес контроллера домена>` — IP-адрес или доменное имя узла контроллера домена. Доменные имена не зависят от регистра и могут содержать латинские буквы (A-z), цифры (0-9), знак «минус» (-) и «точка» (.). Максимальная длина доменного имени — 253 символа.

- `<имя пользователя>` — имя пользователя домена, обладающего правами на чтение журналов системы контроллера домена. Имя пользователя не зависит от регистра и может содержать латинские буквы (A-z), цифры (0-9), знак «минус» (-) и «точка» (.), кроме:

  `"" / \ [ ] : ; | = , + * ? < >`

  Максимальная длина имени пользователя — 20 символов.

  Имя пользователя указывается без домена.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

После успешного выполнения команды в ответ на приглашение командного интерпретатора введите пароль пользователя Active Directory, после чего нажмите клавишу **Enter**. Длина пароля должна быть от 1 до 128 символов. Если пароль не введен, нажатие клавиши **Enter** не сработает.

Пример использования

Для задания параметров соединения с контроллером по адресу 192.168.1.23 и пользователем домена `user23`:

```
hostname# service user-control ad set controller 192.168.1.23 user user23
Enter user23 password:
```

service user-control ad set connection-timeout

Задать допустимое время отсутствия связи с контроллером домена Active Directory.

Синтаксис

```
service user-control ad set connection-timeout <время>
```

Параметры и ключевые слова

`<время>` — допустимое время отсутствия связи с контроллером домена в секундах.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию допустимое время отсутствия связи с контроллером домена составляет 1800 секунд.

- Значение параметра <время> должно быть больше или равно значению периода получения журнала контроллера домена (см. service user-control ad set sync-delay).

Пример использования

```
hostname# service user-control ad set connection-timeout 3600
```

service user-control ad set sync-delay

Задать период получения журнала контроллера домена Active Directory.

Синтаксис

```
service user-control ad set controller sync-delay <период>
```

Параметры и ключевые слова

<период> — период получения журнала контроллера домена Active Directory, целое число в секундах.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию период получения журнала контроллера домена равен 5 секундам.
- Значение параметра <период> должно быть меньше или равно значению времени жизни кеша пользовательских сессий (см. service user-control ad set connection-timeout).

Пример использования

```
hostname# service user-control ad set controller sync-delay 10
```

service user-control cp reset

Сбросить настройки Captive portal.

Синтаксис

```
service user-control cp reset
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

После выполнения команды также останавливается работа службы `uc`.

Пример использования

```
hostname# service user-control cp reset

Stopping uc.sh: uc.
```

service user-control cp set connection-secure

Задать режим соединения Captive portal с LDAP-сервером.

Синтаксис

```
service user-control cp set connection-secure <режим соединения>
```

Параметры и ключевые слова

`<режим соединения>` — параметр может принимать следующие значения:

- `stls` — режим соединения Start TLS, устанавливает соединения на порт LDAP 389.
- `ldaps` — режим соединения на порт LDAP 636.
- `none` — режим открытого соединения.

Значения по умолчанию

Установлен режим открытого соединения (`none`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы задать режим соединения с LDAP-сервером Start TLS:

```
hostname# service user-control cp set connection-secure stls
```

service user-control cp set connection-timeout

Задать время жизни сессии пользователя Captive portal, по истечении которого сессия будет принудительно сброшена.

Синтаксис

```
service user-control cp set connection-timeout <полное время жизни сессии пользователя>
```

Параметры и ключевые слова

`<полное время жизни сессии пользователя>` — целое число в секундах. Если задано значение 0, то длительность пользовательских сессий не ограничена.

Значения по умолчанию

По умолчанию для параметра `<полное время жизни сессии пользователя>` задано значение 43200 секунд.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы задать время жизни сессии пользователя 1 час:

```
hostname# service user-control cp set connection-timeout 3600
```

service user-control cp set custom-login-form

Задать произвольное текстовое сообщение на странице аутентификации пользователей Captive portal.

Синтаксис

```
service user-control cp set custom-login-form <текстовое сообщение>
```

Параметры и ключевые слова

`<текстовое сообщение>` — от 0 до 32 символов, при использовании пробелов необходимо заключить текстовое сообщение в двойные кавычки.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы задать текстовое сообщение «Welcome to Guest Network!» на странице аутентификации пользователей Captive portal:

```
hostname# service user-control cp set custom-login-form "Welcome to Guest Network!"
```

service user-control cp set hostcert

Выбрать сертификат веб-сервера Captive portal из локального хранилища сертификатов ViPNet Coordinator HW.

Синтаксис

```
service user-control cp set hostcert <имя файла сертификата> hostkey <имя файла закрытого ключа>
```

Параметры и ключевые слова

- `<имя файла сертификата>` — имя файла сертификата;
- `<имя файла закрытого ключа>` — имя файла закрытого ключа.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды импортируйте сертификат и его закрытый ключ в корневое хранилище сертификатов ViPNet Coordinator HW (см. service cert import).
- Если вы выбрали сертификат веб-сервера Captive portal и хотите отказаться от его использования, то вам необходимо сбросить настройки Captive portal (см. service user-control cp reset).

Пример использования

Чтобы выбрать сертификат с именем `certificate.pem` и соответствующий ему закрытый ключ с именем `private.pem`:

```
hostname# service user-control cp set hostcert certificate.pem hostkey private.pem
```

service user-control cp set idle-timeout

Задать время бездействия (отсутствия передачи данных) пользователя Captive portal, по истечении которого сессия будет сброшена.

Синтаксис

```
service user-control cp set idle-timeout <время бездействия пользователя>
```

Параметры и ключевые слова

`<время бездействия пользователя>` — целое число в секундах. Если задано значение 0, то время бездействия не ограничено.

Значения по умолчанию

Время бездействия пользователя — 1800 секунд.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы задать время бездействия пользователя 10 минут:

```
hostname# service user-control cp set idle-timeout 600
```

service user-control cp set ldap

Настроить соединение Captive portal с LDAP-сервером.

Синтаксис

```
service user-control cp set ldap <адрес LDAP-сервера> identity <имя администратора> basedn
<база поиска>
```

Параметры и ключевые слова

- `<адрес LDAP-сервера>` — IP-адрес или доменное имя LDAP-сервера. Доменное имя может иметь длину до 253 символов и содержать латинские буквы (`A-z`), цифры (`0-9`), знаки «-» и «.».
- `<имя администратора>` — выделенное имя (DN, Distinguished Name) учетной записи администратора LDAP-сервера, которая обладает правами на чтение записей LDAP-сервера. Выделенное имя администратора может иметь длину до 253 символов и содержать латинские буквы (`A-z`), цифры (`0-9`), знаки «-» и «.», кроме:

```
" / \ [ ] : ; | + * ? < >
```

Выделенное имя администратора должно быть заключено в двойные кавычки.

- `<база поиска>` — выделенное имя (DN, Distinguished Name) базы поиска, от которой начинаются операции поиска в LDAP-каталоге. Выделенное имя базы поиска может иметь длину до 128 символов и содержать латинские буквы (`A-z`), цифры (`0-9`), знаки «-» и «.», кроме:

  ```
  " / \ [ ] : ; | + * ? < >
  ```

  Выделенное имя базы должно быть заключено в двойные кавычки.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

После успешного выполнения команды в ответ на запрос командного интерпретатора введите пароль учетной записи администратора LDAP-сервера.

Пример использования

Предположим, для подключения к LDAP-серверу необходимо указать:

- адрес LDAP-сервера `example.com`;
- учетную запись администратора `admin`, которая находится в организации `People` и домене `example`;
- базу поиска `example`.

Для подключения к LDAP-серверу с указанными параметрами:

```
hostname# service user-control cp set ldap example.com identity
"uid=admin,ou=People,dc=example" basedn "example"

Enter password for LDAP identity:
```

service user-control cp set ldap cacert

Выбрать корневой сертификат LDAP-сервера из локального хранилища сертификатов ViPNet Coordinator HW.

Синтаксис

```
service user-control cp set ldap cacert <имя файла сертификата>
```

Параметры и ключевые слова

`<имя файла сертификата>` — имя файла корневого сертификата в локальном хранилище ViPNet Coordinator HW.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды необходимо импортировать корневой сертификат LDAP-сервера в локальное хранилище сертификатов ViPNet Coordinator HW (см. service cert import).

Пример использования

Чтобы выбрать сертификат с именем `ldap_cert.pem`:

```
hostname# service user-control cp set ldap cacert ldap_cert.pem
```

service user-control cp show

Просмотреть настройки Captive portal.

Синтаксис

```
service user-control cp show
```

Режимы командного интерпретатора

- Режим настройки.
- Режим просмотра.

Пример использования

```
hostname> service user-control cp show
Captive Portal authentication information:
LDAP server 10.254.252.214 is available
LDAP identity: "uid=admin,ou=People,dc=test,dc=local"
LDAP basedn: "dc=test,dc=local"
LDAP connection secured: stls
LDAP server CA certificate: cacert.pem
CP server Web certificate:
```

```
Allowed connection timeout: 3600 sec
Allowed idle timeout: 600 sec
Custom login phrase: Guest Network
```

service user-control fw-rules apply

Создать служебные сетевые фильтры после изменения параметров соединения с сервером Active Directory или Captive portal.

Синтаксис

```
service user-control fw-rules apply
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service user-control fw-rules apply
Applying rules for Active Directory... Please wait.
```

service user-control fw-rules delete

Удалить разрешающие сетевые фильтры, созданные командой `service user-control fw-rules apply`.

Синтаксис

```
service user-control fw-rules delete
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service user-control fw-rules delete
```

service user-control fw-rules show

Просмотреть сетевые фильтры, разрешающие соединение ViPNet Coordinator HW с сервером Active Directory и Captive portal.

Синтаксис

```
service user-control fw-rules show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname# service user-control fw-rules show

empty rule for  Service:

+======+==================+==============+===================+
|Num   |Name         |                   |Option Schedule    |
|Act   |Protocol           |Source       ->|Destination       |
|      |DpiProtocol        |DpiApp             |DomainUser   |
+======+==================+==============+=================+
|8      |user-control auto |                   |User         |
|pass   |@any       |@local       ->|10.10.10.10             |
|       |@any       |@any         |@any                      |
+======+==================+==============+=================+
```

service user-control mode

Включить или выключить автозапуск службы управления пользователями (`uc`) при загрузке ViPNet Coordinator HW.

Синтаксис

```
service user-control mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автозапуск службы `uc`.
- `off` — выключить автозапуск службы `uc`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

По умолчанию автозапуск службы `uc` выключен.

Пример использования

```
hostname# service user-control mode on
```

service user-control show

Просмотреть информацию о состоянии работы службы управления пользователями (`uc`).

Синтаксис

```
service user-control show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В результате выполнения команды выводится следующая информация о статусе работы службы `uc`:

- Состояние службы `uc` и режим ее автозапуска.
- Уровень важности событий, добавляемых в системный журнал (см. service user-control syslog-level).
- Статус настройки и доступность сервера Active Directory и Captive portal.
- Количество активных сессий пользователей (если служба `uc` запущена).

Пример использования

Выполнение команды при запущенной службе `uc` имеет следующий вывод:

```
hostname# service user-control show
User Control service is ON and will NOT restart automatically
Current syslog level is warning and higher
Active Directory authentication is configured and available
Active Directory Domain Controller PDC authentication is configured and available
```

```
Captive Portal authentication is configured and available

No active network users.
```

service user-control syslog-level

Задать уровень важности событий службы управления пользователями (`uc`), которые будут попадать в системный журнал.

Синтаксис

```
service user-control syslog-level <уровень важности>
```

Параметры и ключевые слова

`<уровень важности>` — число от 0 до 5, соответствующее уровням важности событий:

- 0 — критические события;
- 1 — ошибки;
- 2 — извещения;
- 3 — информационные события;
- 4 — отладочные события;
- 5 — детализированные отладочные события.

Каждый последующий уровень включает в себя предыдущие.

Значения по умолчанию

Задан уровень важности 3 (информационные события).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы в системный журнал записывались события службы `uc` уровня 4:

```
hostname# service user-control syslog-level 4
```

service vpn mode

Включить или выключить автозапуск подсистемы VPN при перезагрузке ViPNet Coordinator HW.

Синтаксис

```
service vpn mode {on | off}
```

Параметры и ключевые слова

- `on` — включить автозапуск.
- `off` — выключить автозапуск.

Значения по умолчанию

- По умолчанию автозапуск VPN включен (`on`).
- После изменения текущего режима автозапуска необходимо перезагрузить ViPNet Coordinator HW.
- В кластере команда выполняется только на активном узле.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы включить автозапуск подсистемы VPN:

```
hostname# service vpn mode on

The settings are saved. System must be restarted for the changes to take effect. Restart now Y/N Y

reboot in progress
```

service vpn show status

Просмотреть текущие параметры подсистемы VPN.

Синтаксис

```
service vpn show status
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

При выполнении команды отображаются:

- состояние подсистемы VPN:
  - `VPN subsystem is on` — запущена;
  - `VPN subsystem is off` — остановлена.
- режим автозапуска подсистемы VPN:
  - `VPN subsystem autostart is on` — автозапуск включен;
  - `VPN subsystem autostart is off` — автозапуск выключен.

Пример использования

```
hostname> service vpn show status

VPN subsystem is on

VPN subsystem autostart is on
```

service vpn start

Запустить подсистему VPN.

Синтаксис

```
service vpn start
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Для восстановления доступа к командам настройки L2overIP, которые стали недоступными после отключения подсистемы VPN, перезапустите сессию локального администратора.

Пример использования

```
hostname# service vpn start
```

service vpn stop

Завершить работу подсистемы VPN.

Синтаксис

```
service vpn stop
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

После выполнения команды:

- Перезапустите сессию локального администратора.
- Вычислительные ресурсы ViPNet Coordinator HW будут распределены на другие службы.
- Функции VPN будут ограничены как при истечении срока действия лицензионного объекта VPN (подробнее см. документ «Подготовка к работе», раздел «Функциональные ограничения по окончании срока действия лицензий»).

Пример использования

```
hostname# service vpn stop
```

Команды группы ups

Настройка взаимодействия ViPNet Coordinator HW с источником бесперебойного питания (ИБП).

Примечание. Использование группы команд ups возможно только для аппаратных исполнений ViPNet Coordinator HW. Для исполнения ViPNet Coordinator VA эти команды выполняться не будут.

ups set driver

Выбрать драйвер `UPS`.

Синтаксис

```
ups set driver <драйвер>
```

Параметры и ключевые слова

`<драйвер>` — название драйвера. В текущей версии ViPNet Coordinator HW можно указать только значение `usbhid-ups`.

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы выбрать драйвер `UPS`:

```
hostname# ups set driver usbhid-ups
```

ups set mode

Настроить режим взаимодействия ViPNet Coordinator HW с ИБП.

Синтаксис

```
ups set mode {master | slave <IP-адрес мастера>}
```

Параметры и ключевые слова

- `master` — взаимодействие в режиме главного компьютера. Главным является компьютер, к которому подключен интерфейсный кабель ИБП и который непосредственно взаимодействует с ИБП.

- `slave` — взаимодействие в режиме подчиненного компьютера. Подчиненный компьютер взаимодействует с ИБП через главный компьютер.
- `<IP-адрес мастера>` — IP-адрес главного компьютера, находящегося в режиме `master`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды требуется вручную завершить работу служб пакета NUT (Network UPS Tools) с помощью команды ups stop.

Пример использования

```
hostname# ups set mode master
```

ups set monitoring

Включить или выключить мониторинг состояния ИБП.

Синтаксис

```
ups set monitoring {on | off}
```

Параметры и ключевые слова

- `on` — включить мониторинг;
- `off` — выключить мониторинг.

Значения по умолчанию

Мониторинг состояния ИБП выключен (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- После включения мониторинга запустите службы пакета NUT с помощью команды ups start.
- При выключении мониторинга будет автоматически завершена работа служб пакета NUT.

Пример использования

```
hostname# ups set monitoring on
```

ups show config

Просмотреть текущие настройки взаимодействия ViPNet Coordinator HW с ИБП.

Синтаксис

```
ups show config
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Команда выводит следующую информацию:

- Включен или выключен мониторинг состояния ИБП. Остальная информация выводится только в случае, если мониторинг включен.
- Режим взаимодействия ViPNet Coordinator HW с ИБП (`master` или `slave`).
- Используемый драйвер `UPS` (только в режиме `master`).
- IP-адрес мастера (только в режиме `slave`).
- Состояние служб пакета `NUT` (запущены или работа служб завершена).

Пример использования

```
hostname> ups show config
UPS service mode is Master. Driver: usbhid-ups
UPS service is RUNNING
```

ups show status

Просмотреть информацию о состоянии ИБП.

Синтаксис

```
ups show status [extended]
```

Параметры и ключевые слова

`extended` — просмотр всех параметров состояния ИБП в формате утилиты `upsc`, входящей в состав пакета `NUT`. Эта возможность предназначена для квалифицированных системных администраторов, которые могут самостоятельно интерпретировать результат вывода утилиты `upsc`.

Особенности использования

Команда выводит следующую информацию:

- производитель ИБП;
- модель ИБП;
- текущая нагрузка по мощности (в процентах от максимальной нагрузки);
- текущий режим питания (`OL` — питание от сети, `OB` — питание от батареи);
- текущий уровень заряда батареи (в процентах от максимального уровня);
- расчетное время работы от батареи при текущих нагрузке и уровне заряда (в секундах);
- максимальное время работы от батареи, по истечении которого ИБП посылает сигнал о необходимости выключения компьютера (задается производителем ИБП).

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> ups show status
Manufacturer:   American Power Conversion
Model:          Smart-UPS 750 RM
Load:           24.0%
Power status:   OL
Battery charge: 100%
Runtime:        2520
Runtime to low: 1380
```

ups start

Запустить службы пакета `NUT`, обеспечивающие взаимодействие ViPNet Coordinator HW с ИБП.

