

ViPNet Coordinator IG 5

Справочник команд и конфигурационных файлов

Версия продукта: 5.2.0

ViPNet Coordinator IG10
ViPNet Coordinator IG100
ViPNet Coordinator IG1000

infotecs

© АО «ИнфоТеКС», 2025

ФРКЕ.467759.003ИС6

Версия продукта 5.2.0

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

Все условия эксплуатации и ограничения на использование ViPNet Coordinator IG приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Coordinator IG.

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 ... **20**
О документе ... 21
Соглашения документа ... 22
Обратная связь ... 24

Глава 1. Справочник команд ... **25**
Команды группы admin ... 26
admin certificate create ... 26
admin certificate delete ... 26
admin clear-auth-warning ... 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 system erase ... 33
admin upgrade software ... 34
Команды группы alg ... 36
alg module direct-media ... 36
alg module h323 direct-h245 ... 37
alg module process off ... 37
alg module process on ... 38
alg show ... 39
Команды группы failover ... 41
failover config edit ... 41
failover config mode ... 41
failover show active-mac-address ... 42
failover show config ... 43
failover show info ... 44
failover show sync-connections ... 45
failover start ... 46
failover stop ... 47
failover view ... 47
Команды группы firewall ... 49

firewall add 49
firewall add name 53
firewall change append 54
firewall conntrack flush 56
firewall delete 56
firewall move rule 57
firewall object delete 58
firewall object show 59
firewall rules log-blocked 61
firewall settings 61
firewall settings show 63
firewall show 64
Команды группы inet 68
inet bgp 68
inet bgp as-path-filter add 68
inet bgp as-path-filter clear seq 69
inet bgp as-path-filter delete 69
inet bgp as-path-filter seq 70
inet bgp clear 72
inet bgp community-list add 72
inet bgp community-list clear seq 73
inet bgp community-list delete 73
inet bgp community-list seq 74
inet bgp neighbor add 75
inet bgp neighbor delete 76
inet bgp neighbor remove advertise-map 76
inet bgp neighbor remove as-path-filter 77
inet bgp neighbor remove password 77
inet bgp neighbor remove prefix-list 78
inet bgp neighbor remove route-map 78
inet bgp neighbor set advertise-map 79
inet bgp neighbor set as-path-filter 79
inet bgp neighbor set default-originate 80
inet bgp neighbor set ebgp-multihop 81
inet bgp neighbor set next-hop-self 81
inet bgp neighbor set password 82
inet bgp neighbor set port 82
inet bgp neighbor set prefix-list 83
inet bgp neighbor set remote-as 84

inet bgp neighbor set route-map 84
inet bgp neighbor set ttl-security 85
inet bgp network add 85
inet bgp network delete 86
inet bgp network redistribute 87
inet bgp network redistribute route-map 87
inet bgp router as 88
inet bgp router bestpath AS-path-relax 88
inet bgp router bestpath bandwith 89
inet bgp router conditional-advertisement-timer 90
inet bgp router id 90
inet bgp router reset 91
inet bgp route-reflector client add 91
inet bgp route-reflector client delete 92
inet bgp route-reflector cluster-id 92
inet bgp route-reflector outbound-policy 93
inet bgp show 93
inet bgp show AS-path-filter 96
inet bgp show bestpath 96
inet bgp show community-list 97
inet bgp show neighbors 98
inet bgp show neighbors filters 103
inet bgp show neighbors list 105
inet bgp show network 105
inet bgp show route-reflector 107
inet bgp show summary 107
inet bonding add 108
inet bonding delete 110
inet clear mac-address-table 111
inet dgd configuration default 111
inet dgd configuration interval-time 112
inet dgd configuration response-time 113
inet dgd configuration retries-count 114
inet dgd configuration syslog-level 115
inet dgd next-hop add 115
inet dgd next-hop delete 117
inet dgd mode 117
inet dgd rule add action-priority 118
inet dgd rule add match-next-hop 119

inet dgd rule clear 120
inet dgd rule delete action-priority 120
inet dgd rule delete match-next-hop 121
inet dhcp client route-default-metric 122
inet dhcp client route-distance 122
inet dhcp relay add backup-interface 123
inet dhcp relay add external-interface 124
inet dhcp relay add listen-interface 125
inet dhcp relay delete backup-interface 126
inet dhcp relay delete external-interface 127
inet dhcp relay delete listen-interface 127
inet dhcp relay mode 128
inet dhcp relay reset 129
inet dhcp relay start 130
inet dhcp relay stop 131
inet dhcp server add default-lease-time 131
inet dhcp server add dns 132
inet dhcp server add domain 133
inet dhcp server add host 134
inet dhcp server add interface 135
inet dhcp server add max-lease-time 136
inet dhcp server add ntp 137
inet dhcp server add option 138
inet dhcp server add range 139
inet dhcp server add relay-interface 140
inet dhcp server add router 141
inet dhcp server add subnet-mask 142
inet dhcp server add tftp 143
inet dhcp server add voip 144
inet dhcp server add wins 144
inet dhcp server delete default-lease-time 145
inet dhcp server delete dns 146
inet dhcp server delete domain 147
inet dhcp server delete host 148
inet dhcp server delete interface 149
inet dhcp server delete max-lease-time 150
inet dhcp server delete ntp 150
inet dhcp server delete option 151
inet dhcp server delete range 152

inet dhcp server delete relay-interface 153
inet dhcp server delete router 154
inet dhcp server delete subnet-mask 155
inet dhcp server delete tftp 155
inet dhcp server delete voip 156
inet dhcp server delete wins 157
inet dhcp server mode 158
inet dhcp server reset 159
inet dhcp server start 159
inet dhcp server stop 160
inet dns clients add 160
inet dns clients delete 161
inet dns clients list 161
inet dns forwarders add 162
inet dns forwarders delete 163
inet dns forwarders list 164
inet dns mode 164
inet dns querylog 165
inet dns querylog show 166
inet dns querylog size 167
inet dns start 167
inet dns stop 168
inet ifconfig address 168
inet ifconfig address add 169
inet ifconfig address delete 170
inet ifconfig bonding add 171
inet ifconfig bonding ad-select 172
inet ifconfig bonding delete 173
inet ifconfig bonding lacp-rate 173
inet ifconfig bonding miimon 174
inet ifconfig bonding primary 175
inet ifconfig bonding xmit-hash-policy 175
inet ifconfig class 176
inet ifconfig disable 177
inet ifconfig dhcp 178
inet ifconfig dhcp route-metric 179
inet ifconfig down 180
inet ifconfig enable 181
inet ifconfig mtu 181

inet ifconfig reset 182
inet ifconfig speed 184
inet ifconfig speed auto 185
inet ifconfig type 185
inet ifconfig up 186
inet ifconfig vlan add 187
inet ifconfig vlan delete 188
inet ntp add 188
inet ntp delete 189
inet ntp list 190
inet ntp mode 190
inet ntp orphan 191
inet ntp start 192
inet ntp stop 192
inet ntp use-default 193
inet ospf area auth 193
inet ospf interface keys add 194
inet ospf interface keys remove 195
inet ospf interface password 196
inet ospf mode 196
inet ospf network add 197
inet ospf network delete 198
inet ospf redistribute add 199
inet ospf redistribute delete 199
inet ospf priority 200
inet ospf router-id 201
inet ospf show configuration 202
inet ospf show database 203
inet ospf show neighbour 204
inet ping 205
inet policy active 206
inet policy rule add match 206
inet policy rule add 208
inet policy rule clear 209
inet policy rule delete match 210
inet policy rule delete 211
inet prefix-list add 212
inet prefix-list clear seq 213
inet prefix-list delete 213