Синтаксис

```
ups start
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> ups start
```

ups stop

Завершить работу служб пакета `NUT`, обеспечивающих взаимодействие ViPNet Coordinator HW с ИБП.

Синтаксис

```
ups stop
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> ups stop
```

Команды группы vpn

Загрузка и выгрузка драйверов и служб ViPNet.

vpn config delete

Удалить копию конфигурации VPN.

Синтаксис

```
vpn config delete <имя> [<версия>]
```

Параметры и ключевые слова

- `<имя>` — имя копии конфигурации VPN;
- `<версия>` — версия ПО ViPNet Coordinator HW, к которой относится копия конфигурации VPN. Указывается в формате `Major.Minor.Subminor`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе имени работают автодополнение и подсказка. Данные для подсказки берутся из текущего списка сохраненных копий конфигурации VPN.
- В имени можно указать символ «*» для обозначения любого количества символов. Это позволит удалить сразу нескольких копий конфигурации VPN.
- Если версия не указана и при этом имеется несколько копий конфигурации VPN с совпадающими именами, но различными версиями, то выводится список таких копий конфигурации VPN с предложением указать версию для удаления.

Пример использования

```
hostname# vpn config delete Config_*

Configuration 'Config_2021123' (version 2.0.0) deleted
```

vpn config list

Просмотреть список сохраненных копий конфигурации VPN.

Синтаксис

```
vpn config list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Формат отображения списка сохраненных копий: `"Name", Version, Type, saved on Date at Time, loaded at Date-load at Time-load`, где:

- `Name` — имя копии конфигурации VPN.
- `Version` — версия ПО ViPNet Coordinator HW, в которой была создана копия конфигурации VPN (может отсутствовать).
- `Type` — вид копии конфигурации VPN: `full` (полная) или `part` (частичная).
- `Date`, `Time` — дата и время создания копии конфигурации VPN.
- `Date-load`, `Time-load` — дата и время загрузки копии конфигурации VPN. Если копия конфигурации VPN никогда не загружалась, вместо даты и времени загрузки отображается `never loaded`.

Пример использования

```
hostname# vpn config list
"Config_1", version 5.3.1, full, saved on 13.03.2024 at 20:06, never loaded
```

vpn config load

Загрузить настройки ViPNet Coordinator HW из копии конфигурации VPN.

Синтаксис

```
vpn config load <имя> [<версия>]
```

Параметры и ключевые слова

- `<имя>` — имя копии конфигурации VPN.
- `<версия>` — версия ПО ViPNet Coordinator HW, к которой относится копия конфигурации VPN. Указывается в формате `Major.Minor.Subminor`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите службы `iplir`, `failoverd` и `mftpd`. После выполнения запустите их.
- При вводе имени работают автодополнение и подсказка. Данные для подсказки берутся из текущего списка сохраненных копий конфигурации VPN.
- Если версия не указана и при этом имеется несколько копий конфигурации VPN с совпадающими именами, но различными версиями, то выводится список таких копий конфигурации с предложением указать версию для загрузки.
- Перед загрузкой настроек из копии конфигурации VPN запрашивается подтверждение для сохранения копии текущей конфигурации VPN. В случае подтверждения введите имя, под которым будет сохранена копия текущей конфигурации.
- Если текущая версия ПО ViPNet Coordinator HW ниже версии, указанной в команде, дополнительно подтвердите загрузку настроек из копии конфигурации VPN.

Пример использования

Чтобы загрузить настройки из копии конфигурации VPN с именем `Rollback_config`, относящейся к версии `5.3.1`:

```
hostname# vpn config load Rollback_config 5.3.1
```

vpn config save

Сохранить копию текущей конфигурации VPN.

Синтаксис

```
vpn config save <имя>
```

Параметры и ключевые слова

`<имя>` — имя копии конфигурации VPN.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите службы `iplir`, `failoverd` и `mftpd`.
- В имени можно использовать только символы латинского алфавита, цифры, знаки «дефис» и «подчеркивание».

- Если в списке сохраненных копий конфигурации VPN есть копия с указанным именем, то запрашивается подтверждение на перезапись.
- Сохраненная копия конфигурации VPN включает настройки VPN, сетевых интерфейсов, системы защиты от сбоев, транспортного сервера MFTP, а также сетевые фильтры.

Пример использования

Чтобы сохранить копии текущей конфигурации VPN под именем `Rollback_config`:

```
hostname# vpn config save Rollback_config
```

vpn start

Запустить службы шифрования IP-пакетов (`itcscrpt` и `itcshub`) и прозрачного соединения сегментов сети на уровне L2 (`l2overip`).

Синтаксис

```
vpn start
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда выполняется только в том случае, если перед этим была выполнена команда `vpn stop` или если службы и драйверы не были запущены при загрузке ViPNet Coordinator HW.

Пример использования

```
hostname# vpn start
Applying changes. Please wait...
itcscrpt has already loaded
Loading l2overip module...Done
Starting itcshub deamon...Done
```

vpn stop

Остановить службы шифрования IP-пакетов (`itcscrpt` и `itcshub`) и прозрачного соединения сегментов сети на уровне L2 (`l2overip`).

Синтаксис

```
vpn stop
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# vpn stop
Applying changes. Please wait...
Shutting down itcshub deamon...Done
Unloading l2overip module...Done
Unloading itcscrpt module...Done
```

Команды группы webui

Управление службой `WebUI` ViPNet Coordinator HW, на основе которой функционирует веб-интерфейс.

webui https-cert

Установить сертификат для доступа к ViPNet Coordinator HW по протоколу HTTPS.

Синтаксис

```
webui https-cert <сертификат>
```

Параметры и ключевые слова

`<сертификат>` — имя файла сертификата в формате `*.cer`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если в хранилище отсутствует устанавливаемый сертификат — отображается список доступных для выбора сертификатов.
- Если в момент установки сертификата для доступа к ViPNet Coordinator HW с помощью веб-интерфейса используется протокол HTTPS, то после установки нового сертификата перезапустите службу `WebUI` (webui restart).

Пример использования

```
hostname# webui https-cert webuihttps.cer
Certificate has been set successfully
```

webui info

Просмотреть состояние службы `WebUI`.

Синтаксис

```
webui info
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде выводятся:

- Статус службы — запущена или остановлена.
- Протокол для доступа к ViPNet Coordinator HW с помощью веб-интерфейса.
- Имя файла сертификата протокола HTTPS, если установлен.
- Номер TCP-порта.

Пример использования

```
hostname> webui info
WebUI server is running
Protocol HTTPS
HTTPS cert webuihttps.cer
Port 8080
```

webui port

Задать TCP-порт для доступа к ViPNet Coordinator HW с помощью веб-интерфейса.

Синтаксис

```
webui port <порт>
```

Параметры и ключевые слова

`<порт>` — номер TCP-порта.

Значения по умолчанию

Используется TCP-порт 8080.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если TCP-порт используется другой службой ViPNet Coordinator HW — выводится сообщение `Port in use. Release port or select another.`

- После установки номера TCP-порта:
  - Измените в правиле межсетевого экрана Allow ViPNet WebGui номер TCP-порта: `@any @local tcp: to <порт> pass`.
  - Перезапустите службу WebUI (webui restart).

Пример использования

```
hostname# webui port 443

Web Access port has been set successfully.

For Web Access to function correctly, change port in the Allow WebGUI rule and restart the
Web Access service
```

webui protocol

Выбрать протокол, используемый для доступа к ViPNet Coordinator HW с помощью веб-интерфейса.

Синтаксис

```
webui protocol {http | https}
```

Параметры и ключевые слова

- `http` — протокол HTTP.
- `https` — протокол HTTPS.

Значения по умолчанию

Используется протокол HTTPS.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- До переключения протокола с HTTP на HTTPS установите сертификат (см. webui https-cert).
- При переключении протокола перезапускается служба `WebUI`.

Пример использования

```
hostname# webui protocol https

Protocol HTTPS has been set successfully
HTTPS cert webuihttps.cer
```

webui recreate-cert

Перевыпустить самоподписанный сертификат, используемый для подключения к веб-интерфейсу по протоколу HTTPS.

Синтаксис

```
webui recreate-cert [bits <длина ключа> digest {sha256 | sha384 | sha512} span <срок действия> [subj <subject>]]
```

Параметры и ключевые слова

- `<длина ключа>` — размер создаваемого RSA-ключа в битах, можно задавать следующие значения: 2048, 3072, 4096;
- `sha256` — алгоритм хэширования SHA-256;
- `sha384` — алгоритм хэширования SHA-384;
- `sha512` — алгоритм хэширования SHA-512;
- `<срок действия>` — срок действия самоподписанного сертификата в днях. Возможные значения: `30–1825;`
- `subject` — дополнительные параметры:
  - `/C` — код страны;
  - `/ST` — область (до 64-х символов);
  - `/L` — город (до 64-х символов;
  - `/O` — организация (до 64-х символов);
  - `/OU` — отдел организации (до 64-х символов);
  - `/CN` — доменное имя;
  - `/emailAddress` — электронный адрес;
  - `/subjectAltName` — альтернативные адреса ресурса.

Значения по умолчанию

- Без указания параметров и ключевых слов используются значения, как при инициализации ViPNet Coordinator HW:
  - длина ключа — 2048;
  - алгоритм хэширования — sha256;
  - срок действия — 1825 дней;
  - имя субъекта — имя узла.
- Без указания дополнительных параметров (`subj`) в качестве доменного имени указывается имя узла (`hostname`), а остальные дополнительные параметры сертификата отсутствуют.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Новый сертификат назначается действующим для подключения к веб-интерфейсу ViPNet Coordinator HW по протоколу HTTPS.
- Если служба `WebUI` работала по протоколу HTTPS, то она автоматически перезапустится для применения изменений.
- Если служба `WebUI` работала по протоколу HTTP, установите для нее протокол HTTPS (`webui protocol https` (см. webui protocol)).

Пример использования

```
hostname# webui recreate-cert bits 2048 digest sha512 span 365 subj
"/subjectAltName=DNS:infotecs.biz,IP:127.50.50.50"
Web access certificate would be recreated and set.
Continue? [Yes/No]: y
Certificate recreated and set.
```

webui restart

Перезапустить службу `WebUI`.

Синтаксис

```
webui restart
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> webui restart
Shutting down ViPNet Web GUI service
Loading ViPNet Web GUI service
spawn-fcgi: child spawned successfully: PID: 22996
```

Прочие команды

К прочим относятся команды, которые не входят ни в одну из групп команд, описанных выше.

debug off

Выключить вывод сообщений о событиях.

Синтаксис

```
debug off [<источник> <уровень важности>]
```

Параметры и ключевые слова

- `<источник>` — процесс, для которого требуется выключить вывод сообщений. Например:
  - `kern` — ядро;
  - `user` — пользовательские программы;
  - `mail` — почтовая система;
  - `daemon` — службы.
- `<уровень важности>` — уровень важности сообщений. Например:
  - `err` — сообщения об ошибках;
  - `info` — информационные сообщения;
  - `debug` — отладочные сообщения.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Если в команде не указаны параметры, то будет выключен вывод всех сообщений.

Пример использования

Чтобы выключить вывод сообщений об ошибках служб:

```
hostname# debug off daemon err
```

debug on

Включить вывод сообщений о событиях.

Синтаксис

```
debug on [<источник> <уровень важности>]
```

Параметры и ключевые слова

- `<источник>` — процесс, для которого должны выводиться сообщения. Например:
  - `kern` — ядро;
  - `user` — пользовательские программы;
  - `mail` — почтовая система;
  - `daemon` — службы.
- `<уровень важности>` — уровень важности выводимых сообщений. Например:
  - `err` — события содержащие ошибки;
  - `info` — информационные сообщения;
  - `debug` — отладочные сообщения.

Значения по умолчанию

- `<источник>` — `daemon`.
- `<уровень важности>` — `debug`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Для служб сообщения будут выводиться только в случае, если в их файлах конфигураций в секции `[debug]` задано протоколирование для указанных источника и важности сообщений.

Пример использования

Чтобы включить вывод сообщений об ошибках служб:

```
hostname# debug on daemon err
```

enable

Перейти в режим настройки.

Синтаксис

```
enable
```

Режимы командного интерпретатора

Режим просмотра.

Особенности использования

Команда применима только для пользователей с ролью администратора.

Пример использования

```
hostname> enable
hostname#
```

exit

Выйти из текущего режима командного интерпретатора.

Синтаксис

```
exit
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- В результате выполнения команды в режиме настройки происходит переход в режим просмотра.
- В результате выполнения команды в режиме просмотра происходит завершение работы командного интерпретатора. При этом отображается приглашение ввести имя пользователя и пароль для запуска командного интерпретатора.

Пример использования

```
hostname# exit
```

```
hostname>
```

license

Просмотреть лицензии ViPNet Coordinator HW.

Синтаксис

```
license
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Тип объекта лицензирования:
  - Основной объект в соответствии с исполнением ViPNet Coordinator HW, например `Coordinator VA1000`.
  - `VPN` — VPN.
  - `DPI` — DPI.
  - `DPI Update` — обновление DPI.
  - `IPS` — предотвращения вторжений IPS.
  - `IPS Update` — обновление базы правил IPS.
  - `Failover` — система защиты от сбоев в режиме кластера.
- Максимальная версия ПО ViPNet Coordinator HW, поддерживаемая лицензией.
- Статус объекта лицензирования:
  - `active` — действует.
  - `expired` — не действует.
- Время окончания действия объекта лицензирования в формате `YYYY-MM-DD HH:MM:SS`.

Пример использования

```
hostname> license
License object          Version     Status      Expiration date
--------------          -------     ------      ---------------
Coordinator VA1000      5.99        active      2023-05-13 03:00:00
VPN                     5.99        active      2023-05-13 03:00:00
```

```
DPI                    5.99        active      2023-05-13 03:00:00
DPI update             5.99        active      2023-05-13 03:00:00
IPS                    5.99        active      2023-05-13 03:00:00
IPS update             5.99        active      2023-05-13 03:00:00
Failover               5.99        active      2023-05-13 03:00:00
```

serial

Установить серийный номер ViPNet Coordinator HW.

Синтаксис

```
serial <серийный номер>
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна на аппаратных исполнениях ViPNet Coordinator HW, серийный номер которых не был установлен при производстве.
- Длина серийного номера: 4–18 символов.
- Допустимые символы:
  - Прописные и строчные буквы латинского алфавита: `A–Z`, `a–z`.
  - Цифры: `0–9`.
  - Специальный символ `-`.

Пример использования

```
hostname# serial 431-24758
Appliance serial number successfully set.
```

user certificate create

Издать или перевыпустить сертификат локального аудитора `user`.

Синтаксис

```
user certificate create
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Команда может быть выполнена аудитором или администратором. Если команда выполняется локальным администратором, то потребуется извлечь USB-токен администратора и подключить USB-токен локального аудитора.
- При выполнении команды введите ПИН администратора USB-токена, затем введите и подтвердите ПИН пользователя (требования к ПИНам USB-токена см. в документации на USB-токен).

Пример использования

```
hostname# user certificate create

Extract the admin token and insert the user token. Press Enter to continue...


Upon executing the command, you will lost all current token data. Continue? [Yes/No]: y

Enter admin-token pincode: ********

Enter new user-token pincode: ********

Confirm new user-token pincode: ********

Certificate has been successfully created.
```

user certificate delete

Удалить сертификат локального аудитора `user`.

Синтаксис

```
user certificate delete
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Команда может быть выполнена аудитором или администратором.

- После выполнения команды локальное подключение аудитора `user` к ViPNet Coordinator HW с помощью консоли будет заблокировано, если используется аутентификация по сертификату. При этом остаётся доступным удалённое подключение по SSH и HTTP/HTTPS.

Пример использования

```
hostname# user certificate delete

Upon executing the command, you will not be able to log on with user account. Continue?
[Yes/No]: y

Certificate has been successfully deleted.
```

user passwd

Изменить пароль локального аудитора `user`.

Синтаксис

```
user passwd
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Требования к паролю:
  - Длина пароля: 6–31 символ.
  - Допустимые символы:
    - Прописные и строчные буквы латинского алфавита: `A–Z`, `a–z`.
    - Арабские цифры: `0–9`.
    - Специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- При вводе пароля вводимые символы не отображаются.
- Если ранее пароль локальной учетной записи `user` был сброшен, то после выполнения команды в режиме настройки учетная запись будет разблокирована.
- В кластере команда выполняется только на активном узле.

Пример использования

```
hostname# user passwd
Type the new user password:
```

```
Confirm new user password:
```

user reset passwd

Сбросить пароль локального аудитора `user`.

Синтаксис

```
user reset passwd
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- После выполнения команды:
  - Открытые сессии локального аудитора будут завершены.
  - Локальная учетная запись `user` будет заблокирована.
- В кластере команда выполняется только на активном узле.

Пример использования

```
hostname# user reset passwd
Upon executing the command, you will not be able to log on with the user account. Continue?
Yes
Account password has been reset
```

version

Просмотреть сведения о ViPNet Coordinator HW.

Синтаксис

```
version [full]
```

Параметры и ключевые слова

`full` — просмотр дополнительных сведений:

- версии компонентов ПО ViPNet Coordinator HW;
- имя набора функциональных возможностей;
- архитектура платформы.

Значения по умолчанию

Отображаются основные сведения:

- название продукта;
- аппаратная платформа ViPNet Coordinator HW или платформа виртуализации;
- серийный номер для исполнений ViPNet Coordinator HW на аппаратных платформах;
- базовая лицензия;
- версия ПО ViPNet Coordinator HW.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname# version full
Product: ViPNet Coordinator HW
Platform: HW1000C
Serial number: 123-45678
License: HW1000C
Software version: 5.1.1-4550

WebGUI software version: 3.0.0.273
VPN software version: 5.1.1-1
Iplir driver software version: 4.1.3
Watchdog driver software version: 1.0.5

Crypto driver version: 2.3.2.2668
Crypto core version: NA

DPI version: 5.1_21.10.08
Feature set: base
Architecture: x86_64
```

version features list

Просмотреть список функциональных модулей, входящих в состав текущей версии ViPNet Coordinator HW.

Синтаксис

```
version features list
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> version features list
bonding
dhcp-client
dhcp-relay
dhcp-server
...
```

who

Просмотреть информацию об активных сессиях пользователей.

Синтаксис

```
who
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Информация об активных сессиях обновляется каждые 7 секунд.
- Формат представления информации о сессии:
  - `interface` — тип интерфейса взаимодействия: `CLI` или `WebUI`.
  - `Role` — роль пользователя: `Auditor` или `Admin`.

- `User` — имя пользователя. После имени пользователя текущей сессии отображается `(you)`. Для централизованной учетной записи, совпадающей с локальной (`user` или `admin`), добавляется префикс `center/`.
- `Idle` — время неактивности (отсутствие каких-либо управляющих запросов).

Пример использования

```
hostname> who
Interface  Role     User                                    Idle
-------------------------------------------------------------------
CLI        Auditor  user (you)                          00:00:00
CLI        Admin    center/admin                        00:00:08
WebUI      Admin    Petrov.Petr                         00:00:20
WebUI      Admin    Konstantin.Vasiliev                 00:01:48
```

2

Справочник конфигурационных файлов

Файл iplir.conf 486

Файл iplir.conf-<интерфейс или группа интерфейсов> 499

Файл failover.ini 502

Файл mftp.conf 510

Файл iplir.conf

Параметры защищенной сети ViPNet содержатся в файле `iplir.conf`. Чтобы их настроить:

1. Остановите управляющую службу:

   ```
   hostname# iplir stop
   ```

2. Откройте файл:

   ```
   hostname# iplir config
   ```

3. Настройте параметры, используя описание секций.

4. Запустите управляющую службу:

   ```
   hostname# iplir start
   ```

Секция [adapter]

Секции `[adapter]` описывают статические сетевые интерфейсы компьютера. Каждому интерфейсу соответствует своя секция `[adapter]`. Если статический интерфейс не описан секцией, то все проходящие через него IP-пакеты блокируются.

Примечание. В процессе работы ViPNet Coordinator HW могут создаваться динамические интерфейсы, например, при подключении ViPNet Coordinator HW к сети 3G или Wi-Fi. В ViPNet Coordinator HW по умолчанию разрешена работа динамических интерфейсов, которые входят в одну из следующих групп:

- `ppp` — интерфейсы для встроенных модемов;
- `wifi` — интерфейсы для внешних адаптеров Wi-Fi. В эту группу не входит встроенный интерфейс `wlan0`.

Добавление интерфейсов данных групп в файл `iplir.conf` не требуется.

Если в файле `iplir.conf` нет ни одной секции `[adapter]`, то управляющая служба при запуске получает от системы список сетевых интерфейсов и автоматически создает соответствующие секции.

В процессе работы управляющая служба и драйвер ViPNet периодически получают информацию о параметрах известных им интерфейсов с интервалом времени, заданным параметром `ifcheck_timeout` секции `[misc]` (см. Секция [misc]). Если обнаруживается, что интерфейс выключен в системе, то он выключается и в драйвере ViPNet. После включения или изменения IP-адреса интерфейса эти изменения автоматически загружаются в драйвер ViPNet.

В секции `[adapter]` указываются параметры:

- `allowtraffic` — разрешение или блокирование прохождения IP-трафика через интерфейс. Возможные значения:

- `on` (по умолчанию) — IP-пакеты пропускаются или блокируются в соответствии с сетевыми фильтрами, заданными на узле;
- `off` – IP-пакеты блокируются независимо от остальных настроек.

- `type` — тип интерфейса для драйвера ViPNet. Возможные значения: `internal` (внутренний) или `external` (внешний).

  Тип интерфейса выбирается, исходя из следующего:

  - В режиме «С динамической трансляцией адресов» все интерфейсы должны иметь тип `internal`.
  - В режиме «Со статической трансляцией адресов» (с фиксированным внешним адресом) интерфейсу, посредством которого ViPNet Coordinator HW будет связываться с узлом, выполняющим функции межсетевого экрана, следует назначить тип `external`, остальным интерфейсам — тип `internal`.

Нередактируемые параметры

- `name` — системное имя интерфейса (например, `eth0`). Если в системе задано несколько IP-адресов на одном интерфейсе и присутствуют один или несколько виртуальных интерфейсов (`eth0:0`, `eth0:1` и так далее), то для управляющей службы и драйвера ViPNet все они будут представлять одно физическое устройство с базовым именем (`eth0`).

Секция [debug]

Секция `[debug]` определяет параметры ведения системного журнала управляющей службы `iplircfg`:

Внимание! В исполнениях с одним дисковым накопителем:

- По умолчанию уровень важности равен 1.
- При локальном протоколировании доступны уровни важности от –1 до 3.
- При удаленном протоколировании доступны уровни важности от –1 до 4. При этом если вы используете 4 уровень и выполняете переключение на локальное протоколирование, уровень не изменяется автоматически. Чтобы уровень важности принял значение по умолчанию, перезапустите службу `iplircfg`.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

  Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

Секция [dynamic]

Секция `[dynamic]` содержит параметры для настройки режима подключения к внешней сети через межсетевой экран с динамической трансляцией адресов:

- `always_use_server` — включение или выключение режима, при котором весь трафик с внешними узлами направляется через сервер соединений, указанный в `forward_id` данной секции. Возможные значения: `off` (по умолчанию) или `on`.
- `dynamic_proxy` — включение или выключение режима «С динамической трансляцией адресов». Возможные значения: `on`, `off` или `auto`. Если этот параметр установлен в значение:
  - `off` — остальные параметры в данной секции игнорируются;
  - auto — режим определяется в соответствии с настройкой, заданной в ViPNet Prime.
- `forward_id` — идентификатор сервера соединений для ViPNet Coordinator HW. С помощью сервера соединений ViPNet Coordinator HW будет устанавливать соединения с другими узлами — всегда, если включен режим в `always_use_server`, либо до тех пор, пока соединение с другими узлами не будет установлено напрямую. Указывается в шестнадцатеричном формате с префиксом `0x`, например: `0x15c8000a`.

  

  Внимание! Указанный сервер соединений должен быть доступен из внешней сети по публичному IP-адресу.

- `timeout` — интервал отправки IP-пакетов серверу соединений для поддержания активного соединения с ним и пропуска входящего трафика через межсетевой экран. Указывается в секундах, значение по умолчанию — `25`. Как правило, интервала, заданного по умолчанию, достаточно для поддержки связи с сервером соединений при работе через большинство межсетевых экранов.
- `port_auto_change` — включение или выключение автоматической смены порта при недоступности сервера соединений. Возможные значения: `off` (по умолчанию) или `on`.

Секция [id]

Секция `[id]` используется для описания адресных настроек защищенных узлов, связанных с ViPNet Coordinator HW. Каждому узлу, с которым у ViPNet Coordinator HW есть связь, соответствует своя секция `[id]`. Первая секция соответствует собственным настройкам ViPNet Coordinator HW (собственная секция).

Секция `[id]` содержит параметры:

- `accessiplist` — IP-адреса доступа к узлу и их приоритет, если узел имеет множественные адреса доступа. В каждой секции `[id]` может быть указано любое количество параметров `accessiplist` — по количеству адресов доступа к узлу. Причем в первом параметре `accessiplist` каждой секции в качестве адреса доступа должен быть указан тот же адрес, что и в параметре `firewallip` данной секции. Если в секции не будет параметров `accessiplist`,

то параметр `firewallip` тоже будет отсутствовать. Остальные параметры `accessiplist` в секции используются для формирования списка адресов доступа к узлу с узла ViPNet Coordinator HW.

Параметр `accessiplist` может быть указан во всех секциях `[id]`, кроме собственной, в виде:

`accessiplist = <IP-адрес доступа>, <метрика>, <реальный IP-адрес узла>, <номер интерфейса>, <тип регистрации>, <порт>`, где:

Примечание. Вручную в параметре `accessiplist` можно указать только IP-адрес узла, порт и метрику, остальные параметры определяются управляющей службой `iplircfg` автоматически.

- `<IP-адрес доступа>` — IP-адрес доступа к узлу.
- `<метрика>` — метрика указанного адреса доступа. Она определяет задержку (в миллисекундах) отправки тестовых сообщений при определении адреса доступа узла. Опросы осуществляются периодически (см. параметры `server_pollinterval` и `client_pollinterval` секции `[misc]`). Возможные значения: от `0` до `9999`. По умолчанию метрика имеет значение `auto`, то есть определяется автоматически.
- `<реальный IP-адрес узла>` — реальный IP-адрес узла, соответствующий сетевому интерфейсу, через который будут передаваться IP-пакеты для выбранного IP-адреса доступа. Присваивается автоматически.
- `<номер интерфейса>` — условный номер сетевого интерфейса. Возможные значения: от `0` до `255`.
- `<тип регистрации>` — тип регистрации данного IP-адреса доступа узла:
  - `auto` — задан ViPNet Coordinator HW.
  - `manual` — задан администратором вручную (редактированием файла `iplir.conf`).
  - `addrdoc` — взят из справочников, полученных из ViPNet Prime.
- `<порт>` — порт доступа к узлу. Возможные значения: от `1` до `65535`.

- `blockforward` — включение или выключение блокирования транзитных пакетов, передаваемых через ViPNet Coordinator HW узлу ViPNet, связанному с ViPNet Coordinator HW. Используется только в секциях `[id]`, описывающих настройки узлов ViPNet, связанных с ViPNet Coordinator HW. Возможные значения: `off` — все транзитные пакеты в направлении узла пропускаются, `on` — все транзитные пакеты в направлении узла блокируются с кодом 70. По умолчанию данный параметр отсутствует, что эквивалентно значению `off`.
- `fqdn` — содержит доменное имя координатора, которое используется для восстановления соединения с координатором в случае смены его IP-адреса доступа (параметр `firewallip`). В собственной секции `[id]` параметр используется для задания доменного имени ViPNet Coordinator HW, а в любой секции `[id]`, кроме собственной — для задания доменного имени координатора, связанного с ViPNet Coordinator HW. Значение параметра присваивается автоматически ViPNet Prime и может быть изменено вручную администратором ViPNet Coordinator HW. При этом, если впоследствии администратор сети ViPNet изменит значение параметра в ViPNet Prime, оно будет присвоено несмотря на изменения, сделанные администратором ViPNet Coordinator HW.

Доменное имя, заданное в параметре, должно быть зарегистрировано на DNS-сервере (корпоративном или любом другом, публично доступном). Чтобы ViPNet Coordinator HW был доступен по доменному имени, назначьте ему дополнительное доменное имя в ViPNet Prime и затем отправьте на ViPNet Coordinator HW обновление справочников и ключей. В веб-интерфейсе просмотр доменного имени собственного координатора (Мой узел ViPNet) недоступен.

- `checkconnection_interval` — период автоматической отправки координатором сообщения другому связанному с ним координатору для оперативного определения недоступности этого координатора по текущему адресу доступа и попытки подключения к нему по альтернативному каналу доступа. Указывается в секундах, возможные значения: от 20 до 3600. Если данный параметр не указан в секции [id] координатора, то автоматическая проверка связи с ним будет производиться в соответствии с параметром `server_pollinterval`.
- `ip` — содержит реальный IP-адрес и соответствующий ему виртуальный IP-адрес узла. Первым указывается реальный адрес, затем после запятой — виртуальный (например: `ip = 192.168.201.10, 10.1.0.5)`. Если указан только реальный адрес, то считается, что ему еще не сопоставлен виртуальный.

  Если узел имеет несколько сетевых интерфейсов или несколько IP-адресов на интерфейсе, в каждой секции `[id]` может быть несколько параметров `ip`. Первым должен быть указан параметр, содержащий наиболее приоритетный IP-адрес доступа к данному узлу. При автоматическом обновлении адресов наиболее приоритетный IP-адрес доступа становится первым автоматически. При изменении порядка следования реальных IP-адресов, порядок следования виртуальных адресов не меняется.
- `port` — определяет порт назначения, на который следует посылать пакеты для узла, если этот узел находится за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр.
- `proxyid` — определяет режим работы узла, находящегося за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр. Возможные значения:
  - в собственной секции `[id]`:
    - `0xfffffffe` — при работе в режиме «С динамической трансляцией адресов», если в секции `[dynamic]` параметр `dynamic_proxy` установлен в `on` (см. Секция [dynamic]);
    - `0` — при работе в режиме «Со статической трансляцией адресов»;
  - в любой секции `[id]`, кроме собственной:
    - `0xfffffffe` — при работе в режимах «Со статической трансляцией адресов» или «С динамической трансляцией адресов», если ViPNet Coordinator HW является сервером соединений для узла;
    - идентификатор координатора — при работе в режиме «С динамической трансляцией адресов». Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`.
- `tcptunnelport` — номер порта координатора для входящих соединений по протоколу TCP. Возможные значения: от 0 до 65535, значение по умолчанию 80. Заданный порт используется для работы TCP-туннеля (см. параметр `tcptunnel_establish` секции `[misc]`).

Если параметр задан, то он автоматически рассылается на клиенты, для которых данный координатор служит сервером соединений.

- `tunnel` — содержит адреса незащищенных компьютеров, туннелируемых ViPNet Coordinator HW (указаны в собственной секции) или другими координаторами, в виде: `<ip1>-<ip2> to <ip3>-<ip4>`, где:
  - `<ip1>-<ip2>` — начальный и конечный реальные адреса диапазона туннелируемых узлов;
  - `<ip3>-<ip4>` — диапазон виртуальных адресов, которые соответствуют реальным адресам из диапазона `<ip1>-<ip2>`, и которые будут использоваться вместо реальных адресов туннелируемых узлов, если на узле, который к ним обращается, настроена видимость по виртуальным адресам. Например, если адреса из диапазона `<ip1>-<ip2>` относятся к внутренней сети и уже используются в локальной сети данного координатора. В частных случаях этот диапазон может совпадать с диапазоном `<ip1>-<ip2>`. Значение `ip4` формируется путем прибавления к `ip3` разницы между `ip2` и `ip1`.

  При этом учитывается параметр `tunnel_virt_assignment` секции `[misc]`, который может принимать одно из двух значений:

  - `auto` — при этом параметры `<ip1>` и `<ip2>` задаются администратором сети ViPNet в ViPNet Prime или вручную на ViPNet Coordinator HW.

    Например, чтобы в автоматическом режиме указать, что координатор туннелирует адреса с 192.168.0.1 по 192.168.0.100, достаточно сделать следующую запись:

    ```
    tunnel = 192.168.0.1-192.168.0.100
    ```

  - `manual` — при этом параметры `<ip1>-<ip2>` и `<ip3>` задаются вручную. Начальный адрес диапазона виртуальной видимости туннелируемых узлов `ip3` также необходимо указать вручную на каждом узле ViPNet, который будет работать с этими узлами.

    Например, чтобы вручную указать, что координатор туннелирует адреса с 192.168.0.1 по 192.168.0.100, а соответствующий им виртуальный диапазон адресов — 192.120.0.1-192.120.0.100, следует сделать следующую запись:

    ```
    tunnel = 192.168.0.1-192.168.0.100 to 192.120.0.1
    ```

  В одной секции `[id]` можно задать несколько параметров `tunnel`. Общее число заданных диапазонов туннелируемых узлов не должно превышать 1000.

Внимание! В зависимости от значения параметра `tunnel_virt_assignment` секции `[misc]`, настройки параметра `tunnel` действуют следующим образом:

- для автоматического режима назначения виртуальных адресов — можно задавать только первый и второй IP-адрес.
- для ручного режима назначения виртуальных адресов — можно задать значения всех четырех IP-адресов.

- `exclude_from_tunnels` — используется в любой секции `[id]`, кроме собственной. Исключает адреса из списка туннелируемых координатором адресов, указанных в параметре `tunnel`. Задается в виде: `ip1-ip2`, где `ip1` и `ip2` — начальный и конечный реальные адреса диапазона, который не надо туннелировать.

Например, чтобы исключить адрес 192.168.201.7 из туннелируемого диапазона 192.168.201.5-192.168.201.10 (то есть не шифровать трафик при соединении с узлом, имеющим адрес 192.168.201.7), сделайте следующую запись:

```
exclude_from_tunnels = 192.168.201.7-192.168.201.7
```

В одной секции `[id]` можно задать несколько таких параметров.

Внимание! Параметр `exclude_from_tunnels` имеет приоритет над настройками туннелирования, получаемыми из ViPNet Prime, и не изменяется при получении новых настроек туннелирования.

- `tunnel_local_networks` — параметр, который позволяет ViPNet Coordinator HW не туннелировать IP-адреса, входящие в локальную подсеть ViPNet Coordinator HW. Параметр задается в секциях [id] координаторов, связанных с ViPNet Coordinator HW. Возможные значения:
  - `on` (по умолчанию) — обращаться к туннелируемым узлам только через координатор, который туннелирует данные узлы;
  - `off` — обращаться к узлам, находящимся в локальной подсети, минуя координатор, который туннелирует эти узлы. Рекомендуется использовать в случае, если затруднен доступ к туннелируемым узлам в локальной подсети.
- `tunnelvisibility` — позволяет настроить тип видимости для всех узлов, туннелируемых координатором. Возможные значения:
  - `real` — всегда обращаться к туннелируемым узлам по их реальным адресам;
  - `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.