inet prefix-list seq 214
inet prefix-list show 215
inet route add 216
inet route clear 217
inet route delete 218
inet route-map add 219
inet route-map clear 220
inet route-map delete 220
inet route-map match as-path 221
inet route-map match community 222
inet route-map match prefix-list 222
inet route-map on-match 223
inet route-map seq 224
inet route-map set as-path-prepend 224
inet route-map set community 225
inet route-map set local-preference 226
inet route-map set metric 227
inet route-map set next-hop 227
inet route-map set weight 228
inet route-map show 229
inet serial show 230
inet show dgd configuration 231
inet show dgd next-hop 231
inet show dgd rule 232
inet show dhcp client 233
inet show dhcp server 234
inet show dhcp server lease 235
inet show dhcp relay 236
inet show dns 237
inet show interface 237
inet show interface state 240
inet show mac-address-table 241
inet show ntp 243
inet show policy rule 244
inet show routing 245
inet show traffic 247
inet show usb-modem 248
inet show usb-modem ip-gw 250
inet show usb-modem provider 251

inet show vlan 252
inet show wifi 253
inet show wifi log signal 254
inet snmp autostart 254
inet snmp cluster node community 255
inet snmp cluster node context 256
inet snmp cluster show 256
inet snmp cluster v2 257
inet snmp community add 258
inet snmp community change 259
inet snmp community delete 259
inet snmp community list 260
inet snmp logging 261
inet snmp port 262
inet snmp reset-engineid 262
inet snmp show 263
inet snmp start 264
inet snmp stop 265
inet snmp system contact 265
inet snmp system location 266
inet snmp system name 267
inet snmp trapsink add 268
inet snmp trapsink delete 269
inet snmp trapsink list 269
inet snmp user add 270
inet snmp user delete 271
inet snmp user list 272
inet snmp user set key 273
inet snmp user set name 274
inet snmp user set passwd 275
inet snmp user set read 276
inet snmp user set trapsess 277
inet snmp user set trapsess add 278
inet snmp user set trapsess delete 279
inet snmp v2 279
inet snmp v3 280
inet ssh 281
inet usb-modem add provider 282
inet usb-modem clear provider-base 283

inet usb-modem delete provider ... 284
inet usb-modem dns ... 285
inet usb-modem ip-gw ... 285
inet usb-modem mode ... 286
inet usb-modem pin ... 287
inet usb-modem provider mc ... 288
inet usb-modem provider password ... 289
inet usb-modem provider phone ... 289
inet usb-modem provider type ... 290
inet usb-modem provider username ... 291
inet usb-modem route ... 292
inet usb-modem route-metric ... 293
inet usb-modem select provider ... 293
inet usb-modem sim ... 295
inet vlan comment add ... 295
inet vlan comment delete ... 296
inet wifi access-point channel ... 296
inet wifi access-point hwmode ... 297
inet wifi access-point show ... 298
inet wifi authentication ... 298
inet wifi log signal ... 299
inet wifi mode ... 300
inet wifi role ... 301
inet wifi scan ... 302
Команды группы ipf ... 303
ipf add rules ... 303
ipf change name rules ... 304
ipf delete rules ... 304
ipf iec104 rules iecformat set asdu ... 305
ipf iec104 rules iecformat set cot ... 306
ipf iec104 rules iecformat set default ... 307
ipf iec104 rules iecformat set ioaddress ... 308
ipf iec104 rules iecformat set max_length_apdu ... 309
ipf mode ... 309
ipf rules disable ... 310
ipf rules enable ... 311
ipf rules fw add ... 311
ipf rules fw append ... 313
ipf rules fw change ... 314

ipf rules fw delete ... 316
ipf rules rule add ... 316
ipf rules rule append ... 319
ipf rules rule change ... 320
ipf rules rule delete ... 321
ipf rules rule disable ... 321
ipf rules rule enable ... 322
ipf rules rule move ... 323
ipf set journal maxsize ... 324
ipf set journal registerall ... 324
ipf set syslog-level ... 325
ipf show ... 326
ipf show iec104 rules iecformat ... 328
ipf show rules ... 329
ipf show stat ... 330
Команды группы iplir ... 332
iplir adapter add ... 332
iplir adapter delete ... 333
iplir adapter traffic ... 333
iplir config ... 334
iplir info ... 335
iplir option be-default-gateway ... 337
iplir option interface-timeout ... 337
iplir option ip-forwarding ... 338
iplir option keepalive-timeout ... 338
iplir option maxtimediff ... 339
iplir option mode ... 340
iplir option mss-decrease ... 340
iplir option ping-timeout ... 341
iplir option server-ping-timeout ... 342
iplir option show ... 342
iplir option sync-time ... 344
iplir option syslog-level ... 345
iplir option udp-ports-count ... 346
iplir ping ... 347
iplir set l2overip interface ... 347
iplir set l2overip local-port ... 348
iplir set l2overip mac-ttl ... 349
iplir set l2overip mode ... 349

iplir set l2overip remote-port ... 350
iplir set l2overip remote-port delete ... 351
iplir set l2overip unsolicited-frames ... 351
iplir node access-point add ... 352
iplir node access-point delete ... 353
iplir node blockforward ... 353
iplir node add domain-name ... 354
iplir node delete domain-name ... 355
iplir node list ... 355
iplir node show ... 357
iplir node show domain-names ... 359
iplir node update domain-name cache ... 360
iplir show adapter ... 360
iplir show adapters ... 361
iplir show adapters groups ... 362
iplir show authentication-type ... 362
iplir show ciphertype ... 362
iplir show config ... 363
iplir show exchange-keys ... 364
iplir show firewall status ... 365
iplir show key-info ... 367
iplir show l2overip ... 368
iplir show tcptunnel-info ... 369
iplir start ... 370
iplir stop ... 371
iplir tcptunnel client mode ... 371
iplir tcptunnel client on/off ... 372
iplir tcptunnel client port ... 373
iplir tcptunnel role ... 373
iplir tcptunnel server on/off ... 374
iplir tcptunnel server port ... 375
iplir view ... 375
iplir warning-threshold ... 376
Команды группы machine ... 378
machine backup ... 378
machine backup export ... 379
machine backup schedule ... 380
machine config export usb ... 381
machine config import ... 382

machine halt 384
machine hosts add 385
machine hosts remove 386
machine hosts show 386
machine logs clear dns 387
machine logs export usb 387
machine logs export-and-clear usb 390
machine logs export ipf-traffic usb 391
machine logs export network-traffic usb 392
machine logs settings cef include 393
machine logs settings cef event-type 393
machine logs settings cef exclude 394
machine logs settings size 395
machine logs settings network-traffic maxsize 395
machine logs settings network-traffic omit-client-port 396
machine logs settings network-traffic register 397
machine logs settings network-traffic timediff 398
machine logs settings show 399
machine logs show crypto-audit 400
machine logs show ipf-traffic 402
machine logs show mftp 403
machine logs show network-traffic 404
machine logs show syslog 405
machine logs show user-audit 406
machine mode set 408
machine mode show 409
machine reboot 410
machine reboot-schedule 410
machine reboot-schedule show 411
machine reboot-schedule time 411
machine self-test 412
machine session-inactivity-timeout set 414
machine session-inactivity-timeout show 415
machine set date 415
machine set hostname 416
machine set loghost 417
machine set log invalid-packet 418
machine set log queue 418
machine set timezone 419