  При обновлении ViPNet Coordinator HW до версии 4.2.x и выше проверяется файл `iplir.conf` и в случае, если в какой-либо секции `[id]` есть назначенные виртуальные адреса, то параметру присваивается значение `virtual`. Значение данного параметра по умолчанию определяется параметром `tunneldefault` секции `[visibility]` (см. Секция [visibility]).
- `usetunnel` — используется в любой секции `[id]`, кроме собственной. Включает или выключает туннелирование координатором незащищенных узлов. Возможные значения: `on` (по умолчанию) или `off`. Если этот параметр на координаторе имеет значение `off`, то при соединении ViPNet Coordinator HW с узлами, которые туннелирует данный координатор, трафик шифроваться не будет.
- `visibility` — позволяет настроить тип видимости узла. Возможные значения:
  - `real` — всегда обращаться к данному узлу по его реальному адресу;
  - `virtual` — всегда обращаться к данному узлу по его виртуальному адресу.

  

  Внимание! Для узлов ViPNet, расположенных на мобильных устройствах, параметру `visibility` всегда автоматически присваивается значение `virtual`.

  Этот параметр не является обязательным и используется, только если для данного узла необходимо индивидуально задать тип видимости. В случае отсутствия параметра `visibility` видимость узла определяется параметрами секции `[visibility]` (см. Секция [visibility]), то

есть параметрами видимости всей сети, к которой этот узел принадлежит, либо параметрами видимости узлов по умолчанию.

Примечание. Использовать параметр `visibility` нужно осторожно, так как у сетевых узлов, которые видны по виртуальным адресам, могут совпадать реальные адреса (если эти узлы находятся в частных сетях).

Нередактируемые параметры

- `accessip` — текущий IP-адрес доступа к узлу со стороны ViPNet Coordinator HW. Может принимать значение одного из реальных или виртуальных IP-адресов, в зависимости от физической топологии сети, режимов подключения к внешней сети ViPNet Coordinator HW и данного узла.
- `always_use_server` — признак работы узла в режиме использования межсетевого экрана с динамической трансляцией адресов с направлением трафика через выбранный координатор. Параметр присутствует только в случае работы данного узла в указанном режиме и принимает значение `on`.
- `dynamic_timeout` — период опроса (в секундах) ViPNet-координатора, выбранного в качестве межсетевого экрана для данного узла, с целью обеспечения пропуска входящего трафика через межсетевой экран. Данный параметр присутствует во всех секциях `[id]`, кроме собственной.
- `id` — уникальный идентификатор узла. По этому параметру управляющая служба отличает одну секцию `[id]` от другой. Идентификатор присваивается сетевому узлу ViPNet при его создании в ViPNet Prime. В каждой секции `[id]` может быть только один такой параметр.
- `firewallip` — внешний IP-адрес доступа к узлу в случае, если этот узел находится за межсетевым экраном. При работе с узлом, установленным за межсетевым экраном, все направленные к нему зашифрованные пакеты инкапсулируются в единый UDP-пакет с адресом назначения, указанным в данном параметре, и портом назначения, указанным в параметре `port` данной секции. Если узел не находится за межсетевым экраном, то параметр `firewallip` отсутствует. В каждой секции `[id]` может быть только один такой параметр.
- `fixfirewall` — признак автоматического получения настроек собственного узла (внешний IP-адрес и порт доступа к ViPNet Coordinator HW) от узлов внешней сети для работы через внешний межсетевой экран. Возможное значение — `off`.
- `name` — имя узла. Задается администратором сети ViPNet в ViPNet Prime и предназначен для удобства настройки. Данный параметр записывается в конфигурационный файл автоматически при его сохранении. В каждой секции `[id]` может быть только один такой параметр.
- `virtualip` — базовый виртуальный адрес узла. В каждой секции `[id]` может быть только один такой параметр.
- `version` — версия протокола обмена служебной информацией между узлами сети ViPNet.

Секция [misc]

Секция `[misc]` содержит дополнительные параметры:

- `ciphertype` — алгоритм шифрования исходящих пакетов, адресованных сетевым узлам ViPNet. Может принимать только значение `gost` (шифрование с помощью алгоритма ГОСТ).
- `cef_enabled: yes` — запустить, `no` — остановить экспорт CEF.
- `cef_ip` — IP-адрес сетевого узла, на который будут посылаться сообщения CEF.

  Нельзя указывать локальный узел `localhost`, собственные IP-адреса и дополнительные IP-адреса (алиасы) интерфейсов.
- `cef_port` — порт UDP для передачи сообщений CEF. Значение по умолчанию — `514`.
- `cef_format` — режим формирования сообщений CEF:
  - `hw` — формирование полных сообщений CEF;
  - `ips` — формирование сообщений CEF только по событиям IPS 67 и 142 для совместимости с ViPNet TIAS.
- `client_pollinterval` — период опроса координатора ViPNet Coordinator HW клиентами, для которых он выполняет функцию сервера IP-адресов. Значение этого параметра координатор сообщает своим клиентам в каждом сеансе работы. Если от какого-либо клиента, который должен обмениваться пакетами с координатором, не было получено никаких служебных пакетов в течение времени, указанного в данном параметре, то такому клиенту посылается специальный пакет, на который должен прийти ответ. Если ответ не приходит, то узел клиента считается недоступным (выключенным). Указывается в секундах, значение по умолчанию — `300` (5 минут). Уменьшение значения данного параметра позволяет более оперативно определять неработоспособность узла, но повышает объем служебного трафика.
- `config_version` — версия модуля шифрования.
- `ifcheck_timeout` — период опроса параметров сетевых интерфейсов, известных управляющей службе. Указывается в секундах, значение по умолчанию — `30`.
- `iscaggregate` — включение или выключение накопления служебного трафика, обрабатываемого на координаторе. С помощью этого параметра вы можете снизить постоянную нагрузку на сеть за счет того, что служебный трафик будет накапливаться и передаваться периодически, а не постоянно. Возможные значения:
  - `on` (по умолчанию) — накопление служебного трафика происходит в течение минуты с последующей рассылкой на узлы не чаще, чем раз в минуту;
  - `off` — накопление служебного трафика выключено. В этом случае служебный трафик передается постоянно.
- `ipforwarding` — управление IP-форвардингом (маршрутизацией транзитных IP-пакетов через координатор ViPNet Coordinator HW). Возможные значения:
  - `on` — включать IP-форвардинг при запуске управляющей службы;
  - `off` — выключать IP-форвардинг при запуске управляющей службы;

- `system` — не изменять текущие настройки IP-форвардинга при запуске управляющей службы.

Примечание. При выключенном IP-форвардинге не работают пересылка транзитных IP-пакетов и туннелирование, поэтому рекомендуется устанавливать параметр `ipforwarding` в значение `on`. Значения `off` и `system` рекомендуется использовать только при отладке.

- `msg_compress_level` — степень сжатия служебных межсерверных сообщений. Возможные значения: от 1 (минимальное сжатие, максимальная скорость) до 9 (максимальное сжатие, минимальный объем служебного трафика). По умолчанию — `3`.

Примечание. На высоконагруженных узлах не рекомендуется устанавливать значение параметра `msg_compress_level` больше 5.

- `mssdecrease` — число байт, на которое будет уменьшен параметр MSS (максимальный размер сегмента) протокола TCP. По умолчанию — `0`.

  Уменьшать параметр MSS рекомендуется, если между вашим и другими защищенными или туннелируемыми узлами успешно проходит проверка соединения (ping), но не устанавливается TCP-соединение. Причиной блокирования шифрованных IP-пакетов, передаваемых в рамках TCP-соединения, может быть фрагментация этих IP-пакетов на устройствах, стоящих на пути от отправителя к получателю.

  Во избежание фрагментации рекомендуется уменьшить размер IP-пакетов, принимаемых на узле, присвоив параметру `mssdecrease` значение от 20 до 40 байт. Чтобы уменьшить размер исходящих IP-пакетов узла, значение параметра `mssdecrease` следует изменить на узле получателя этих IP-пакетов. Для установления TCP-соединения достаточно изменить параметр `mssdecrease` на одном из взаимодействующих узлов.

Внимание! Не изменяйте параметр `mssdecrease` без крайней необходимости.

- `packettype` — формат шифрованных пакетов. Возможные значения: `4.1` (по умолчанию) или `4.0`. Определяет только формат пакетов, отправляемых данным сетевым узлом. Формат входящих пакетов определяется автоматически, и их расшифрование производится независимо от установленного значения параметра `packettype`. Формат пакетов 4.0 рекомендуется использовать, если необходимо связываться с узлами, на которых установлены старые версии ПО ViPNet.
- `server_pollinterval` — период опроса данным координатором других координаторов. Если от какого-либо координатора, который должен обмениваться пакетами с данным координатором, не было получено никаких служебных пакетов в течение времени, указанного в данном параметре, то такому координатору направляется специальный пакет, на который должен прийти ответ. Если ответ не приходит, то узел координатора считается недоступным (выключенным). Указывается в секундах, значение по умолчанию — `900` (15 минут).
- `tcptunnel_establish` — включение или выключение TCP-туннеля. Возможные значения: `on` или `off` (по умолчанию). Для входящих соединений по протоколу TCP по умолчанию используется порт 80 — параметр `tcptunnelport` секции `[id]`.

- `timediff` — максимально допустимая разница между временем отправки и приема IP-пакетов. Из соображений безопасности драйвер ViPNet блокирует входящие IP-пакеты, если время их отправки отличается от времени их приема более чем на число секунд, указанное в этом параметре. Значение параметра должно быть не меньше 1 секунды и не больше 7200 секунд. Значение по умолчанию — `7200` (2 часа).
- `timesync` — параметр используется только для клиентского ПО, на координаторе значение установлено в `off`, изменять его нельзя.
- `tunnel_virt_assignment` — режим назначения виртуальных адресов для узлов, туннелируемых координатором:
  - `auto` (по умолчанию) — задаются автоматически;
  - `manual` — задаются вручную в параметрах `tunnel` и `exclude_from_tunnels` секции `[id]`.

Внимание! После обновления ПО ViPNet Coordinator HW до версии 4.5.2 и выше ручная настройка виртуальных адресов туннелируемых узлов сохраняется. В случае автоматической настройки все виртуальные адреса для туннелируемых узлов будут переназначены.

- `warnoldautosave` — включение или выключение предупреждения о наличии конфигураций, содержащих настройки ПО ViPNet, которые были автоматически сохранены более месяца назад. Возможные значения: `on` (по умолчанию) или `off`. Если параметр установлен в значение `on`, то предупреждения выводятся каждый раз при запуске управляющей службы.

Секция [servers]

Секция `[servers]` содержит список координаторов, известных данному сетевому узлу. Каждому координатору соответствует один нередактируемый параметр `server`, в котором через запятую указаны идентификатор координатора и его имя.

Секция [virtualip]

Секция `[virtualip]` описывает настройки виртуальных IP-адресов и содержит параметры:

- `maxvirtualip` — максимальный адрес для формирования базовых виртуальных адресов защищенных узлов (по умолчанию параметр не используется). Используется для задания верхнего ограничения диапазона назначаемых базовых виртуальных адресов вручную. Значение параметра `maxvirtualip` должно быть больше значения параметра `startvirtualip`.
- `startvirtualip` — стартовый адрес для формирования базовых виртуальных адресов защищенных узлов (значение по умолчанию — `11.0.0.1`). При изменении данного параметра назначение всех базовых виртуальных адресов узлов производится заново, как при начальном формировании файлов конфигурации. Кроме того, для узлов производится назначение виртуальных адресов в параметрах `ip`.

- `starttunnelvirtualip` — стартовый адрес для формирования диапазонов виртуальных адресов туннелируемых узлов в автоматическом режиме (по умолчанию для диапазонов адресов туннелируемых узлов — `12.0.0.1`, для адресов одиночных туннелируемых узлов — `11.0.0.1`).

Секция [visibility]

Секция `[visibility]` содержит настройки видимости защищенных сетевых узлов, с которыми связан ViPNet Coordinator HW. В отличие от параметра `visibility`, с помощью которого в секциях [id] задается видимость отдельных узлов, в этой секции можно задать видимость сразу для всех узлов сетей или подсетей ViPNet. Настройки, заданные в секции `[visibility]`, учитываются при определении видимости узлов со стороны собственного узла.

Секция может содержать параметры:

- `default` — видимость узлов по умолчанию. Возможные значения:
  - `real` — доступ к узлам по их реальным IP-адресам;
  - `virtual` (по умолчанию) — доступ к узлам по их виртуальным IP-адресам.
- `subnet_real` — идентификаторы сетей ViPNet, для которых настраивается видимость узлов по реальным IP-адресам.

  Идентификатор сети вы можете посмотреть в ViPNet Prime или с помощью команды `iplir info`. Идентификаторы сетей указываются в шестнадцатеричном формате с префиксом `0x`. В одной секции `[visibility]` можно задать несколько параметров `subnet_real`. При этом в каждом параметре можно указать либо один идентификатор, либо несколько идентификаторов через запятую. Например:

  ```
  subnet_real = 0x5155
  subnet_real = 0x5156,0x5157,0x5158
  ```
- `subnet_virtual` — идентификаторы сетей ViPNet, для которых настраивается видимость узлов по виртуальным IP-адресам. Задается так же, как параметр `subnet_real`.

Внимание! Один и тот же идентификатор сети ViPNet можно указать только в одном из параметров `subnet_real` или `subnet_virtual`.

  Параметры `subnet_real` и `subnet_virtual` являются необязательными и по умолчанию отсутствуют в секции `[visibility]`.

  При старте управляющей службы идентификаторы, заданные в параметрах `subnet_real` и `subnet_virtual` автоматически сортируются в порядке возрастания и группируются в строки, каждая из которых содержит максимум 8 идентификаторов.
- `tunneldefault` — тип видимости для всех узлов, туннелируемых координатором, который будет указываться по умолчанию вне зависимости от режима назначения адресов туннелируемых узлов (см. параметр `tunnel_virt_assignment` секции `[misc]`) при отсутствии в секции `[id]` параметра `tunnelvisibility`. Возможные значения:

- `real` (по умолчанию) — всегда обращаться к туннелируемым узлам по их реальным адресам;
- `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.

Файл iplir.conf-<интерфейс или группа интерфейсов>

Параметры журнала прохождения трафика через любой активный сетевой интерфейс настраиваются в конфигурационных файлах `iplir.conf-<интерфейс или группа интерфейсов>`. Для каждого статического интерфейса, описанного секцией `[adapter]` в файле `iplir.conf` (см. Секция [adapter]), а также для каждой группы динамических интерфейсов управляющая служба при запуске автоматически создает такой файл с параметрами по умолчанию.

Примечание. В ViPNet Coordinator HW по умолчанию разрешена работа динамических интерфейсов, которые входят в одну из групп:

- `ppp` — интерфейсы для встроенных модемов;
- `wifi` — интерфейсы для внешних адаптеров Wi-Fi. В эту группу не входит встроенный интерфейс `wlan0`.

Чтобы отредактировать файл `iplir.conf-<интерфейс или группа интерфейсов>`:

1. Остановите управляющую службу:

   ```
   hostname# iplir stop
   ```

2. Откройте файл для редактирования:

   ```
   hostname# iplir config <интерфейс или группа интерфейсов>
   ```

3. Выполните изменения.

4. Запустите управляющую службу:

   ```
   hostname# iplir start
   ```

Внимание! Конфигурационный файл `iplir.conf-<интерфейс>` может отсутствовать для статического интерфейса, если соответствующая секция `[adapter]` была добавлена в файл `iplir.conf` вручную и после этого управляющая служба не перезапускалась. Поэтому после добавления секций `[adapter]` в файл `iplir.conf`:

1. Запустите управляющую службу: `iplir start`.
2. Завершите работу управляющей службы: `iplir stop`.
3. Отредактируйте нужный файл `iplir.conf-<интерфейс>`.
4. Запустите управляющую службу: `iplir start`.

Секция [db]

Для каждого статического интерфейса и группы динамических интерфейсов ведется свой журнал IP-пакетов, который хранится в файле `iplir.db-<интерфейс или группа интерфейсов>`, расположенном в подкаталоге `iplirdb` каталога, содержащего файлы `iplir.conf-<имя интерфейса или группа интерфейсов>`.

Записи о пакетах регистрируются в журнале до тех пор, пока не будет достигнут его максимальный размер, после чего самые ранние записи стираются и на их место записываются новые. Для уменьшения размера журнала, а также для удобства его просмотра одинаковые записи о пакетах, зарегистрированные в течение заданного времени, объединяются в одну запись. Поэтому при просмотре журнала можно узнать, сколько раз было зафиксировано событие, описываемое этой записью.

Секция `[db]` содержит параметры:

- `maxsize` — максимальный размер журнала, Мбайт.

  Значение параметра по умолчанию и максимальное значение зависят от исполнения ViPNet Coordinator HW:

  Таблица 6. Размер по умолчанию и максимальный размер журнала IP-пакетов

Исполнение	Размер по умолчанию (Мбайт)	Максимальный размер (Мбайт)
HW50	10	10
HW100	50	50
HW1000	50	для физических интерфейсов — 1800 для виртуальных интерфейсов — 200
HW2000	50	для физических интерфейсов — 1800 для виртуальных интерфейсов — 200
HW5000	50	для физических интерфейсов — 1800 для виртуальных интерфейсов — 200
ViPNet Coordinator VA	50	для физических интерфейсов — 1800 для виртуальных интерфейсов — 200

  Каждый раз при запуске управляющей службы в значение параметра `maxsize` после размера журнала автоматически дописывается слово `MBytes`, если оно отсутствует. Поэтому при изменении значения этого параметра его можно не писать. Значение параметра `0` выключает ведение журнала. При этом если до выключения журнала в нем были записи, то просмотреть их будет невозможно.

- `timediff` — интервал времени, в течение которого одинаковые события объединяются в журнале в одну запись. Задается в секундах, значение по умолчанию — `60`. Если этот параметр установлен в `0`, то объединение событий не используется. В этом случае при интенсивном трафике в журнале могут регистрироваться не все пакеты.
- `registerall` — включение или выключение регистрации записей обо всех пакетах, проходящих через интерфейс. Возможные значения: `off` (по умолчанию) или `on`. То есть по умолчанию регистрируются только записи о блокированных пакетах и изменении адресов сетевых узлов.
- `registerbroadcast` — включение или выключение регистрации записей о широковещательных пакетах. Возможные значения: `off` (по умолчанию) или `on`.