machine show backup 420
machine show date 421
machine show hostname 421
machine show loghost 422
machine show log invalid-packet 422
machine show log queue 423
machine show memory 423
machine show priority-stats 425
machine show timezone 426
machine show uptime 426
machine update-queue 427
Команды группы mftp 429
mftp config 429
mftp info 430
mftp show config 431
mftp start 432
mftp stop 432
Команды группы poe 433
poe interface check-ip action add restart 433
poe interface check-ip action clean 434
poe interface check-ip action del restart 435
poe interface check-ip address 435
poe interface check-ip failed-attempts 436
poe interface check-ip frequency 437
poe interface check-ip mode 438
poe interface faststart 439
poe interface limit 440
poe interface power 441
poe interface priority 442
poe set syslog-level 442
poe show 443
Команды группы service 448
service cert delete 448
service cert import 449
service cert list 450
service cert request create 451
service cert request delete 453
service cert request export 453
service cert request list 454

service cert request show 454
service cert show cert 455
service cert show crl 456
service http-proxy antivirus bypass 457
service http-proxy antivirus mode 458
service http-proxy antivirus server-url add 458
service http-proxy antivirus server-url delete 459
service http-proxy antivirus server-url list 460
service http-proxy antivirus show-status 460
service http-proxy cache 461
service http-proxy content-filter add 462
service http-proxy content-filter change num 464
service http-proxy content-filter default-reply-action 465
service http-proxy content-filter default-request-action 466
service http-proxy content-filter delete 467
service http-proxy content-filter list 467
service http-proxy content-filter mode 468
service http-proxy content-filter move 469
service http-proxy content-filter show-status 470
service http-proxy external-address set 470
service http-proxy external-address show 471
service http-proxy fw-rules apply 471
service http-proxy fw-rules delete 472
service http-proxy fw-rules show 473
service http-proxy listen-address add 473
service http-proxy listen-address delete 474
service http-proxy listen-address list 475
service http-proxy mode 475
service http-proxy reset 476
service http-proxy show 477
service http-proxy start 477
service http-proxy stop 478
service http-proxy transparent-mode 478
service mbgw add 479
service mbgw after-send-delay 480
service mbgw baudrate 480
service mbgw before-send-delay 481
service mbgw delete 482
service mbgw mode 483

service mbgw parity ... 483
service mbgw port ... 484
service mbgw request-timeout ... 485
service mbgw response-timeout ... 486
service mbgw routing add ... 486
service mbgw routing change ... 487
service mbgw routing delete ... 488
service mbgw routing show ... 489
service mbgw serial ... 490
service mbgw show ... 490
service mbgw start ... 492
service mbgw stop ... 492
service mbgw syslog-level ... 493
service mbgw type ... 494
service piomonitor mode ... 494
service piomonitor reset ... 495
service piomonitor set activelevel ... 496
service piomonitor set In custom ... 497
service piomonitor set In emergency ... 497
service piomonitor set In tamper ... 498
service piomonitor set Out cluster ... 499
service piomonitor set Out event ... 499
service piomonitor set syslog-level ... 500
service piomonitor show ... 501
service piomonitor start ... 502
service piomonitor stop ... 503
service usbmodem set syslog-level ... 503
service usbmodem show config ... 504
service usbmodem show status ... 504
service vpn mode ... 506
service vpn show status ... 507
service vpn start ... 507
service vpn stop ... 508
Команды группы ups ... 509
ups set driver ... 509
ups set mode ... 509
ups set monitoring ... 510
ups show config ... 511
ups show status ... 511

ups start ... 512
ups stop ... 513
Команды группы user ... 514
user certificate create ... 514
user certificate delete ... 515
user passwd ... 515
user reset passwd ... 516
Команды группы vpn ... 518
vpn config delete ... 518
vpn config list ... 518
vpn config load ... 519
vpn config save ... 520
Команды группы webui ... 522
webui https-cert ... 522
webui info ... 522
webui port ... 523
webui protocol ... 524
webui recreate-cert ... 525
webui restart ... 526
Прочие команды ... 528
debug off ... 528
debug on ... 529
enable ... 530
exit ... 530
hardware-status show ... 531
hardware-status show memory ... 531
license ... 534
serial ... 535
version ... 536
version features list ... 537
who ... 537

Глава 2. Справочник конфигурационных файлов ... 539
Файл iplir.conf ... 540
Секция [adapter] ... 540
Секция [debug] ... 541
Секция [dynamic] ... 542
Секция [id] ... 542
Секция [misc] ... 548

Секция [servers] ... 551
Секция [virtualip] ... 551
Секция [visibility] ... 551
Файл iplir.conf-<интерфейс или группа интерфейсов> ... 553
Секция [db] ... 553
Секция [cef] ... 555
Файл failover.ini ... 556
Секция [channel] ... 556
Секция [debug] ... 559
Секция [misc] ... 559
Секция [network] ... 561
Секция [sendconfig] ... 562
Секция [events] ... 564
Файл mftp.conf ... 565
Секция [channel] ... 565
Секция [debug] ... 566
Секция [journal] ... 567
Секция [misc] ... 568
Секция [reserv] ... 570
Секция [transport] ... 571
Секция [upgrade] ... 571

Приложение А. Термины и сокращения ... 573



Введение

О документе 21

Соглашения документа 22

Обратная связь 24

О документе

Документ содержит описание команд, доступных для выполнения в командном интерпретаторе ViPNet Coordinator IG. В нем приведены синтаксис команд, руководство по использованию, а также примеры команд. Команды сгруппированы по первому ключевому слову, список групп и список команд внутри каждой группы упорядочены по алфавиту.

Также в документе приведено подробное описание параметров следующих конфигурационных файлов ViPNet Coordinator IG:

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

Параметры в конфигурационных файлах используются для настройки ViPNet Coordinator IG. Некоторые параметры задаются программным обеспечением (далее — ПО) ViPNet® автоматически, они носят информационный характер и служат для того, чтобы администратор в процессе работы мог посмотреть их значения для выполнения каких-либо настроек или подключения к ViPNet Coordinator IG. Изменять такие параметры вручную не следует, в данном документе они называются нередактируемыми и описаны в специальных подразделах.

Соглашения документа

Внимание! Все сценарии работы с ViPNet Coordinator IG 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 26

Команды группы alg 36

Команды группы failover 41

Команды группы firewall 49

Команды группы inet 68

Команды группы ipf 303

Команды группы iplir 332

Команды группы machine 378

Команды группы mftp 429

Команды группы poe 433

Команды группы service 448

Команды группы ups 509

Команды группы user 514

Команды группы vpn 518

Команды группы webui 522

Прочие команды 528

Команды группы admin

Управление паролем и сертификатом администратора, 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 PIN-код администратора USB-токена, затем введите и подтвердите PIN-код 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 IG 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 в следующих сценариях:

- перезагрузка;
- обновление ПО;
- проверка целостности ПО;
- восстановление конфигурации.

Пример использования

```
hostname# admin clear-auth-warning

Password guessing counter was cleared.
```

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 достаточно изменить пароль только на активном узле. Если узлы кластера переключились до того, как активный узел передал новый пароль на пассивный, доступ на узел, который стал активным, вы можете получить по старому паролю.

Пример использования

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

admin remove keys

Удалить ключи и справочники ViPNet Coordinator IG.

Синтаксис

```
admin remove keys
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда недоступна в удаленной SSH-сессии.
- Если на ViPNet Coordinator IG 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 2025
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 IG.

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 IG.

Синтаксис

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

Режимы командного интерпретатора

Режим настройки.

Особенности

Если вы выполните команду при удалённом подключении по протоколу SSH, то удалённая сессия будет разорвана.

Пример использования

```
hostname# admin ssh reset-key local
command: admin ssh remove key local
Resetting 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]-----+
Resetting 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 IG.

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 system erase

Удалить ПО ViPNet Coordinator IG вместе с ключами, справочниками и настройками.



Внимание! После выполнения команды ViPNet Coordinator IG станет неработоспособным. Для восстановления работоспособности необходимо установить ПО и инициализировать ViPNet Coordinator IG (см. документ «Настройка с помощью командного интерпретатора», раздел «Установка ПО с USB-носителя»).

Синтаксис

```
admin system erase
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна для исполнений ViPNet Coordinator IG10 и ViPNet Coordinator IG100.
- Команда недоступна по SSH.
- Перед использованием команды рекомендуется выполнить экспорт файлов системного журнала ViPNet Coordinator IG (см. machine logs export usb).
- Чтобы подтвердить удаление ПО, после соответствующего сообщения нажмите и удерживайте кнопку **Reset** на корпусе ViPNet Coordinator IG в течение 1–2 секунд.

Пример использования

```
hostname# admin system erase
This command completely removes all VPN software and cannot be reverted,
it will be necessary to deploy new software after executing this command.
Do you really wish to execute this command ? [Yes,No]: Yes
For removing all ViPNet software press RESET button within 30 seconds
Stopping Advanced Configuration and Power Interface daemon: acpid.
ViPNet system software erase started.
```

admin upgrade software

Обновить ПО ViPNet Coordinator IG вручную с USB-носителя.

Синтаксис

```
admin upgrade software
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда недоступна по SSH.
- Для обновления ПО необходимы:
  - файл обновления ПО: `<платформа ViPNet Coordinator IG>_vipnet_base_x86_64_driv_<версия ViPNet Coordinator IG>.zip`, например, `ig100_vipnet_base_x86_64_driv_5.2.0-4388.zip`;
  - файл ЭП обновления: `<платформа ViPNet Coordinator IG>_vipnet_base_x86_64_driv_<версия ViPNet Coordinator IG>.zip.sig`.
- Файл обновления ПО и файл ЭП обновления должны находиться в одном каталоге USB-носителя.
- Если ViPNet Coordinator IG работает как межсетевой экран типа «Д», то перед обновлением переключите его в режим регламентного обслуживания (см. machine mode set).
- После обновления ПО необходимо перезагрузить ViPNet Coordinator IG.
- После ввода команды сессии всех пользователей завершаются.

Пример использования

```
hostname# admin upgrade software
Insert USB flash drive and press <Enter>
Checking integrity and signature of 'ig100_vipnet_base_arm_driv_5.2.0-4669.zip'
Select file to use for software upgrade:
1 — /mnt/tmp/sdb1/ig100_vipnet_base_arm_driv_5.2.0-4669.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

Разрешить или запретить прохождение потоков RTP-сессий между IP-телефонами напрямую при обработке прикладного протокола H.323 или SIP.

Синтаксис

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

Параметры и ключевые слова

- `<прикладной протокол>` — имя обрабатываемого прикладного протокола: `h323` или `sip`
- `on` — пропускать RTP-сессию, если она создаётся с тем же IP-адресом источника или назначения, что и родительская сигнальная сессия;
- `off` — пропускать RTP-сессию с любым IP-адресом.

Значения по умолчанию

При включении обработки H.323 или SIP сетевые фильтры будут пропускать RTP-сессию, если она создаётся с тем же IP-адресом источника или назначения, что и родительская сессия (`on`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Чтобы настройки вступили в силу, выполните команду:

```
hostname# firewall conntrack flush
```

Пример использования

Если потоки родительской сигнальной сессии проходят через SIP-сервер, а потоки RTP-сессии должны проходить между IP-телефонами напрямую (пути прохождения потока сигнальной сессии и RTP-потока отличаются), выполните команду:

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

alg module h323 direct-h245

Разрешить или запретить прохождение потоков H.245-сессий между IP-телефонами напрямую при обработке прикладного протокола H.323.

Синтаксис

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

Параметры и ключевые слова

- `on` — пропускать H.245-сессию, если она создаётся с теми же IP-адресами, что и родительская H.225-сессия;
- `off` — пропускать H.245-сессию с любым IP-адресом.

Значения по умолчанию

При включении обработки H.323 сетевые фильтры будут пропускать H.245-сессию, если она создаётся с теми же IP-адресами, что и родительская H.225-сессия (`on`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Чтобы настройки вступили в силу, выполните команду:

```
hostname# firewall conntrack flush
```

Пример использования

Если потоки родительской H.225-сессии проходят через контроллер зоны, а потоки H.245-сессии должны проходить между IP-телефонами напрямую (пути прохождения H.225-потока и H.245-потока отличаются), выполните команду:

```
hostname# alg module h323 direct-h245 off
```

alg module process off

Выключить обработку прикладного протокола.

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.

Пример использования

Чтобы выключить обработку прикладного протокола DNS:

```
hostname# alg module dns process off
Waiting for alg daemon..
```

alg module process on

Включить обработку прикладного протокола или изменить параметры его обработки.

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 `ftp`, `h323`, `sccp` или `sip`.
- `udp` — транспортный протокол UDP для обработки прикладного протокола `sip`, `h323` или `dns`.
- `<порты>` — номера портов для обработки.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

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
Waiting for alg daemon..
```

alg show

Просмотреть параметры обработки прикладных протоколов.

Синтаксис

```
alg show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются:

- `SERVICE` — название прикладного протокола.
- `PROTOCOL` — транспортный протокол для обработки.
- `PORTS` — порты для обработки.
- `ON/OFF` — состояние обработки: `ON` (включена) или `OFF` (выключена).

Пример использования

```
hostname> alg show
=============================================================
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
-------------------------------------------------------------
MODBUS         TCP             502                  OFF
-------------------------------------------------------------
IEC104         TCP             2404                 OFF
-------------------------------------------------------------
SIP            TCP             5060,5080            ON
```

```
-------------------------------------------------------------
SIP             UDP             5060,5080            ON
-------------------------------------------------------------
```

Команды группы failover

Настройка и управление системой защиты от сбоев ViPNet Coordinator IG.

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 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

Изменить режим работы системы защиты от сбоев.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Установлен одиночный режим (`single`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды завершите работу службы `failoverd`.
- При установке режима кластера автоматически будет завершена работа драйверов и служб, которые не поддерживаются в этом режиме.
- При установке одиночного режима автоматически будет завершена работа всех служб.

Пример использования

Перевести систему защиты от сбоев в режим кластера:

```
hostname# failover config mode cluster
Do you want to switch to the cluster mode? [Yes,No]:Yes
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 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 информацию о состоянии 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 IG и системы защиты от сбоев;
- `ID` — идентификатор и имя узла ViPNet;
- `workstation time` — локальное время на узле ViPNet;
- `failover mode` — режим работы системы защиты от сбоев:
  - `single` — одиночный режим работы;
  - `active` — активный режим работы в составе кластера;
  - `passive` — пассивный режим работы в составе кластера;
- `failover uptime` — время непрерывной работы системы защиты от сбоев;
- `total cpu` — общая загруженность процессора;
- `total memory` — общий объём памяти;
- `available memory` — объём доступной памяти;
- сведения о текущем состоянии служб failover, iplir, mftp, webgui, usbmodem, piomonitor, ipf:
  - статус службы:
    - `initializing` — загружается;
    - `works` — работает;
    - `stopped` — работа завершена;

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

- сведения о ресурсах процессора, используемых службой.