- `omittcpclientport` — включение или выключение скрытия информации о порте клиента ViPNet при соединении по протоколу TCP. Возможные значения: `off` (по умолчанию) или `on`.

  Обычно порт клиента при TCP-соединении выделяется динамически и никакой полезной информации не несет. Если с какого-либо сетевого ресурса производятся попытки подключиться к какому-либо порту на компьютере, а соединение по каким-то причинам не будет установлено, то при следующей попытке установить соединение с того же ресурса будет использоваться другой порт. При использовании сканеров портов или каких-либо сетевых атаках число таких попыток может достигать нескольких сотен в секунду. Поскольку клиент использует каждый раз разные порты, то такие пакеты не считаются одинаковыми и для каждого из них создается своя запись в журнале, что засоряет его и затрудняет последующий анализ. Если параметр `omittcpclientport` установлен в значение `on`, порт клиента при TCP-соединении не регистрируется и не учитывается, а в журнале числовое значение номера порта указывается равным нулю, что позволяет объединить события о попытках подключения к какому-либо порту на компьютере с определенного адреса в одну запись. Это часто бывает удобно.

- registerevents — включение или выключение регистрации служебных событий. Список служебных событий см. в документе «Настройка с помощью командного интерпретатора», в приложении «Типы событий журнала IP-пакетов». Возможные значения: `off` или `on` (по умолчанию).

Секция [cef]

Секция `[cef]` содержит следующие параметры:

- `event` — формирование сообщений CEF при регистрации IP-пакетов, проходящих через интерфейс:
  - `all` — для всех IP-пакетов;
  - `blocked` — для блокированных IP-пакетов или с предупреждением о вторжении (значение по умолчанию);
- `exclude` — формирование сообщений CEF, заданных в `event`, за исключением указанных номеров типов событий. Их перечисление допускается в любом порядке через запятую.

Файл failover.ini

Настройка параметров работы системы защиты от сбоев осуществляется путем редактирования конфигурационного файла `failover.ini`.

Чтобы отредактировать файл `failover.ini`:

1. Завершите работу службы `failoverd`:

   ```
   hostname# failover stop
   ```

2. Откройте файл для редактирования:

   ```
   hostname# failover config edit
   ```

3. Внесите изменения.

4. Запустите службу `failoverd`:

   ```
   hostname# failover start
   ```

Секция [channel]

Каждый сетевой интерфейс активного узла, работоспособность которого должна контролироваться системой защиты от сбоев при работе в режиме кластера, должен быть описан секцией `[channel]`. Это необходимо для своевременного обнаружения неработоспособности интерфейса и переключения кластера.

Примечание. Параметры секций `[channel]` интерпретируются только при работе системы защиты от сбоев в режиме кластера.

Чтобы отключить контроль работоспособности какого-либо интерфейса, удалите из файла `failover.ini` соответствующую секцию `[channel]`.

Секция `[channel]` содержит параметры:

- `activeip` — IP-адрес и маска, которые будет иметь интерфейс активного узла кластера. Маска может быть указана после IP-адреса через символ «/» в нотации CIDR или в прямой нотации. Например:
  - в нотации CIDR: `activeip = 192.168.201.1/24`
  - в прямой нотации: `activeip = 68.21.12.34/255.255.252.0`

  Примечание. Независимо от того, в какой нотации была указана маска, после сохранения файла `failover.ini` и запуска службы `failoverd` маска будет перезаписана в нотации CIDR.

- `checkonlyidle` — указание на необходимость проверки только неактивных интерфейсов:
  - `yes` (по умолчанию) — активный узел посылает echo-запросы на интерфейсы, адреса которых указаны в соответствующих параметрах `testip`, только если за период опроса

IP-адресов, указанный в параметре `checktime` в секции `[network]`, на данных интерфейсах не было или входящих или исходящих пакетов;

- `no` — echo-запросы на интерфейсы, адреса которых указаны в соответствующих параметрах `testip`, посылаются постоянно.

- `device` — имя интерфейса (`eth0`, `eth1` и так далее).
- `ident` — текстовая строка, идентифицирующая интерфейс. Для интерфейсов, подключенных к одинаковым сетям, параметры `ident` должны совпадать.

Примечание. Не рекомендуется использовать разные имена (несимметричные конфигурации) интерфейсов кластера.

- `testdevice` — имя сетевого интерфейса, для которого необходимо контролировать состояние физического соединения. При потере соединения на указанном интерфейсе будет выполнено переключение узлов кластера.

  В качестве сетевого интерфейса в параметре `testdevice` вы можете указать только физический интерфейс. Не допускается задавать виртуальные, агрегированные или VLAN интерфейсы, а также `localhost`. При этом вы можете указать физический интерфейс, который задан как trunk-интерфейс для VLAN.

  В каждой секции `[channel]` можно задать только один параметр `testdevice`.

Внимание!

- Не изменяйте параметры сетевого интерфейса, указанного в `testdevice`, если служба `failoverd` запущена в режиме кластера. Иначе это будет воспринято системой как потеря физического соединения и приведет к переключению узлов кластера.
- В качестве `device` и `testdevice` указывайте только те сетевые интерфейсы, состояние которых действительно должно контролироваться для работоспособности кластера.

- `testip` — IP-адрес маршрутизатора или другого стабильного объекта сети, которому будут посылаться эхо-запросы для проверки работоспособности интерфейса.

  При необходимости можно для каждого из интерфейсов указать несколько параметров `testip`. В этом случае сбоем интерфейса будет считаться ситуация, когда ни от одного из заданных IP-адресов не будет получено ответа.

  Например, чтобы эхо-запросы отправлялись на IP-адреса 192.168.100.34 и 192.168.100.25, добавьте следующие строки:

```
testip = 192.168.100.34
testip = 192.168.100.25
```

Внимание! Для каждого интерфейса, описанного секцией `[channel]`, в параметре `testip` должен быть задан свой адрес, принадлежащий подсети данного интерфейса.

Если в параметре `testip` один и тот же адрес указан для нескольких интерфейсов, будет проверяться работоспособность только сетевого интерфейса, указанного в конфигурационном файле первым.

Если в параметре `testip` задан адрес, не принадлежащий подсети данного интерфейса, то для этого адреса должен быть задан статический маршрут или шлюз по умолчанию.

В качестве параметра `testip` не рекомендуется задавать адрес интерфейса «внутренней петли» (loopback), например, `127.0.0.1`, так как в этом случае реальной проверки работоспособности сетевого интерфейса не производится.

- `usevirtualmac` — включает или выключает использование виртуальных MAC-адресов для сетевых интерфейсов кластера, заданных в данной секции `[channel]`. Возможные значения:
  - `yes` — использовать виртуальные MAC-адреса для сетевых интерфейсов;
  - `no` (по умолчанию) — не использовать виртуальные MAC-адреса для сетевых интерфейсов.

  Использование параметра `usevirtualmac` имеет особенности:
  - Виртуальные MAC-адреса для сетевых интерфейсов кластера генерируются на основе значения параметра `virtualmacprefix` в секции `[network]`.
  - Если параметр `usevirtualmac` включен, то на активном узле кластера для сетевых интерфейсов, описанных в данной секции `[channel]`, используются виртуальные MAC-адреса, а после переключения в пассивном режим для интерфейсов восстанавливаются аппаратно заданные MAC-адреса.
  - Если параметр `usevirtualmac` выключен, то система не проверяет MAC-адреса на сетевых интерфейсах кластера.
  - Если параметр `usevirtualmac` использовался и затем был выключен, то для сетевых интерфейсов кластера могут использоваться виртуальные MAC-адреса до перезагрузки ViPNet Coordinator HW. Чтобы сбросить MAC-адреса, перезагрузите ViPNet Coordinator HW с помощью команды `machine reboot`.
  - Для работы этой функции настройте коммутационное оборудование таким образом, чтобы разрешить использование двух MAC-адресов для одного Ethernet-порта.

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала событий службы `failoverd` и содержит параметры:

- `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `-1` до `4` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация записывается в журнал. Значение параметра `-1` выключает ведение журнала (при этом некоторые важные системные события по-прежнему будут выводиться в журнал).

Уровень важности `4` используется только для диагностики возможных проблем и должен быть включен по рекомендации специалистов ИнфоТеКС. Не задавайте его для постоянного использования.

Внимание! В исполнениях с одним дисковым накопителем:

- По умолчанию уровень важности равен `1`.
- При локальном протоколировании доступны уровни важности от `-1` до `3`.

При удаленном протоколировании доступны уровни важности от `-1` до `4`. При этом если вы используете `4` уровень и выполняете переключение на локальное протоколирование, уровень не изменяется автоматически. Чтобы уровень важности принял значение по умолчанию, перезагрузите службу `failoverd`: failover stop и failover start.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

  Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

Секция [misc]

Секция `[misc]` содержит дополнительные параметры работы системы защиты от сбоев в режиме кластера и в одиночном режиме:

- `maxjournal` — максимальное количество дней, за которое необходимо хранить записи в журнале переключений кластера. По умолчанию это ограничение отсутствует.
- `reboot` — действие системы в случае обнаружения полной неработоспособности какой-либо службы или драйвера ViPNet Coordinator HW:
  - `yes` (по умолчанию) — включить механизм регистрации в watchdog-драйвере и перезагружать систему, если какая-либо служба или драйвер не может восстановить свою работу;
  - `no` — выключить механизм регистрации в watchdog-драйвере и не перезагружать систему, если какая-либо служба или драйвер не может восстановить свою работу.
- `syncalgtcp` — синхронизация сессий прикладных протоколов DNS, FTP, H.323, SCCP, SIP в кластере:
  - `yes` — включить синхронизацию сессий;
  - `no` (по умолчанию) — выключить синхронизацию сессий.
- `syncconnections` — синхронизация сетевых соединений в кластере:

- `yes` — включить синхронизацию соединений. В этом случае при переключении узлов кластера соединения, открытые на активном узле до момента переключения узлов, продолжат работу на пассивном узле после его переключения в активный режим. При этом не будут синхронизированы следующие типы соединений:
  - открытые сессии разрешения доменных имен;
  - защищенные соединения по TCP-туннелям;
  - локальные соединения (открытые и защищенные соединения, в которых сетевой узел ViPNet Coordinator HW является источником или назначением);
  - соединения, использующие прикладные протоколы.

  После переключения узлов кластера связь по указанным типам соединений может быть прервана.
- `no` (по умолчанию) — выключить синхронизацию соединений.

Для синхронизации соединений параметр должен иметь значение `yes` на обоих узлах кластера.

- `syncdatetime` — синхронизация времени и часового пояса между узлами кластера.
  - `yes` (по умолчанию) — включить синхронизацию времени между узлами кластера: активный узел кластера передает пассивному узлу данные времени и часового пояса;
  - `no` — выключить синхронизацию времени между узлами кластера.

  Значение параметра должно быть одинаковым для обоих узлов кластера (для корректного переключения их режимов работы).
- `interclustermtu` — значение MTU на интерфейсах синхронизации кластера; по умолчанию — 1500 байт.

Нередактируемые параметры секции [misc]

- `activeconfig` — абсолютный путь к файлу конфигурации управляющей службы, который будет использоваться на активном узле кластера. Значение по умолчанию — `/etc/iplirpsw`.
- `passiveconfig` — абсолютный путь к файлу конфигурации управляющей службы, который будет использоваться на пассивном узле кластера. Значение по умолчанию — `/etc/iplirpsw`.

Примечание. Параметры `activeconfig`, `passiveconfig` и `maxjournal` интерпретируются только при работе системы защиты от сбоев в режиме кластера.

Секция [network]

Секция `[network]` описывает параметры работы системы защиты от сбоев, относящиеся к посылке пакетов в сеть в режиме кластера.

Примечание. Все параметры секции `[network]` интерпретируются только при работе системы защиты от сбоев в режиме кластера.

Все параметры этой секции рекомендуется настроить одинаково на обоих узлах кластера.

Секция `[network]` содержит параметры:

- `activeretries` — количество неуспешных попыток опроса пассивным узлом активного узла, после которых делается вывод об отсутствии активного узла с опрашиваемым IP-адресом. По умолчанию — `3`.
- `channelretries` — количество неуспешных попыток опроса интерфейса тестового узла, после которых этот интерфейс считается неработоспособным. По умолчанию — `3`.
- `checktime` — период опроса:
  - на активном узле — для проверки работоспособности интерфейса;
  - на пассивном узле — для поиска IP-адресов активного узла.

  Указывается в секундах, по умолчанию — `10`.

  Внимание! Значение параметра `checktime` должно быть больше, чем значение параметра `timeout`.
- `fastdown` — указывает на принудительное выключение сетевых интерфейсов перед перезагрузкой узла. Возможные значения: `yes` (по умолчанию) или `no`. Значение, выбранное по умолчанию, позволяет быстрее установить отсутствие активного узла в сети и дать возможность второму узлу перейти в активный режим, однако при этом завершение работы сетевых служб происходит уже при выключенных интерфейсах и может быть некорректным.
- `synctime` — период отправки пакетов синхронизации между узлами кластера. Указывается в секундах, значение по умолчанию — `5`.
- `timeout` — время ожидания ответа на запрос (эхо-запрос или запрос IP-адресов активного узла), по истечении которого делается вывод о неуспешности этого запроса. Указывается в секундах, по умолчанию — `2`.
- `virtualmacprefix` — исходное значение для расчета первого октета виртуального MAC-адреса, генерируемого для сетевых интерфейсов кластера (см. описание параметра `usevirtualmac` в секции `[channel]`). Указывается в десятичном виде, значение по умолчанию — `39`.

  Виртуальный MAC-адрес для IP-адреса интерфейса генерируется следующим образом:
  - 1-й октет: вычисляется на основе значения параметра `virtualmacprefix`;
  - 2-й—5-й октеты: активный IP-адрес сетевого интерфейса в шестнадцатеричном виде;
  - 6-й октет: 0.

  Например, для IP-адреса 10.20.2.1 при значении параметра `virtualmacprefix` по умолчанию будет сгенерирован виртуальный MAC-адрес 9e:0a:14:02:01:00.

  Значения параметра `virtualmacprefix` должны совпадать на активном и пассивном узлах кластера.

Секция [sendconfig]

В секции `[sendconfig]` задаются параметры, контролирующие отправку конфигурационных файлов с активного узла на пассивный для их резервирования и синхронизации настроек узлов кластера.

Примечание. Все параметры секции `[sendconfig]` интерпретируются только при работе системы защиты от сбоев в режиме кластера.

Секция `[sendconfig]` содержит параметры:

- `activeip` — IP-адрес интерфейса синхронизации другого узла кластера.
- `config` — включение или выключение резервирования группы конфигурационных файлов. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят следующие конфигурационные файлы:
  - `iplir.conf`;
  - `iplir.conf-<интерфейс или группа интерфейсов>`, кроме файла для интерфейса синхронизации;
  - `mftp.conf` (см. Файл mftp.conf);
  - файлы, содержащие сетевые фильтры и правила трансляции (заданные пользователем и полученные из Policy Management (модуль ViPNet Prime));
  - файлы с настройками функции L2OverIP;
  - файлы `*.crg` с контрольными суммами конфигурационных файлов;
  - файлы с настройками маршрутизации и статическими маршрутами (если такие создавались);
  - другие служебные конфигурационные файлы.
- `connectport` — номер порта, используя который данный узел кластера при работе в пассивном режиме соединяется с активным узлом и принимает от него файлы для резервирования. По умолчанию этот параметр отсутствует и равен значению параметра `port` данной секции.

  

  Внимание! Номер порта, заданный в параметре `connectport`, по умолчанию используется пассивным узлом кластера для проверки доступности сетевых интерфейсов активного узла, поэтому изменять значение этого параметра без явной необходимости не рекомендуется.

- `device` — имя интерфейса синхронизации текущего узла кластера.

  

  Внимание! Запрещено использовать имена дополнительных (alias) или агрегированных (bond) интерфейсов.

- `file` — абсолютный путь к файлу для резервирования. По умолчанию отсутствует. В секции может быть несколько таких параметров, в каждом из которых может быть указан любой файл, который требуется резервировать и который не входит в группы конфигурационных файлов (`config`), файлов справочников и ключей (`keys`) и файлов журналов (`journals`). Размер указанного файла не должен превышать 1 Мбайт, и для его пересылки должно быть достаточно времени, указанного в параметре `sendtime` данной секции.

Примечание. Чтобы выбрать для резервирования не все, а один или несколько файлов, входящих в группы конфигурационных файлов или журналов, установите параметр `config` или `journal` в значение `no` и укажите нужные файлы в параметрах `file`.

- `journals` — включение или выключение резервирования группы файлов журналов ПО ViPNet. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят:
  - файлы журналов IP-пакетов сетевых интерфейсов, кроме интерфейса синхронизации;
  - файлы журнала конвертов транспортного сервера MFTP;
  - другие служебные файлы журналов.
- `keys` — включение или выключение резервирования группы файлов справочников и ключей. Возможные значения: `yes` (по умолчанию) или `no`.

Внимание! Набор файлов, входящих в группы конфигурационных файлов (`config`), файлов справочников и ключей (`keys`) и файлов журналов (`journals`), определяется службой `failoverd` автоматически на активном узле. Пассивный узел в каждом цикле синхронизации запрашивает сначала список файлов, входящих в каждую группу, для которой включено резервирование, и другие файлы для резервирования (`file`), а затем инициирует передачу этих файлов.

Резервирование групп файлов производится только при запущенных на активном узле службах `iplircfg` и `mftpd`, а также если параметры `config`, `keys` и `journal` установлены в значение `yes`. Не рекомендуем отключать резервирование групп файлов, так как это может привести к некорректной работе ПО ViPNet.

- `port` — номер порта, на котором данный узел кластера при работе в активном режиме ожидает соединения от пассивного узла, чтобы передать ему файлы для резервирования. По умолчанию — `10090`.
- `sendtime` — период резервирования файлов, то есть период между попытками пересылки файлов для синхронизации настроек узлов кластера. Указывается в секундах, по умолчанию — `60`.

Файл mftp.conf

Параметры работы транспортного сервера MFTP содержатся в файле `mftp.conf`.

Чтобы отредактировать файл `mftp.conf`:

1. Завершите работу службы `mftpd`:

   ```
   hostname# mftp stop
   ```

2. Откройте файл для редактирования:

   ```
   hostname# mftp config
   ```

3. Внесите изменения.

4. Запустите службу `mftpd`:

   ```
   hostname# mftp start
   ```

Секция [channel]

Секции `[channel]` содержат настройки каналов, по которым ViPNet Coordinator HW может обмениваться данными с другими узлами. Каждому узлу, зарегистрированному за ViPNet Coordinator HW в ViPNet Prime (координатор является сервером IP-адресов), а также каждому координатору, с которым есть межсерверный канал связи, соответствует своя секция `[channel]`.

Внимание! Добавление и удаление секций `[channel]` осуществляется автоматически, делать это вручную не следует.

Секции `[channel]` содержат следующие параметры:

- `type` — тип канала: `mftp`.
- `off_flag` — признак выключения канала. Возможные значения:
  - `no` (по умолчанию) — канал включен. В этом случае попытка передачи конверта по каналу производится немедленно.
  - `yes` — канал выключен. В этом случае исходящие конверты, передаваемые по каналу, остаются в очереди до тех пор, пока канал не будет включен или инициатором соединения по данному каналу не станет удаленный транспортный сервер (координатор). Если инициатором соединения станет удаленный клиент, то предназначенные ему конверты не отправляются, а этому клиенту передается специальная команда, которая выключает соответствующий канал в настройках его транспортного сервера.
- `call_flag` — признак немедленной передачи конвертов по каналу MFTP:
  - `yes` — попытка передачи конверта по каналу производится немедленно (по умолчанию для каналов обмена с координаторами);

- `no` — конверт остается в очереди до тех пор, пока инициатором соединения не станет удаленный узел (по умолчанию для каналов обмена с клиентами).

Примечание. Если параметры `type`, `off_flag`, `call_flag` отсутствуют в секции, то используются их значения по умолчанию.

- `ip` — IP-адрес удаленного сетевого узла. Определяется управляющей службой. Если значение этого параметра по каким-либо причинам не было получено от управляющей службы, то оно будет установлено в `0.0.0.0`. В этом случае его можно задать вручную, а затем перезапустить транспортный сервер. Данный параметр может изменяться в процессе работы.
- `call_timeout` — период опроса удаленного сетевого узла в секундах (время следующего опроса узла отсчитывается с момента разрыва последнего соединения с этим узлом). По умолчанию имеет значение `-1`, то есть опрос не производится. Если параметр `call_timeout` отсутствует, то используется его значение по умолчанию.
- `transit` — идентификатор узла, на который необходимо перенаправлять конверты, отправляемые по данному каналу. Используется для настройки каналов обмена с координаторами при межсетевом взаимодействии и позволяет снизить нагрузку на шлюзовой координатор за счет передачи через него конвертов без обработки транспортным сервером. Задается в шестнадцатеричном формате с префиксом `0x`.

  По умолчанию параметр `transit` отсутствует, и при межсетевом взаимодействии используется значение, заданное в ViPNet Prime. Если параметр указан, изменение значения в ViPNet Prime не учитывается.

Нередактируемые параметры

- `id` — уникальный идентификатор сетевого узла ViPNet, с которым происходит обмен данными по каналу. Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`, например: `id = 0x270e000a`.
- `name` — имя сетевого узла ViPNet, с которым происходит обмен данными по каналу.
- `last_port` — порт, по которому осуществлялось последнее удачное MFTP-соединение. Этот порт будет использоваться при следующей попытке соединения с этим узлом.
- `last_call` — время последней попытки опроса канала.
- `last_err` — время, когда произошла последняя ошибка при попытке соединения или в процессе передачи данных.

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала событий транспортного сервера MFTP и содержит следующие параметры:

- `debuglevel` — уровень важности событий, записываемых в журнал. Возможные значения: от `-1` до `4` (по умолчанию `3`). Чем выше уровень важности, тем более подробная информация

записывается в журнал. Значение параметра `-1` выключает ведение журнала (при этом некоторые важные системные события по-прежнему будут выводиться в журнал).

Уровень важности `4` используется только для диагностики возможных проблем и должен быть включен по рекомендации специалистов ИнфоТеКС. Не задавайте его для постоянного использования.

Внимание! В исполнениях с одним дисковым накопителем:

- По умолчанию уровень важности равен `1`.
- При локальном протоколировании доступны уровни важности от `-1` до `3`.

При удаленном протоколировании доступны уровни важности от `-1` до `4`. При этом если вы используете `4` уровень и выполняете переключение на локальное протоколирование, уровень не изменяется автоматически. Чтобы уровень важности принял значение по умолчанию, перезагрузите транспортный сервер MFTP с помощью команд mftp stop и mftp start.

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
  - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы) или `daemon` (системные службы).
  - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

  Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

Секция [journal]

Секция `[journal]` содержит параметры настройки журнала MFTP-конвертов, обрабатываемых транспортным сервером. В процессе работы транспортный сервер записывает в этот журнал информацию о полностью принятых, отправленных, удаленных и поврежденных конвертах.

Секция `[journal]` содержит следующие параметры:

- `dump_interval` — период выгрузки информации из журнала конвертов в днях. В процессе работы транспортный сервер записывает информацию об обработанных конвертах в текущий файл дампа. По истечении периода времени, заданного данным параметром, создается новый файл дампа, в имени которого содержится текущая дата. По умолчанию каждый день создается новый файл дампа (`dump_interval = 1`).
- `max_size` — максимальный размер файла журнала конвертов в мегабайтах (по умолчанию — `1`). Если размер текущего файла журнала превышает значение этого параметра, то новая информация будет записываться в этот файл на место информации, которая была записана раньше остальной. В случае изменения значения этого параметра, если размер этого файла превышает новое значение, то из него удаляется информация, которая была записана раньше остальной.

Внимание! Не рекомендуется задавать размер журнала более чем 100 мегабайт, так как при превышении этого значения могут возникнуть проблемы с просмотром журнала конвертов в веб-интерфейсе.

- `use_journal` — включение или выключение ведения журнала работы транспортного сервера. Возможные значения: `yes` (по умолчанию) или `no`.

Примечание. Если параметры `dump_interval`, `max_size`, `use_journal` отсутствуют в секции, то используются их значения по умолчанию.

Нередактируемые параметры

- `dump_filename` — префикс имени текстового файла, в который регулярно выгружается информация из журнала конвертов (файла дампа). Значение по умолчанию — `/var/log/mftpenv.log`.

  Постфикс имени этого файла определяется текущей датой и зависит от периода выгрузки информации (см. параметр `dump_interval` данной секции). Пример имени файла дампа: `/var/log/mftpenv.log.2024.09.23`.

- `last_dump` — время последней выгрузки информации из журнала конвертов.

Секция [misc]

Секция `[misc]` содержит различные параметры, определяющие работу транспортного сервера MFTP в целом:

- `connect_timeout` — интервал времени в секундах, в течение которого клиент будет пытаться установить соединение с удаленным узлом по каналу MFTP (от `2` до `300`, по умолчанию — `5`). Если по истечении этого времени соединение не установлено, то повторные попытки соединения будут производиться по истечении времени, указанного в параметре `outenv_timeout` данной секции.
- `max_connections` — максимальное количество входящих и исходящих соединений по каналам MFTP (от `1` до `1000`, по умолчанию — `900`).
- `max_listen_ports` — диапазон значений перебора портов для соединений по каналу MFTP с удаленным узлом в случае неудачи (от `1` до `10`, по умолчанию — `3`). Транспортный сервер циклично перебирает порты в диапазоне от `port` до `port+max_listen_ports-1`. Ожидая входящие соединения, транспортный сервер прослушивает все порты указанного диапазона.
- `num_attempts` — количество последовательных попыток соединения, после которых устанавливается тайм-аут, если соединиться так и не удалось (от `1` до `10`, по умолчанию — `3`).
- `outenv_timeout` — интервал времени в секундах, в течение которого исходящие конверты для канала, на котором произошла ошибка передачи, не могут быть повторно отправлены (от `5` до `600`, по умолчанию — `300`). Если на каком-либо канале произошла ошибка передачи (например, из-за разрыва соединения) и для этого канала существуют исходящие конверты, то

следующая попытка передачи произойдет по истечении времени, указанного в параметре `outenv_timeout`.

- `pingpong` — включение или выключение режима поочередного обмена конвертами по каналу MFTP:
  - `yes` (по умолчанию) — сторона, передавшая конверт, позволяет передать конверт другой стороне, то есть узлы обмениваются конвертами поочередно;
  - `no` — сторона, начавшая передавать конверты, будет их передавать, пока они не закончатся, и только после этого позволит передавать конверты другой стороне.
- `port` — порт, на котором служба `mftpd` ожидает соединения по каналу MFTP от удаленных сетевых узлов (от `1` до `65535`, по умолчанию — `5000`).
- `recv_buff_size` — размер буфера приема в байтах. Параметр имеет нередактируемое значение `65500`.
- `send_buff_size` — размер буфера передачи в байтах. Параметр имеет нередактируемое значение `65500`.

Примечание. Обычно значение `65500` параметров `send_buff_size` и `recv_buff_size` оптимально для обеспечения максимальной скорости приема и передачи конвертов транспортным сервером.

- `save_sent` — включение или выключение хранения имен отправленных прикладных конвертов:
  - `no` (по умолчанию) — имена отправленных конвертов не сохраняются;
  - `yes` — при успешной отправке конверта в подкаталоге `sent` каталога, указанного в параметре `out_path` секции `[transport]`, создается файл нулевой длины с именем отправленного конверта.
- `ttl_ctl` — время жизни конвертов, содержащих управляющие запросы, в исходящей очереди. Указывается в днях, возможные значения от `10` до `90`, значение по умолчанию — `10`. Если по истечении времени, указанного в параметре `ttl_ctl`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `ttl_out` — время хранения конвертов в исходящей очереди в днях, возможные значения от `10` до `90`, значение по умолчанию — `30`. Если по истечении времени, указанного в параметре `ttl_out`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `ttl_trash` — время хранения конвертов в корзине в днях, возможные значения от `10` до `90`, значение по умолчанию — `90`. Если время хранения конверта в корзине превышает указанное в параметре `ttl_trash`, то он удаляется.
- `wait_timeout` — время ожидания активности в установленном MFTP-соединении. Указывается в секундах, возможные значения от `3` до `300`, значение по умолчанию — `30`. Если в течение этого времени узлы, установившие соединение, не обменялись никакой информацией, то данное соединение закрывается. Если в процессе обмена исходящие конверты для удаленного узла были переданы не полностью, то повторные попытки соединения будут происходить по истечении времени, указанного в параметре `outenv_timeout`.

- `task_envelope_limit` — минимальный размер свободного места на диске для приема прикладных конвертов (деловая почта, файловый обмен). Значение параметра указывается в процентах от общего размера диска (от `0` до `20`), значение по умолчанию — `20`. Если процент свободного места на диске станет ниже заданного значения, конверты от сетевых узлов приниматься не будут.
- `control_envelope_limit` — минимальный размер свободного места на диске для приема управляющих конвертов (квитанции, обновление ПО, криптографическая информация, политики). Значение параметра указывается в процентах от общего размера диска (от `0` до `10`), значение по умолчанию — `10`. Если процент свободного места на диске станет ниже заданного значения, конверты от сетевых узлов приниматься не будут.
- `remote_net_route` — включение или выключение использования прямой маршрутизации между сетями ViPNet:
  - `yes` (по умолчанию) — при настройке перенаправления конвертов с помощью параметра `transit` в секции `[channel]` шлюзовые координаторы не будут обрабатывать конверты, передаваемые между сетями ViPNet;
  - `no` — все настройки прямой маршрутизации будут сброшены, и обрабатывать конверты будут шлюзовые координаторы. При последующем включении использования прямой маршрутизации потребуется повторная настройка обхода шлюзовых координаторов.

Секция [reserv]

Секция `[reserv]` содержит параметры настройки транспортного сервера MFTP на координаторе, работающем в составе кластера:

- `cmd_port` — порт, на котором служба `mftpd` пассивного узла ожидает соединений с активным узлом через интерфейс синхронизации для приема управляющих команд (по умолчанию — `6084`). Данный параметр должен иметь одинаковое значение в файлах конфигурации транспортного сервера на «активном» и «пассивном» координаторах.
- `unpack_timeout` — период времени в секундах, в течение которого активный узел будет ожидать ответы на команды от пассивного узла, и в случае отсутствия ответов повторять команды (по умолчанию — `60`). Этот параметр используется системой удаленного обновления ПО. Он также определяет период сканирования каталога, заданного параметром `upgrade_path` секции `[upgrade]`, для анализа состояния процесса обновления ПО.
- `transfer_timeout` — период времени в секундах, в течение которого активный узел будет пытаться передавать копии MFTP-конверта пассивному узлу в случае неполного дублирования данного конверта (по умолчанию — `60`). В течение этого времени обработка конверта на активном узле блокируется. Если по истечении этого времени конверт не будет передан на пассивный узел, то его обработка продолжится.
- `use_reserv` — включение или выключение режима резервирования конвертов в кластере:
  - `yes` (по умолчанию) — конверты резервируются;

- `no` — резервирование конвертов не производится. В этом случае синхронизировать данные и обновление ПО на узлах кластера необходимо вручную. Кроме того, для корректной работы кластера настройки узлов кластера должны быть одинаковы.

При частом переключении режимов на пассивном узле могут сохранятся файлы устаревших обновлений. Файлы будут удалены при переключении узла кластера в активный режим или через промежуток времени, указанный в параметре `ttl_ctl` секции `[misc]`.

Секция [transport]

Секция `[transport]` содержит ряд параметров, определяющих пути к транспортным каталогам, то есть к каталогам, участвующим в обмене конвертами и их обработке. Эти параметры задают лишь основные каталоги. Вспомогательные каталоги создаются транспортным сервером MFTP в процессе работы как подкаталоги основных. При создании конфигурационного файла значения параметров этой секции определены по умолчанию относительно каталога, содержащего справочники и ключи.

Примечание. Транспортный сервер MFTP при каждом запуске проверяет наличие каталогов, заданных параметрами секции `[transport]`, и при необходимости создает их.

Секция `[transport]` содержит следующие параметры:

- `in_path` — абсолютный путь к каталогу, в который помещаются полностью принятые конверты (по умолчанию — `/opt/vipnet/in`).
- `out_path` — абсолютный путь к каталогу, в который внешние приложения помещают сформированные конверты для отправки (по умолчанию — `/opt/vipnet/out`).
- `trash_path` — абсолютный путь к каталогу, в который помещаются устаревшие конверты из очереди исходящих конвертов — так называемая «корзина» (по умолчанию — `/opt/vipnet/trash`).
- `local_path` — абсолютный путь к каталогу, в который помещаются прикладные конверты, предназначенные для передачи по локальному каналу другим узлам сети ViPNet (по умолчанию — `/opt/vipnet/local`). Данный параметр не используется в ViPNet Coordinator HW.
- `app_in_path` — абсолютный путь к каталогу, в который помещаются файлы, полученные от других узлов сети ViPNet (по умолчанию — `/opt/vipnet/in/app`). Данный параметр не используется в ViPNet Coordinator HW.

Секция [upgrade]

Данная секция содержит параметры, которые определяют поведение транспортного сервера MFTP при приеме обновлений ПО ViPNet из ViPNet Prime:

- `confsave` — тип конфигурации, автоматически создаваемой перед обновлением:

  - `partial` (по умолчанию) — частичная конфигурация, включающая только конфигурационные файлы (без справочников и ключей).
  - `full` — полная конфигурация, включающая конфигурационные файлы, справочники и ключи.
  - `off` — конфигурация не создается автоматически.
- `maxautosaves` — максимальное число автоматически сохраненных конфигураций. Возможные значения: от 1 до 10. Значение по умолчанию — `10`. Перед автоматическим созданием очередной конфигурации проверяется число ранее сохраненных конфигураций. Если это число равно значению `maxautosaves`, то конфигурация, созданная раньше остальных, удаляется, после чего сохраняется текущая конфигурация.
- `upgrade_checktimeout` — период проверки транспортного каталога, заданного параметром `upgrade_path`, на наличие файлов обновления программного обеспечения. Указывается в секундах, значение по умолчанию — `300`. В случае соответствия обнаруженных файлов обновления (время обновления и так далее) вызывается модуль обновления.
- `upgrade_for_kc_path` — абсолютный путь к каталогу, в который внешние приложения помещают файлы `*.sok` с запросами на сертификаты (по умолчанию — `/opt/vipnet/ccc/for_kc`).
- `upgrade_ini` — имя конфигурационного файла для процесса обновления (по умолчанию — `/opt/vipnet/user/upgrade.conf`).
- `upgrade_path` — абсолютный путь к каталогу, в который помещаются файлы обновления программного обеспечения после распаковки соответствующих конвертов (по умолчанию — `/opt/vipnet/ccc`).