Пример использования

```
hostname> failover show info
Running failover info

Versions: ViPNet 5.2.0 (40258), daemon 1.5 (1)

Workstation configured for ID 2CEC000A (IG100-I1-1)

The workstation works in a single mode of protection against failures

Workstation time (utc: 1406806848) Tue May 28 17:31:45 2024

  failover mode            * single
  failover uptime          * 0d 0:14
  total cpu                * 6%
  total memory             * 2055488 Kb
  available memory         * 1915324 Kb
  failover state           * works
  failover cpu             * 1%
  iplir state              * works
  iplir cpu                * 4%
  mftp state               * works
  mftp cpu                 * 1%
  webgui state             * works
  webgui cpu               * 0%
  usbmodem state           * stopped
  piomonitor state         * stopped
  ipf state                * works
  ipf cpu                  * 1%
```

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 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 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 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 10.02.2022.08.00.00 15.02.2022.19.00.00
  View journal of failover switching
  Versions: ViPNet 4.5.1 (40318), daemon 1.5 (1)
  Workstation configured for ID 3412000E (IG-10-1)
  The workstation works in a cluster mode of protection against failures
  Workstation time (utc: 1594810209) Tue Feb 15 08:00:00 2022

  10 Feb 2022 12:51:42    <P_START> Start failover daemon in passive mode
  11 Feb 2022 12:27:27    <A_START> Start failover daemon in active mode
  11 Feb 2022 14:10:35    <A_START> Start failover daemon in active mode
  11 Feb 2022 15:30:46    <BOOT> Boot the system
12 Feb 2022 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>
[<протокол>] [<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.
- `<протокол>` — транспортный протокол, по которому передаются IP-пакеты.
- `<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 вы можете указать:
  - 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 `local` и `remote`;
  - для фильтров защищённой 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 отправителя не `local`, то адрес получателя должен быть `local` или `broadcast`.
  - для фильтров туннелируемых узлов — то же, что для локальных фильтров открытой сети и фильтров защищённой сети, но в таких фильтрах можно использовать только следующие системные группы объектов: `any`, `allcoordinators`, `allclients` или `tunneledip`; кроме того, если в качестве адреса отправителя задан идентификатор узла ViPNet, то в качестве адреса получателя должен быть адрес открытого узла, и наоборот.
  - 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 вы также можете указать для локальных и транзитных фильтров открытой сети и фильтров туннелируемых узлов:
  - сетевой интерфейс собственного узла в виде:

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

  - системную группу объектов (`local`, `remote`, `multicast`, `broadcast` кроме `any`) и сетевой интерфейс собственного узла:

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

- В качестве адреса получателя вы также можете указать:
  - для локальных фильтров открытой сети — системную группу `broadcast` или `multicast`;
  - для фильтров защищённой сети — системную группу `broadcast`.

- При задании доменного имени нельзя использовать кириллицу.
- Транспортный протокол вы можете задать, используя:
  - имена протоколов, написанные строчными буквами и разделённые пробелами. При этом вы можете задать дополнительные параметры:
    - для TCP и UDP: `sport` (порт или диапазон портов источника пакета), `dport` (порт или диапазон портов назначения пакета) или оба этих параметра — сначала `sport`, затем `dport`. Чтобы указать несколько портов или диапазонов портов, укажите название протокола (`tcp` или `udp`) перед каждым номером порта или диапазоном портов. Например: `tcp sport 2525 tcp dport 443 tcp dport 4444-4445`.
    - для ICMP: `type` (тип пакета) или `type` с параметром `code` (код пакета). Если `code` не задан, то под условие будут подпадать все ICMP-пакеты указанного типа.
  - номера протоколов. Перед номером каждого протокола укажите `proto`;
  - пользовательские группы протоколов в виде: `service @<имя группы>`.
- Для правила трансляции с использованием порта назначения укажите адрес назначения и транспортный протокол TCP или UDP.
- Расписание задаётся 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 вы можете 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 в журнале IP-пакетов при срабатывании фильтра задаётся лексемой `log`:
  - `on` — регистрировать IP-пакеты.

    По умолчанию устанавливается для всех фильтров с действием блокировать (`drop`) и отклонить (`reject`).
  - `off` — не регистрировать IP-пакеты.

    По умолчанию устанавливается для всех фильтров с действием пропускать (`pass`).
- Действие для сетевых фильтров задаётся одной из следующих лексем:
  - `pass` — пропускать IP-пакеты;
  - `drop` — блокировать IP-пакеты;
  - `reject` — отклонять IP-пакеты с отправкой ICMP-уведомления об ошибке `Destination port unreachable`;

    Для отправки других ICMP-уведомлений доступны модификации `reject`:
    - `rej-net-unreachable` — отправлять ICMP-сообщение `Destination net unreachable`;
    - `rej-host-unreachable` — отправлять ICMP-сообщение `Destination host unreachable`;
    - `rej-proto-unreachable` — отправлять ICMP-сообщение `Destination protocol unreachable`;
    - `rej-net-prohibited` — отправлять ICMP-сообщение `Network administratively prohibited`;
    - `rej-host-prohibited` — отправлять ICMP-сообщение `Host administratively prohibited`;
    - `rej-admin-prohibited` — отправлять ICMP-сообщение `Communication administratively prohibited`;
    - `rej-tcp-reset` — отправлять ICMP-сообщение `TCP reset` (только для TCP-пакетов).
- Действие для правил трансляции адресов задаётся одной из следующих лексем:
  - `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;
  - `change dst <адрес>:[<порт>]` — перенаправлять пакеты на указанные адрес и порт.

- После создания фильтра защищённой сети, локального фильтра открытой сети или фильтра туннелируемых узлов, такой фильтр не будет действовать на уже установленные соединения до истечения времени жизни этих соединений. Транзитный фильтр открытой сети действует сразу после его создания.

Примеры использования

Примечание. В первом сетевом фильтре, для примера указан номер и имя фильтра, в последующих фильтрах эти параметры не указаны.

- Создать локальный фильтр, блокирующий IP-пакеты, отправляемые узлом с адресом 192.168.30.1 через порт 2525 на порт 443 открытого узла с адресом 172.16.35.1 по протоколу TCP/IP:

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

- Создать фильтр, разрешающий отправку IP-пакетов от защищённого узла с идентификатором 0x1234abab туннелируемому узлу с адресом 192.168.0.1 ежедневно в интервал с 8 утра до 8 вечера:

  ```
  hostname# firewall tunnel add src 0x1234abab dst 192.168.0.1 daily 8:00-20:00 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 координатор подменял адрес получателя (публичный IP-адрес координатора) на локальный адрес, создайте правило трансляции адреса назначения:

  ```
  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 координатора, создайте правило трансляции адреса источника:

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

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

  ```
  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. Допустимые символы: a–z, A–Z, 0–9, _ и точка.
- `<состав>` — объекты, входящие в группу.
- `<исключения>` — объекты, не входящие в группу.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Имя группы объектов должно быть уникальным.
- 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

Примечание. В зависимости от текущего уровня вычислительной нагрузки ViPNet Coordinator IG выполнение команды может занимать до 30 секунд.

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

Синтаксис

```
firewall <тип> change append <номер> [src <адрес отправителя>] [dst <адрес получателя>]
[<протокол>] [<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.
- `<адрес отправителя>` — добавляемый адрес отправителя IP-пакетов.
- `<адрес отправителя>` — добавляемый адрес получателя IP-пакетов.
- `<протокол>` — добавляемый транспортный протокол, по которому передаются IP-пакеты.
- `<расписание>` — добавляемое расписание применения фильтра или правила трансляции.
- `log` — регистрация IP-пакетов при срабатывании фильтра в журнале IP-пакетов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Синтаксис адреса отправителя, адреса получателя, протокола и расписания — тот же, что при создании сетевого фильтра или правила трансляции с помощью команды firewall add.
- Можно указать несколько параметров.