A

Список служб ПО ViPNet Coordinator HW

Службы ViPNet:

- aad — служба аутентификации и авторизации;
- bonding_helper — скрипт управления модулем агрегирования каналов;
- controld — служба обработки запросов;
- dgdd — служба проверки состояния удаленных шлюзов (DGD);
- drviplir — драйвер перехвата сетевого трафика;
- external-controld — служба взаимодействия с ViPNet Prime;
- failover, failoverd — служба системы защиты от сбоев;
- http_proxy — скрипты управления прокси-сервером squid;
- l2overip — драйвер прозрачного соединения сегментов сети на уровне L2;
- iplircfg — служба настройки драйвера перехвата сетевого трафика, ведения журнала IP-пакетов, обновления справочно-ключевой информации;
- iplirpasswd — утилита проверки паролей аудитора и администратора;
- itcscrpt — драйвер шифрования IP-пакетов;
- itcskrniface — драйвер перехвата сетевого трафика;
- itcswd — драйвер службы мониторинга системы;
- mftp, mftpd — службы транспортного сервера MFTP;
- ntp_service — скрипт управления службы NTP;
- rvpn_shell — командный интерпретатор ViPNet;

- session_watcher — служба, отслеживающая сессии пользователей ViPNet;
- uc — служба идентификации пользователей сети;
- vipnetsnmp — служба SNMP;
- unmerge — утилита распаковки дистрибутива справочников и ключей;
- vupgrade — утилита обновления ПО ViPNet Coordinator HW;
- webgui (webgui_captive_portal, webgui-fcgi-server, webgui_php, webgui_frontend) — служба веб-интерфейса.

Службы Linux:

- acpid — служба обработки ACPI-событий;
- bonding — модуль агрегирования каналов;
- crond — служба запуска задач по расписанию;
- dhcpd — служба DHCP-сервера;
- dhcrelay — служба агента-ретранслятора DHCP-запросов;
- icap — служба icap-сервера, используемая для антивирусной проверки совместно с прокси-сервером;
- licd — служба лицензирования;
- login — служба аутентификации и открытия сессий;
- named — служба DNS;
- ntpd — служба NTP;
- pcscd — служба работы с токенами;
- snmpd — служба SNMP;
- sshd — служба SSH;
- squid — служба прокси-сервера squid;
- syslogd — служба системного журнала;
- ospfd — служба протокола OSPF динамической маршрутизации;
- udhcpc — служба DHCP-клиента;
- upsd, upsmon — службы ИБП;
- vmunix — ядро Linux;
- watchquagga — служба слежения за службой динамической маршрутизации;
- xinetd — служба запуска сетевых серверных процессов;
- zebra — служба динамической маршрутизации;
- zdhcpd — служба протокола DHCP динамической маршрутизации.

B

События системного журнала и журнала аудита

События Linux

Событие	Запись в системном журнале
Запуск Linux	`vmunix: [0.000000] Linux version 4.4.267 (vipnet@build-linux) (gcc version 6.3.0 20170516 (Debian 6.3.0-18+deb9u1)) #1 SMP Sun Jan 29 21:29:00 UTC 2023`

Завершение работы Linux	`rvpn_shell[9071]: [02-06 11:21:48.944568]< 9071>(00007fb2c6dcbc40)[L3] | Command:'machine halt'`
	`...`
	`failoverd[6656]: [02-06 11:21:49.074969]< 6656>(00007ff5b1929c40)[L2] StopServices | stop all services`
	`failoverd[6656]: [02-06 11:21:49.074975]< 6656>(00007ff5b1929c40)[L2] StopServices | kill threads`
	`...`

Сброс устройства к заводским настройкам	`factory_reset.sh[722]: Deletion of keys and host links has been started`
	`factory_reset.sh[722]: Keys and host links will be deleted in 29 seconds. To cancel, press Ctrl+C`
	`remove_keys.sh[1018]: key system deinitialization was done successfully`
	`...`
	`factory_reset.sh[722]: Delete host links and keys [success] [System] Details: GRUB reset [Local].`
	`factory_reset.sh[722]: Device has been reset to factory defaults. Press Enter to reboot`

События, инициированные пользователями

Событие	Запись в системном журнале	Запись в журнале аудита
Вход в системную командную оболочку	`rvpn_shell[21805]: <management> [va2000-3e130499] [local] [Single Mode] Exit to system shell [success] [admin] Details: Command:'admin escape '`	–
Выход из системной командной оболочки	`rvpn_shell[21805]: [02-01 12:39:48.077911]< 21805>(00007facbdf72c40 )[L3] | Command:'admin escape ' finished with rc=0 AAA__62ede3_dfdb39_5340f2_339e02 rc=0 done`	`Exit to system shell SUCCESS`
Завершение работы устройства	`rvpn_shell[16519]: [02-01 09:31:26.570476]< 16519>(00007fc450e17c40 )[L3] | Command:'machine halt'`	`Shutdown SUCCESS`
Перезагрузка устройства	`rvpn_shell[8548]: [02-01 09:46:09.213821]< 8548>(00007f68d2725c40 )[L3] | Command:'machine reboot'`	`Restart device SUCCESS`
Успешный запуск командного интерпретатора с помощью консоли	`login[23583]: pam_aauth(login:auth): granted access to user admin by LOGIN(uid=0)` `login[23583]: pam_aauth(login:session): session opened for user admin by LOGIN(uid=0)`	`User logon SUCCESS`

Выход из командного интерпретатора, работающего в режиме просмотра	`rvpn_shell[19591]: <EXIT> Command 'exit'`
	`...`
	`rvpn_shell[19591]: <EXIT> logout success`
	`...`
	`login[19247]: pam_aauth(login:session): session closed for user user`
		`Logoff SUCCESS`

Принудительное завершение сессии командного интерпретатора	`itcs-aad[10792]: [02-06 16:24:03.281567]< 10792>(00007f4574847700 )[L0] | AUDIT IsAllowed: user:"" action System:AA:Logout ticket AAA__20b6f5_fb0453_d931c8_d1a1b3 terminated (not allowed)` `rvpn_shell[14381]: Session is forcefully terminated`	–

Событие	Запись в системном журнале	Запись в журнале аудита
Успешный удаленный запуск командного интерпретатора по протоколу SSH	sshd[14734]: pam_aauth(sshd:auth): granted access to user user by (uid=0) sshd[14731]: Accepted keyboard-interactive/pam for user from 192.168.16.39 port 58168 ssh2 sshd[14731]: pam_aauth(sshd:session): session opened for user user by (uid=0) ... rvpn_shell[14742]: <LOGIN> Command: login - User logged in	User logon SUCCESS
Не удалось запустить командный интерпретатор при удаленном подключении по протоколу SSH	aauth-tool[20299]: error: failed to login user user through AA: 8448 sshd[20297]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.16.39 user=user	User logon FAILED
Завершение удаленного подключения по протоколу SSH	rvpn_shell[20685]: <EXIT> Command 'exit' ... rvpn_shell[20685]: <EXIT> logout success ... sshd[20626]: Received disconnect from 192.168.16.39 port 60808:11: disconnected by user sshd[20626]: Disconnected from 192.168.16.39 port 60808	Logoff SUCCESS
Включение вывода сообщений о событиях	rvpn_shell[23693]: [02-01 16:52:13.269594]< 23693>(00007f07bbdaec40)[L3] | Command:'debug on'	Turn debug notification on/off SUCCESS
Выключение вывода сообщений о событиях	rvpn_shell[23693]: [02-01 16:54:29.797997]< 23693>(00007f07bbdaec40)[L3] | Command:'debug off'	Turn debug notification on/off SUCCESS
Включение сетевого интерфейса	rvpn_shell[14053]: [02-01 14:22:24.093250]< 14053>(00007ff757d34c40)[L3] | Command:'inet ifconfig eth1 up' ... vmunix: [13614.681497] vmxnet3 0000:0b:00.0 eth1: NIC Link is Up 10000 Mbps	Set network interface state SUCCESS
Выключение сетевого интерфейса	rvpn_shell[14053]: [02-01 14:24:18.566469]< 14053>(00007ff757d34c40)[L3] | Command:'inet ifconfig eth1 down' ... rvpn_shell[14053]: <management> [va2000-3e130499] [local] [Single Mode] Set network interface state [success] [admin]	Set network interface state SUCCESS

Событие	Запись в системном журнале	Запись в журнале аудита
	Details: Command:'inet ifconfig eth1 down '	
Задание IP-адреса сетевого интерфейса	rvpn_shell[14053]: [02-01 14:17:19.204305]< 14053>(00007ff757d34c40)[L3] | Command:'inet ifconfig eth1 address 172.16.100.200 netmask 255.255.255.0' ... rvpn_shell[14053]: <management> [va2000-3e130499] [local] [Single Mode] Set network interface address [success] [admin] Details: Command:'inet ifconfig eth1 address 172.16.100.200 netmask 255.255.255.0 '	Set network interface address SUCCESS
Установка параметров скорости сетевого интерфейса	rvpn_shell[24896]: [02-01 14:46:34.109814]< 24896>(00007fbf6f4457c0)[L3] | Command:'inet ifconfig eth0 speed 10 duplex full autoneg off' eth_speed_duplex.sh[25376]: The given values of speed and duplex are valid for eth0.	Set network interface speed SUCCESS
Сброс настроек сетевого интерфейса	rvpn_shell[14053]: [02-01 14:19:24.060641]< 14053>(00007ff757d34c40)[L3] | Command:'inet ifconfig eth1 reset' ... rvpn_shell[14053]: <management> [va2000-3e130499] [local] [Single Mode] Reset network interface [success] [admin] Details: Command:'inet ifconfig eth1 reset ' rvpn_shell[14053]: [02-01 14:19:26.401259]< 14053>(00007ff757d34c40)[L3] | Command:'inet ifconfig eth1 reset ' finished with rc=0 AAA__fe5ce7_c48cd8_b47d02_77fe14 rc=0 done	Reset network interface SUCCESS
Создание виртуального интерфейса VLAN	rvpn_shell[5154]: [02-01 14:59:39.831224]< 5154>(00007ff178884c40)[L3] | Command:'inet ifconfig eth1 VLAN add 5' ... rvpn_shell[5154]: New VLAN interface eth1.5 was created. ... rvpn_shell[5154]: <management> [va2000-3e130499] [local] [Single Mode] Add VLAN interface [success] [admin] Details: Command:'inet ifconfig eth1 VLAN add 5 '	Add VLAN interface SUCCESS
Удаление виртуального интерфейса VLAN	rvpn_shell[5154]: [02-01 15:01:55.530482]< 5154>(00007ff178884c40)[L3] | Command:'inet ifconfig eth1 vlan delete 5' <management> [va2000-3e130499] [local] [Single Mode] Delete VLAN interface [success] [admin] Details: Command:'inet ifconfig eth1 vlan delete 5 '	Delete VLAN interface SUCCESS

Событие	Запись в системном журнале	Запись в журнале аудита
Добавление статического маршрута	rvpn_shell[5154]: [02-01 14:51:13.179302]< 5154>(00007ff178884c40)[L3] | Command:'inet route add' itcs-controld[5303]: [02-01 14:51:13.350052]< 5303>(00007f192ee01700)[L3] | System::Routing172.16.100.0 255.255.255 .0 172.16.100.1 5 5 rvpn_shell[5154]: <management> [va2000-3e130499] [local] [Single Mode] Add static route [success] [admin] Details: Command:'inet route add distance=5,gateway=172.16.100.1,host=172.16 .100.0,netmask=255.255.255.0,table_name=,ta ble_number=254,weight=5' .. itcs-controld[5303]: [02-01 14:51:13.350100]< 5303>(00007f192ee01700)[L3] | System::Routing<SR_ADD_ROUTE> Run command 'Command: inet route add' successful rvpn_shell[5154]: [02-01 14:51:13.354015]< 5154>(00007ff178884c40)[L3] | Command:'inet route add distance=5,gateway=172.16.100.1,host=172.16 .100.0,netmask=255.255.255.0,table_name=,ta ble_number=254,weight=5' finished with rc=0 AAA__839737_b01001_4c11d5_b8e4a9 rc=0 done	Add static route SUCCESS
Удаление статического маршрута	rvpn_shell[5154]: [02-01 14:56:52.403755]< 5154>(00007ff178884c40)[L3] | Command:'inet route delete' itcs-controld[5303]: [02-01 14:56:52.463365]< 5303>(00007f192f602700)[L3] | System::Routing172.16.100.0 255.255.255 .0 172.16.100.1 5 5 itcs-controld[5303]: [02-01 14:56:52.463374]< 5303>(00007f192f602700)[L3] | System::Routing<RT_DEL> Command: inet route delete 172.16.100.0. The following route was deleted: Table 254 (MAIN), Destination Netmask Next hop Distance Weight, ---------- ------- -------- -------- ------, 172.16.100.0 255.255.255.0 172.16.10 0.1 5 5 , itcs-controld[5303]: [02-01 14:56:52.463416]< 5303>(00007f192f602700)[L3] | System::Routing<SR_DELETE_ROUTE_COMMON> 'C ommand: inet route delete' successful	Delete route SUCCESS
Изменение сетевых фильтров и	vpncmd: [02-01 16:46:40.780465]< 24801>(00007f50d34c87c0)[L3] syslog | A rule was deleted: vpncmd: [02-01	Add firewall filter SUCCESS

Событие	Запись в системном журнале	Запись в журнале аудита
правил трансляции адресов	16:46:40.780527]< 24801>(00007f50d34c87c0)[L3] syslog | Type:User ID:4000001 local src @any dst @local service @HTTP pass Enabled iplircfg[19943]: [02-01 16:46:40.797926]< 19943>(00007fdfc67fc700)[L3] syslog | User rules dataname has been changed. ... iplircfg[19943]: [02-01 16:46:40.798004]< 19943>(00007fdfc67fc700)[L3] syslog | <Rule IsActive="true" xsi:type="vn:LocalRule"> iplircfg[19943]: [02-01 16:46:40.798009]< 19943>(00007fdfc67fc700)[L3] syslog | - <RuleId>4000001</RuleId> iplircfg[19943]: [02-01 16:46:40.798014]< 19943>(00007fdfc67fc700)[L3] syslog | - <OrderId>300035</OrderId> iplircfg[19943]: [02-01 16:46:40.798020]< 19943>(00007fdfc67fc700)[L3] syslog | - <Name/>	
Локальное обновление ПО	rvpn_shell[8141]: [02-06 11:02:50.483980]< 8141>(00007ff6e4c7cc40)[L3] | Command:'admin upgrade software' ... rvpn_shell[8141]: /sbin/driv_upgrade.sh: process 8528 has been created	Update software locally using a USB drive SUCCESS
Удаленное обновление ПО	rvpn_shell[8141]: [02-06 11:02:50.483980]< 8141>(00007ff6e4c7cc40)[L3] | Command:'admin upgrade software' ... rvpn_shell[8141]: /sbin/driv_upgrade.sh: process 8528 has been created	Update software locally using a USB drive SUCCESS
Успешное изменение файла iplir.conf	rvpn_shell: <I_CFG> Command: iplir config - iplir.conf has been edited successfully.	SetIplirConfig SUCCESS
Не удалось изменить содержимое файла iplir.conf	rvpn_shell[26362]: [02-01 13:30:18.341300]< 26362>(00007f6a6568bc40)[L3] | Command:'iplir config' ... rvpn_shell: <I_CFG> Command: iplir config: incorrect configuration rvpn_shell[26362]: error: Configuration checking failed rvpn_shell[26362]: Roll back the changes and restore the previous version of the file или rvpn_shell[26362]: [02-01	SetIplirConfig FAILED

Событие	Запись в системном журнале	Запись в журнале аудита
	13:27:07.237100]< 26362>(00007f6a6568bc40)[L3] | Command:'iplir config' ... rvpn_shell[26362]: error: Changing the settings is invalid when the process iplir is running. Please stop the process (iplir stop) rvpn_shell[26362]: <management> [va2000-3e130499] [local] [Single Mode] Open iplir.conf [failed] [admin] Details: Command:'iplir config	
Успешная смена пароля локального администратора	rvpn_shell[26362]: [02-01 13:33:28.397697]< 26362>(00007f6a6568bc40)[L3] | Command:'admin passwd' ... rvpn_shell[26362]: The new password has been successfully set.	Set local administrator password SUCCESS Set local user password SUCCESS
Не удалось сменить пароль локального администратора	rvpn_shell[29610]: [02-01 13:36:24.261962]< 29610>(00007f8604fa1c40)[L3] | Command:'admin passwd' ... rvpn_shell[29610]: error: Entered passwords do not match. rvpn_shell[29610]: <management> [va2000-3e130499] [local] [Single Mode] Set local administrator password [failed] [admin] Details: Command:'admin passwd '	Set local administrator password FAILED Set local user password FAILED
Применение обновления информации о ViPNet Prime	<management> [va2000-3e1306af] [local] [Single Mode] control action [success] [System] Action id: Applying Manager Information Updates Details: Starting ApplyPolicy	Applying Manager Information Updates SUCCESS/FAIL
Применение изменений фильтров из ViPNet Prime	itcs-external-controld[4378]: <management> [hw5000-3f670001] [local] [Single Mode] control action [success] [System] Action id: Apply firewall filters received from the management software Details: Starting ApplyPolicy	Apply firewall filters received from the management software SUCCESS/FAIL
Применение обновления лицензии из ViPNet Prime	itcs-external-controld[4742]: <management> [va2000-3e1306af] [local] [Single Mode] control action [success] [System] Action id: Applying a license upgrade from a control application Details: Starting ApplyPolicy ... itcs-external-controld[4742]: <management> [va2000-3e1306af] [local] [Single Mode] control action [success] [System] Action id: Applying a license upgrade from a control application Details: Finish	Applying a license upgrade from a control application SUCCESS/FAIL
Подключение к	Connection established, subcribed to	

Событие	Запись в системном журнале	Запись в журнале аудита
транспортному серверу UT5	`publisher endpoint`	
Отсутствие подключения к транспортному серверу UT5	`Connection error: <Connection timed out! Wait and repeat connection...>`	

Успешная установка дистрибутива ключей	`keysetup[2242]: appliance initialization file ds5 will be installed from USB`
	`vmunix: [11866.213796] usb 1-2.1: New USB device found, idVendor=8564, idProduct=1000`
	`keysetup[2242]: Partition /dev/sdc1 was successfully mounted on /tmp/usb`
	`keysetup[2242]: Suitable ds5-file /tmp/usb/sdc1/va_vipnet_base_x86_64_5.2.0-4977.ds5 found.`
	`...`
	`keysetup[2242]: User password was correct and ds5-file VEM_va_vipnet_base_x86_64_5.2.0-4977.ds5 installed successfully.`
		–