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 ещё 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
```

firewall conntrack flush

Закрыть все открытые соединения.

Синтаксис

```
firewall conntrack flush
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# firewall conntrack flush
connection tracking table has been emptied
```

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 (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 (правила трансляции) с помощью команды firewall add.
- Можно указать несколько параметров.
- Поиск фильтров (правил трансляции) для удаления выполняется 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            |
+====+============+==========+============+==========+
|7   |Allow syslog outgoing  |User        |          |
+----+-----------+-----------+------------+----------+
|pass|udp: to 514 |@local    |@any                   |
+====+============+==========+============+==========+
Do you want to perform the action on the above rule? [Yes/No]:
```

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 группы объектов по типам: ViPNet-узлы, IP-адреса, интерфейсы, протоколы и расписания.

Синтаксис

```
firewall <тип группы> show
```

Параметры и ключевые слова

`<тип группы>` — тип группы объектов:

- `ip-object` — группы IP-адресов;
- `vpn-object` — группы ViPNet-узлов;
- `interface-object` — группы сетевых интерфейсов;
- `service-object` — группы протоколов;
- `schedule-object` — группы расписаний;
- `object` — все типы групп объектов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- По каждому типу группы объектов отображаются:
  - название типа группы объектов:
    - `VPN Objects` — ViPNet-узлы;
    - `Ip Objects` — IP-адреса;
    - `Interface Objects` — интерфейсы;

    - `Service Objects` — протоколы;
    - `Schedule Objects` — расписания;
  - `Current Rules Set Id` — номер текущей конфигурации сетевых фильтров и правил трансляции адресов;
  - `Num` — порядковый номер группы;
  - `Name` — имя группы;
  - `Creation Type` — тип группы:
    - `Policy` — группа из ViPNet Prime Policy Management;
    - `User` — задана по умолчанию или настраиваемая группа;
  - `Inclusion` — объекты, входящие в группу;
  - `Exclusion` — объекты, не входящие в группу.
- Чтобы завершить просмотр, нажмите **Q**.

Пример использования

```
hostname> firewall object show
Ip Objects
Current Rules Set Id: 139
================================================================================
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
Current Rules Set Id: 139
================================================================================
Num  Name                                          Creation type
Inclusion                          Exclusion
================================================================================
1    DHCP                                          User
udp: from 67-68 to 67-68
--------------------------------------------------------------------------------
2    CITRIX                                        User
tcp: to 1494
--------------------------------------------------------------------------------
...
--------------------------------------------------------------------------------
Schedule Objects
Current Rules Set Id: 139
```

```
================================================================================
Num  Name                                                Creation type
Inclusion                              Exclusion
================================================================================
1    Workdays                                            User
weekly: 00:00:00 - 23:59:00 Mon Tue
Wed Thu Fri
--------------------------------------------------------------------------------
2    Weekends                                            User
weekly: 00:00:00 - 23:59:00 Sat Sun
--------------------------------------------------------------------------------
```

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 settings

Изменить параметры межсетевого экрана.

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` (по умолчанию) или выключено — `off`;
- `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 — 300;
- `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 IG.

Таблица 1. Значения max-connections для исполнений ViPNet Coordinator IG

Аппаратная платформа	По умолчанию	Максимальное
ViPNet Coordinator IG10 I1	1000	1000
ViPNet Coordinator IG10 I2	1000	1000
ViPNet Coordinator IG100 I1	15000	15000
ViPNet Coordinator IG100 I4	1000000	1000000
ViPNet Coordinator IG100 I5	15000	15000
ViPNet Coordinator IG1000 Q1	2500000	2500000

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 1000:

```
hostname# firewall settings max-connections 1000
```

firewall settings show

Просмотреть параметры межсетевого экрана ViPNet Coordinator IG.

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;
- `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.
- `Log invalid packet` — регистрация нарушения параметров таблицы соединений;
- `Log queue` — регистрация событий об отклонённых IP-пакетах.

Пример использования

```
hostname# firewall settings show
Antispoofing                off
Block fragmented packets    on
Connection ttl TCP          1800
```

```
Connection ttl UDP          300
Connection ttl IP           300
Connection ttl stream UDP   180
ICMP timeout                30
Max connections             1000000
TCP SYN RECV timeout        30
TCP SYN SENT timeout        30
TCP WAIT timeout            15
Log invalid packet          on
Log queue                   off
```

firewall show

Просмотреть сетевые фильтры или правила трансляции адресов.

Синтаксис

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

Параметры и ключевые слова

- `<тип>` — тип сетевых фильтров или правила трансляции адресов:
  - `local` — локальные фильтры открытой сети;
  - `forward` — транзитные фильтры открытой сети;
  - `tunnel` — фильтры туннелируемых узлов;
  - `vpn` — фильтры защищённой сети;
  - `nat` — правила трансляции адресов;
  - `rules` — все типы сетевых фильтров и правила трансляции адресов;
- `<параметры>` — параметры фильтров или правил трансляции, отбираемых для просмотра:
  - `<номер>` — порядковый номер сетевого фильтра или правила трансляции адресов;
  - `pass`, `drop`, `reject` — действие сетевого фильтра;
  - `src <адрес>` — адрес отправителя;
  - `dst <адрес>` — адрес получателя;
  - `tcp [sport <порт> и/или dport <порт>]`, `udp [sport <порт> и/или dport <порт>]`, `icmp` — протокол, указанный в сетевом фильтре или правиле трансляции.

Значение по умолчанию

Без указания параметров отображаются все сетевые фильтры заданного типа или правила трансляции адресов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Можно указать несколько параметров, если не указан `<номер>`.
- Поиск фильтров и правил трансляции выполняется по строгому совпадению с указанными параметрами.
- При сочетании параметров `rules` и `<номер>` поиск выполняется только в фильтрах типа `vpn`.
- По команде отображаются таблицы, содержащие соответствующие типы сетевых фильтров или правила трансляции адресов, в следующем порядке:
  - `VPN` — фильтры защищённой сети;
  - `Tunnel` — фильтры туннелируемых узлов;
  - `Local` — локальные фильтры открытой сети;
  - `Forward` — транзитные фильтры открытой сети;
  - `NAT` — правила трансляции адресов.
- Для таблиц сетевых фильтров каждого типа отображаются:
  - фильтры по группам сетевых фильтров:
    - `Service` — служебные фильтры;
    - `Policy` — фильтры политик безопасности;
    - `User` — настраиваемые фильтры;
    - `Default` — фильтр по умолчанию;
  - `Current Rules Set Id` — номер текущей конфигурации типа сетевых фильтров;
  - структура таблицы отображения группы сетевых фильтров:
    - `Num` — порядковый номер фильтра;
    - `Name` — идентификатор и имя фильтра;
    - `Option` — группа фильтра;
    - `Schedule` — расписание действия фильтра;
    - `Act` — действие фильтра;
    - `Protocol` — протокол, по которому передаются IP-пакеты;

        - `Source` — адрес отправителя IP-пакетов;
        - `Destination` — адрес получателя IP-пакетов;
- Если для фильтра включена регистрация IP-пакетов при его срабатывании, то перед именем фильтра отображается префикс `[LOG]`.
- Для таблиц правил трансляции адресов отображаются:
    - правила трансляции по группам правил:
        - `Policy` — правила трансляции политик безопасности;
        - `User` — настраиваемые правила трансляции;
    - `Current Rules Set Id` — номер текущей конфигурации правил трансляции;
    - структура таблицы отображения группы правил:
        - `Num` — порядковый номер правила;
        - `Name` — идентификатор и имя правила;
        - `Option` — группа правила;
        - `Schedule` — расписание действия фильтра;
        - `Act` — действие правила (всегда `NAT`);
        - `Protocol` — протокол, по которому передаются IP-пакеты;
        - `Source` — адрес отправителя IP-пакетов;
        - `Destination` — адрес получателя IP-пакетов;