Удаление справочников и ключей	`rvpn_shell[31061]: [02-01 13:53:29.486327]< 31061>(00007fd698e8dc40 )[L3] | Command:'admin remove keys'`
	`...`
	`rvpn_shell[31061]: <management> [va2000-3e130499] [local] [Single Mode] Delete host links and keys [success] [admin] Details: Command:'admin remove keys '`
	`rvpn_shell[31061]: [02-01 13:54:06.144942]< 31061>(00007fd698e8dc40 )[L3] | Command:'admin remove keys ' finished with rc=0 AAA__b141b9_7ae3c6_7a9cf8_60fafd rc=0 done`
		`Delete host links and keys SUCCESS`

Сохранение копии конфигурации VPN	`rvpn_shell[5154]: [02-01 15:08:34.604639]< 5154>(00007ff178884c40 )[L3] | Command:'admin config save test_config'` `rvpn_shell[5154]: <management> [va2000-3e130499] [local] [Single Mode] Current ViPNet configuration backing up [success] [admin] Details: Command:'admin config save test_config '`	`Current ViPNet configuration backing up SUCCESS`

Загрузка копии конфигурации VPN	`rvpn_shell[5154]: [02-01 15:13:03.525172]< 5154>(00007ff178884c40 )[L3] | Command:'admin config load test_config '`
	`rvpn_shell[5154]: command: admin config load test_config`
	`rvpn_shell[5154]: <management> [va2000-3e130499] [local] [Single Mode] Load`
		`Load VPN configuration backup SUCCESS`

Событие	Запись в системном журнале	Запись в журнале аудита
	VPN configuration backup [success] [admin] Details: Command:'admin config load test_config '	
Экспорт журнала IP-пакетов на USB-носитель	rvpn_shell[13459]: [02-06 15:57:56.005795]< 13459>(00007fec1de51c40)[L3] | Command:'machine logs export network-traffic usb netlog' export_packetdb.sh[14737]: File successfully copied. Unmounting USB drive..	Export IP packet log to a USB drive SUCCESS
Экспорт индивидуальной конфигурации устройства	rvpn_shell[18277]: [02-01 15:51:57.712051]< 18277>(00007f6513325c40)[L3] | Command:'machine backup export' ... create_appliance_configuration_file.sh[1943 1]: create_appliance_configuration_file.sh executed successfully. export_appliance_configuration_file_to_usb. sh[20293]: File successfully copied. Unmounting USB drive.. rvpn_shell[18277]: <management> [va2000-3e130499] [local] [Single Mode] Schedule configuration backup [success] [admin] Details: Command:'machine backup export '	Export configuration backup SUCCESS
Экспорт файлов журналов на USB-носитель	rvpn_shell[15863]: [02-01 15:35:28.143657]< 15863>(00007fc0c0022c40)[L3] | Command:'machine logs export usb' export_log.sh[16540]: Copying logs_va_3e130499_va2000-3e130499_2023_02_01 _15_35_34.tar.gz to USB drive. Press ^+C to abort export_log.sh[16540]: File successfully copied. Unmounting USB drive...	Export event log SUCCESS

События запуска и остановки служб

Событие	Запись в системном журнале	Запись в журнале аудита
Загрузка драйверов и запуск служб	rvpn_shell[10750]: [02-02 09:04:22.170807]< 10750>(00007f0fd160d c40)[L3] | Command:'service vpn start' ... rvpn_shell[10750]: <management> [va2000-3e130499] [local] [Single Mode] Set VPN status [success] [admin] Details: Command:'service vpn start '	Set VPN status SUCCESS
Выгрузка драйверов и	rvpn_shell[27370]: [02-01 17:09:54.870397]< 27370>(00007f80c264f	Set VPN status SUCCESS

Событие	Запись в системном журнале	Запись в журнале аудита
завершение работы служб	c40)[L3] | Command:'vpn stop' ... hwvipnet[28088]: Stop vpn services... ... rvpn_shell[27370]: <management> [va2000-3e130499] [local] [Single Mode] Set VPN-related services status [success] [admin] Details: Command:'vpn stop '	
Запуск службы системы защиты от сбоев failoverd	rvpn_shell[10750]: [02-02 09:20:06.271505]< 10750>(00007f0fd160d c40)[L3] | Command:'failover start' rvpn_shell[10750]: <management> [va2000-3e130499] [local] [Single Mode] Start/Stop failover daemon [success] [admin] Details: Command:'failover start '	Start/Stop failover daemon SUCCESS
Завершение работы службы системы защиты от сбоев failoverd	rvpn_shell[10750]: [02-02 09:10:17.495945]< 10750>(00007f0fd160d c40)[L3] | Command:'failover stop' rvpn_shell[10750]: <management> [va2000-3e130499] [local] [Single Mode] Start/Stop failover daemon [success] [admin] Details: Command:'failover stop '	Start/Stop failover daemon SUCCESS
Запуск управляющей службы iplircfg	rvpn_shell[10750]: [02-02 09:23:52.367623]< 10750>(00007f0fd160d c40)[L3] | Command:'iplir start' hwvipmod[16584]: Loading ViPNet modules ... rvpn_shell[10750]: <management> [va2000-3e130499] [local] [Single Mode] Start/Stop iplir daemon [success] [admin] Details: Command:'iplir start '	Start/Stop iplir daemon SUCCESS
Завершение работы управляющей службы iplircfg	rvpn_shell[10750]: [02-02 09:21:56.031335]< 10750>(00007f0fd160d c40)[L3] | Command:'iplir stop' ... rvpn_shell[10750]: <management> [va2000-3e130499] [local] [Single Mode] Start/Stop iplir daemon [success] [admin] Details: Command:'iplir stop '	Start/Stop iplir daemon SUCCESS
Запуск транспортного сервера MFTP	rvpn_shell[10750]: [02-02 09:30:01.975053]< 10750>(00007f0fd160d c40)[L3] | Command:'mftp start' ... mftp[17817]: [02-02 09:30:02] Daemon started ... rvpn_shell[10750]: <management> [va2000-3e130499] [local] [Single Mode] Turn MFTP on/off [success] [admin] Details:	Turn MFTP on/off SUCCESS

Событие	Запись в системном журнале	Запись в журнале аудита
	Command:'mftp start '	
Завершение работы транспортного сервера MFTP	rvpn_shell[10750]: [02-02 09:28:16.951420]< 10750>(00007f0fd160dc40)[L3] | Command:'mftp stop' ... rvpn_shell[10750]: <management> [va2000-3e130499] [local] [Single Mode] Turn MFTP on/off [success] [admin] Details: Command:'mftp stop '	Turn MFTP on/off SUCCESS
Перезапуск службы веб-сервера	rvpn_shell[10750]: [02-02 09:33:03.879052]< 10750>(00007f0fd160dc40)[L3] | Command:'webui restart' ... rvpn_shell[10750]: <management> [va2000-3e130499] [local] [Single Mode] Restart web server [success] [admin] Details: Command:'webui restart '	Restart web server

События системы защиты от сбоев

Событие	Запись в системном журнале
Смена режима работы узла кластера из пассивного в активный	failoverd[6976]: [02-02 10:13:38.300387]< 6976>(00007f054f9847c0)[L2] Exit | active server not responding, switching to active mode failoverd[6976]: [02-02 10:13:38.300423]< 6976>(00007f054f9847c0)[L1] syslog | switching to active mode vmunix: [320.636326] [DUP] switch cluster mode: passive (1) => active (2)
Перезагрузка узла кластера из-за сбоя на сетевом интерфейсе	vmunix: [4927.663675] vmxnet3 0000:0b:00.0 eth1: NIC Link is Down failover-node[31518]: Configuring state of daemons for passive mode vmunix: [4940.296325] [DUP] switch cluster mode: active (2) => passive (1)
Перезагрузка узла кластера из-за конфликта режимов	failoverd[18143]: [02-02 13:04:44.026129]< 18143>(00007f4db882e7c0)[L1] syslog | Rebooted due conflict mode at Thu Feb 2 13:04:44 2023
Перезагрузка узла кластера из-за обнаружения службой failoverd ошибки другого контролируемого сервиса	failoverd[6973]: [02-02 12:19:35.032019]< 6973>(00007f9a752617c0)[L1] CheckApp | Reached maximum count of application restarts [iplircfg] pid 2008 failoverd[6973]: [02-02 12:19:35.032029]< 6973>(00007f9a752617c0)[L3] OnInvokeEventCmd | Rebooting the appliance in order to recover

Событие	Запись в системном журнале

	`failoverd[6973]: [02-02 12:19:35.470798]< 6973>(00007f9a752617c0)[L1] syslog | one or more subsystems failed, rebooting`
	`failoverd[6973]: [02-02 12:19:35.470823]< 6973>(00007f9a752617c0)[L1] syslog | Rebooted due to watcher detected error at Thu Feb 2 12:19:35 2023`
	`syslogd (GNU inetutils 1.9.4): restart`

События обмена служебной информацией между узлами ViPNet

Событие	Запись в системном журнале
Получение сообщения о доступности узла ViPNet (сообщения рассылаются при включении узла, а затем периодически)	`iplircfg[7226]: [02-02 15:11:38.237440]< 7226>(00007fcb66e40980)[L2] | got message: type 1 from ID 0x3E130001 (msg name 'YY0N29WO.KI5')`
Получение сообщения о доступности узла ViPNet (сообщения рассылаются при первом обращении к серверу IP-адресов сети ViPNet)	`iplircfg[5095]: [01-23 10:14:59.709058]< 5095>(00007ff998c2f980)[L2] | got message: type 3 from ID 0x3E130001 (msg name 'GJ5ZUZSZ.JJ0')`
Первое обращение к серверу соединений, если сервер не является также сервером IP-адресов сети ViPNet	`iplircfg[1684]: [02-07 21:28:10.979295]< 1684>(00007f5563f66980)[L2] | got message: type 23 from ID 0x3E1305DA (msg name 'AAZD}YP7.493')`
Отключение узла ViPNet от сервера IP-адресов сети ViPNet	`iplircfg[29142]: [02-02 13:36:53.678221]< 29142>(00007f40cc3a3980)[L2] | got message: type 2 from ID 0x3E130001 (msg name 'DKNYU56I.BV1')`
Проверка соединения с узлом ViPNet (запрос)	`iplircfg[29142]: [02-02 13:33:36.169191]< 29142>(00007f40cc3a3980)[L2] | got message: type 5 from ID 0x3E1304A5 (msg name '6RB8POLJ.DGC')`
Подтверждение получения сообщения (кроме уведомлений об изменении адреса доступа удаленного узла ViPNet)	`iplircfg[29142]: [02-02 13:33:36.320283]< 29142>(00007f40cc3a3980)[L2] | got message: type 7 from ID 0x3E1304A5 (msg name 'UOPO9T1T.DRR')`
Уведомление об изменении адреса доступа удаленного узла ViPNet	`iplircfg[29142]: [02-02 13:46:06.699250]< 29142>(00007f40cc3a3980)[L2] | got message: type 50 from ID 0x3E130002 (msg name 'NTP964KK.0FJ')`
Подтверждение получения уведомления об изменении	`iplircfg[7226]: [02-02 15:03:56.491499]< 7226>(00007fcb66e40980)[L2] | got`

Событие	Запись в системном журнале
адреса доступа удаленного узла ViPNet	`message: type 70 from ID 0x3E130001 (msg name '31J92W9V.6YN')`
Изменение параметров адреса доступа удаленного узла ViPNet	`iplircfg[25757]: [02-02 15:23:54.171023]< 25757>(00007fbcf1f9f980)[L2] | load natsettings for 0x3E130193: firewallip=192.168.166.105 port=55888 timeout=25 virtualip=0.0.0.1 proxyid=0x3E130001 DRV_ALWAYS_USE_SERVER=no DRV_GREEN_NODE=yes DRV_STOP_FIREWALL_IP=no DRV_ELAPSE=no DRV_BROADCAST_HOST=no DRV_INCAPS_FORCE_REAL_ADDR=yes`

События об ошибках ДСЧ и шифратора

Событие	Запись в системном журнале

Проверка при запуске и регламентная проверка ДСЧ в криптодрайвере	`uprngd: uprngd  0x7f2963fff700 lcuprng.c  :434 core_normative_control Normative control was successfully completed.`
	
	`itcshubd[17962]: <crypto> [va2000-3e130628] [local] [Single Mode] CryptoEvent0 [failed] [] Details: SoftToken 0x7f55da5ad700 Reglament inspection passed`
	`itcshubd[17962]: SoftToken 0x7f55da5ad700 Reglament inspection passed`

Проверка при запуске и регламентная проверка шифраторов в криптодрайвере	`itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146  | AUDIT INFO: CryptSystem GOST status=0 (0x854CAC47)`
	`itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146  | AUDIT INFO: CryptSystem GOST status=0 (0x854CAC47)`
	`itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146  | AUDIT INFO: CryptSystem FIPS status=8000000 (0x854CAC47)`
	`itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146  | AUDIT INFO: CryptSystem FIPS status=8000000 (0x854CAC47)`
	`itcshubd[2652]: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146  | AUDIT INFO: CryptSystem CUSTOM status=8000000 (0x854CAC47)`
	`itcshubd[2652]: <crypto> [hw100] [local] [Single Mode] Cryptodriver status check completed successfully [success] [9b12a8a2-d776-43a4-b10b-d99949555cdb] Details: KeySystemInproc 0x7fc88517f700 key_loader_impl.cpp:146  | AUDIT INFO: CryptSystem CUSTOM status=8000000 (0x854CAC47)`

События антивирусной проверки и контент-фильтрации

Событие	Запись в системном журнале
Сработало запрещающее правило контроля содержимого трафика по HTTP-методу	`(squid): 1 172.16.50.5 TCP_DENIED/403 19183 GET http://kremlin.ru/ - NONE/- text/html`
Сработало запрещающее правило контроля содержимого трафика по MIME-типу	`(squid): 58 172.16.100.5 TCP_DENIED_REPLY/403 19248 GET http://static.kremlin.ru/media/events/files/ru/QdJ0ybmN7Kocwc8eyTGosdyuylM6qXpj.pdf - DIRECT/95.173.136.78 text/html`
Антивирус заблокировал скачивание зараженного файла	`(squid): ICAP: 13 172.16.100.5 icap://192.168.32.11:1344/virus_scan RESPMOD http://www.virusanalyst.com/eicar.zip`

Термины и сокращения

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задает связи между ними.
- ViPNet Rollout Center — модуль быстрого развертывания защищенных устройств ViPNet в больших распределенных сетях.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в нее устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

ViPNet TIAS

Система ViPNet TIAS (Threat Intelligence Analytics System) анализирует события информационной безопасности, поступающие от различных источников: ViPNet IDS NS, ViPNet IDS HS, ViPNet xFirewall, ViPNet EPP; автоматически выявляет инциденты информационной безопасности на основании потока этих событий и оперативно информирует заинтересованных лиц о произошедших инцидентах.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями.

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet и по которым приложения отправляют свой трафик.

Адреса доступа

IP-адреса, по которым узел доступен в сети (например, адреса межсетевого экрана, за которым он находится).

Базовый виртуальный адрес

Является точкой отсчета при назначении виртуальных адресов для каждого из реальных адресов узла. Если в данный момент узел виден по виртуальному адресу, его адресом доступа считается либо базовый виртуальный адрес, либо вторичный виртуальный адрес, соответствующий первому в списке реальному адресу.

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

Дистрибутив ключей

Набор симметричных ключей обмена с защищенными узлами сети ViPNet. Формируется в ViPNet Prime на основе заданных связей между узлами.

В ViPNet Coordinator HW версии 5.0 и выше используется дистрибутив ключей `ds5`. Содержит справочники, ключи и лицензии, необходимые для инициализации и работы ViPNet Coordinator HW.

В ViPNet Coordinator HW версий 4.4.x, ViPNet xFirewall и ViPNet Client используется дистрибутив ключей `dst`.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключи защиты

Ключи защиты обеспечивают безопасное удаленное обновление ключей обмена из ключевого центра ViPNet Prime и их хранение ViPNet Coordinator HW.

Ключи обмена

На ключах обмена защищается канал передачи данных между двумя связанными узлами сети ViPNet.

Командный интерпретатор

Командная оболочка, предназначенная для администрирования программного обеспечения ViPNet Coordinator HW с помощью ряда специальных команд.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Межсетевое взаимодействие

Информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

Метрика адреса доступа

Определяет задержку (в миллисекундах) отправки тестовых пакетов при выполнении опроса узла для определения доступности адреса. Предназначена для задания приоритета использования каналов связи.

Прикладная квитанция

Файл, оповещающий отправителя о доставке и (или) прочтении прикладного конверта.

Прикладной конверт

Файл, формируемый приложениями ViPNet (например, «Деловая почта», «Файловый обмен») для передачи другим сетевым узлам.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

Сетевой узел ViPNet

Сетевой узел с ПО ViPNet, зарегистрированный в ViPNet Prime VPN.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Справочники и ключи

Настройки узла ViPNet, ключи защиты, ключи обмена и ключи пользователя.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки транспортного конверта MFTP.

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на защищенные узлы ViPNet транспортным сервером MFTP.

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами сети ViPNet.

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

Туннелирующий координатор

Координатор, который осуществляет туннелирование.

Шлюзовой координатор

Координатор, через который осуществляется обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие. Шлюзовые координаторы назначаются в ViPNet Prime каждой сети при организации взаимодействия между двумя различными сетями ViPNet.

Электронная подпись (ЭП)

Откреплённая CMS-подпись, сформированная по Р 1323565.1.025–2019 и ГОСТ 34.10-2012 (512 бит).