Пример использования

Для просмотра локальных фильтров для протокола UDP:

```
hostname> firewall local show udp
empty rule for  Service:
 User:
Current Rules Set Id: 2
================================================================================
Num    Name                                          Option         Schedule
Act    Protocol               Source                -> Destination
================================================================================
5      4000064 - Allow DNS                           User
pass   udp:                   @local                -> @any
        to 53,
       tcp:
        to 53
```

```
--------------------------------------------------------------------------------
6      4000064 - Allow NTP                                 User
pass   udp:                    @local                  -> @any
        to 123
--------------------------------------------------------------------------------
7      4000066 - Allow DHCP server req                     User
pass   udp:                    @local                  -> @any
        from 67
        to 68
--------------------------------------------------------------------------------
```

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 IG.
- `off` — выключить BGP-маршрутизацию и не включать при перезагрузке ViPNet Coordinator IG.

Режимы командного интерпретатора

Режим настройки.

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.

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.

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.

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 2. 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.

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.

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.

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.

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.

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 bgp 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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`, `` `~!@#$%^&*()-_=+{}[]|\/:;"'<>,. ``

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.

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.

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.

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.

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.

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.

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 подсеть.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим настройки.

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.

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.

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.

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.

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.

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.

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 IG.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

По умолчанию router id назначается автоматически.

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`.

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.

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.

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).

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.

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 только 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 только 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 только 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 только 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 только 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 только 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 только 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 только 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 только 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 только 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

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 IG (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 IG нельзя использовать в одном агрегированном интерфейсе.

Пример использования

Чтобы создать агрегированный интерфейс `bond2`, работающий в режиме `balance-rr`, с подчиненными физическими интерфейсами `eth2` и `eth3`:

```
hostname# inet bonding add 2 mode balance-rr slaves eth2 eth3

New bond interface bond2 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/4G 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/4G 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/4G 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 IG. 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 IG.

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 IG (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);
  - интерфейс «внутренней петли» (loopback, localhost);

- виртуальные интерфейсы, созданные после назначения дополнительных IP-адресов физическим интерфейсам (alias).

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);

- 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 IG.

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 IG, 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 VPN-узла, 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 VPN-узла, 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 VPN-узла 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 VPN-узла, 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 VPN-узла 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.
- 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 VPN-узла, 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 VPN-узла, 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 VPN-узла 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.
- 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 VPN-узла, 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).
  - Удалите сетевой интерфейс DHCP-сервера.
- 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.

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 VPN-узла, для которого задана опция DHCP-сервера (в параметрах секции `[id]` указанного узла).

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 VPN-узла, 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 VPN-узла, для которого задана маска подсети (в параметрах секции `[id]` указанного узла).

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 VPN-узла, для которого заданы параметры TFTP-сервера (в параметрах секции `[id]` указанного узла).

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 VPN-узла, для которого заданы параметры TFTP-сервера Cisco VoIP (в параметрах секции `[id]` указанного узла).

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.

Синтаксис

```
inet dhcp server delete wins <IP-адрес>
```

Параметры и ключевые слова

`<IP-адрес>` — IP-адрес WINS-сервера.

Значения по умолчанию

По умолчанию список адресов WINS-серверов содержит адрес 172.16.1.1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

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

Пример использования

Чтобы из списка передаваемых адресов WINS-серверов удалить адрес 172.16.1.1:

```
hostname# inet dhcp server delete wins 172.16.1.1
```

inet dhcp server mode

Включить или выключить автоматический запуск DHCP-сервера при загрузке ViPNet Coordinator IG.

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 IG, 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 IG.

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 IG.

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 работает автозаполнение 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
```

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 выполняется 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 автозаполнение 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 IG.

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.

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-2025 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-2025 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 максимальный размер журнала DNS-запросов.

Синтаксис

```
inet dns querylog size <размер>
```

Параметры и ключевые слова

`<размер>` — максимальный размер журнала DNS-запросов: 1–50 МБайт.

Значения по умолчанию

10 МБайт (`10`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Если команда выполняется при запущенном DNS-сервере, он перезапускается.

Пример использования

```
hostname# inet dns querylog size 50
DNS requests log size: 50 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 автозаполнение 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, если система защиты от сбоев запущена в режиме кластера. Иначе это может вызвать сбои в работе кластера.

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 к агрегированному.

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

- Задаваемый подчиненный физический интерфейс должен относиться к классу `slave` (см. inet ifconfig class).
- Задаваемый подчиненный физический интерфейс не должен быть привязан ни к одному агрегированному интерфейсу.
- Для каждого агрегированного интерфейса можно добавить не более трех подчиненных физических интерфейсов.
- Максимальное количество интерфейсов в ViPNet Coordinator IG (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.

Пример использования

Чтобы для агрегированного интерфейса `bond1` добавить физический 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 IG 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 прохождение 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 автозаполнение 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 IG.

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 IG.

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>` — максимальный размер полезного блока данных одного пакета, который может быть передан без фрагментации. Допустимые значения: 1280–9000 байт.
- `auto` — задаёт значение MTU по умолчанию (1500 байт).

Значения по умолчанию

По умолчанию используется значение MTU 1500 байт.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна в исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1. Во всех других исполнениях значение MTU не меняется и равно 1500 байт.



Примечание. Для исполнения ViPNet Coordinator IG100 I4 задавайте MTU в диапазоне 1280–1518.

- 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 подчинённых физических интерфейсах класса `slave`.
- При создании агрегированного интерфейса с помощью командного интерпретатора для всех подчинённых физических интерфейсов автоматически задаётся значение MTU 1500 байт.
- Если вы исключаете подчинённый физический интерфейс из агрегированного, для исключённого интерфейса устанавливается значение MTU 1500 байт.

Пример использования

Задать MTU 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.
  - 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`.
- `duplex` — режим передачи данных:
  - `half` — полудуплекс;
  - `full` — полный дуплекс.
- `autoneg` — режим автосогласования скорости интерфейса (autonegotiation):
  - `on` — режим автосогласования включен;
  - `off` — режим автосогласования выключен.

Значения по умолчанию

На интерфейсе установлены автоматические параметры (определяются, исходя из характеристик интерфейса).

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 к интерфейсам класса slave (см. inet ifconfig class).
- Установку параметров скорости интерфейса следует использовать с осторожностью и только в тех случаях, когда это действительно необходимо — например, для согласования работы внешнего интерфейса ViPNet Coordinator IG и коммутационного оборудования, подключенного к данному интерфейсу.

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

- 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 к интерфейсам класса slave (см. inet ifconfig class).

Пример использования

Чтобы на интерфейсе `eth1` установить режим автоматического определения параметров скорости:

```
hostname# inet ifconfig eth1 speed auto
```

inet ifconfig type

Задать тип сетевого интерфейса относительно защищённой сети.

Синтаксис

```
inet ifconfig <интерфейс> type {internal | external}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса;
- тип сетевого интерфейса:
  - `internal` — внутренний;
  - `external` – внешний.

Значения по умолчанию

Для всех сетевых интерфейсов задан тип `internal`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Тип `external` предназначен для режима «Со статической трансляцией адресов» с фиксированным внешним адресом, который не используется в ViPNet Coordinator IG, начиная с версии 5.1.0.

Пример использования

```
hostname# inet ifconfig eth1.10 type internal
```

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 IG (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. Для исполнения ViPNet Coordinator IG10 I2 дополнительно зарезервированы для служебного использования номера виртуальных интерфейсов 4093–4094 — для физических интерфейсов `eth0` и `eth1`.

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 автозаполнение 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.

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.

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 `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 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 IG.

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.

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.

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 ntp use-default

Включить или выключить использование NTP-серверов, заданных по умолчанию.

Синтаксис

```
inet ntp use-default {on | off}
```

Параметры и ключевые слова

- `on` — в процессе синхронизации времени использовать NTP-серверы, заданные по умолчанию, а также заданные пользователем и полученные по DHCP.
- `off` — в процессе синхронизации времени использовать только NTP-серверы, заданные пользователем и полученные по DHCP.

Значения по умолчанию

В процессе синхронизации времени используются NTP-серверы, заданные по умолчанию, а также заданные пользователем и полученные по DHCP (`on`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Если необходимо выключить использование NTP-серверов по умолчанию, добавьте не менее четырёх дополнительных NTP-серверов. Иначе, если один из серверов выйдет из строя, у ViPNet Coordinator IG не будет достаточно информации, чтобы определить, какой из оставшихся серверов предоставляет правильное время.

Пример использования

Чтобы выключить использование NTP-серверов по умолчанию и использовать только дополнительные NTP-серверы:

```
hostname# inet ntp use-default off
The default servers are not used for synchronisation.
```

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. Способы 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 способ аутентификации, команда изменяет этот способ.

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, ! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

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.

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, ! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.

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 IG.

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 IG включен протокол маршрутизации OSPF (см. inet ospf mode).
- Чем больше значение приоритета, тем выше вероятность того, что ViPNet Coordinator IG будет выбран назначенным маршрутизатором DR или резервным назначенным маршрутизатором BDR.
- Если приоритет равен нулю, то ViPNet Coordinator IG не участвует в выборе DR или BDR.

- Если ключевое слово `interface` не задано, то значение приоритета для всех интерфейсов ViPNet Coordinator IG устанавливается равным параметру `<приоритет>`.

Пример использования

```
hostname# inet ospf priority 10

Stopping ospf ...

Starting ospf ...
```

inet ospf router-id

Задать идентификатор ViPNet Coordinator IG в формате адреса протокола IPv4.

Синтаксис

```
inet ospf router-id {<идентификатор> | auto}
```

Параметры и ключевые слова

- `<идентификатор>` — идентификатор ViPNet Coordinator IG в формате адреса протокола IPv4.
- `auto` — автоматический выбор идентификатора ViPNet Coordinator IG исходя из максимального значения IP-адреса, назначенного на интерфейсах ViPNet Coordinator IG.

Значения по умолчанию

Максимальное значение IP-адреса из назначенных на интерфейсах ViPNet Coordinator IG.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Использование команды разрешено, если на ViPNet Coordinator IG 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 IG: включен/выключен;
  - идентификатор ViPNet Coordinator IG;
  - состояние перераспределения статических маршрутов: включены/выключены;
  - состояние перераспределения DHCP маршрутов: включены/выключены;
  - список сетей, в которых ViPNet Coordinator IG выполняет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);
  - приоритеты ViPNet Coordinator IG на интерфейсах.
- В кластере команда доступна только 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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 только 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 serial show

Просмотреть информацию обо всех настроенных шлюзах Modbus на последовательных интерфейсах RS-232 и RS-485.

Синтаксис

```
inet serial show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> inet serial show


Serial Port: rs232
Serial Type: rs232
TTY device speed: 115200
TTY device parity: even
Modbus gateway: "electric" is running
Modbus gateway autostart (mode): on
Modbus gateway type: tcp-to-rtu


Serial Port: rs485
Serial Type: rs485
```
```

```
Empty.
```

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 параметры шлюзов.

Синтаксис

```
inet show dgd next-hop [<имя шлюза>]
```

Параметры и ключевые слова

`<имя шлюза>` — уникальное текстовое имя шлюза. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа. При указании данного параметра команда выводит информацию только для указанного шлюза. Если параметр не указан, выводится информация обо всех шлюзах.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В выводе команды содержатся значения заданных параметров шлюзов, такие как:

- имя шлюза;
- собственный IP-адрес шлюза;
- тестовый IP-адрес шлюза;
- способ проверки шлюза;
- режим проверки шлюза;
- количество проверок шлюза;
- время последнего изменения статуса шлюза.

Пример использования

Чтобы просмотреть заданные параметры всех шлюзов:

```
hostname> inet show dgd next-hop
```

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 `all` (`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      2025-12-12 01:37:06
d8:a2:5e:94:40:81  192.168.0.178   foo-2            2025-12-12 01:04:56
e8:9a:8f:6e:0f:60  192.168.0.127   angela           2025-12-11 23:55:32
ec:55:f9:c5:f2:55  192.168.0.179   angela           2025-12-11 23:54:56
f0:4f:7c:3f:9e:dc  192.168.0.183   kindle-1234567   2025-12-11 23:54:31
f4:ec:38:e2:f9:67  192.168.0.185   -NA-             2025-12-11 23:55:40
f8:d1:11:b7:5a:62  192.168.0.184   -NA-             2025-12-11 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 2025/01/30 08:02:54;
ends 5 2025/02/04 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.

Пример использования

```
hostname> inet show dns
DNS server autostart is on
DNS server is RUNNING
```

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:
  - IP-адрес и маска подсети.
  - MAC-адрес физического интерфейса.
  - Настройки получения информации от DHCP-сервера и заданная метрика для маршрутов DHCP-сервера, если на интерфейсе включён 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 (включён или выключен).
- Для интерфейса `wlan0` дополнительно выводится информация о подключении Wi-Fi, в том числе качество и уровень сигнала.
- Если в качестве параметра вы указали имя агрегированного интерфейса, дополнительно выводится информация:
  - режим работы агрегированного канала;
  - частота проверки соединения для подчинённых 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 подчинённый интерфейс;
  - список подчинённых физических интерфейсов.
- Чтобы завершить просмотр нажмите **Q**.

Текущее состояние сетевого интерфейса можно определить по сочетанию выводимых параметров и флагов:

Таблица 3. Состояния сетевого интерфейса

Состояние сетевого интерфейса	Выводимые параметры и флаги
Интерфейс включён и функционирует	Флаги: `<UP RUNNING>` — присутствуют

Состояние сетевого интерфейса	Выводимые параметры и флаги
	Параметры: • `Link detected: yes` • `Speed: определено` • `Duplex: определено`
Интерфейс выключен программно	Флаги: `<UP RUNNING>` — отсутствуют Параметры: • `Link detected: no` • `Speed: определено` • `Duplex: определено`
Отключён 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  flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
              inet 192.168.0.1  netmask 255.255.255.0 broadcast 192.168.0.255
              ether 00:14:2d:61:8a:5b txqueuelen 1000 (Ethernet)
              RX packets 50885 bytes 14311469 (13.6 MiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 11053 bytes 7558101 (7.2 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

              Configured by DHCP: yes
              Information requested from DHCP server: IP address, routes, DNS servers,
              NTP servers
              DHCP route metric: default (70)
              Class: access

              Speed: 100Mb/s
              Duplex: Full
              Auto-negotiation: on
              Link detected: yes
```

Просмотреть информацию об интерфейсе `wlan0`:

```
hostname> inet show interface wlan0
```

```
wlan0  flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
               inet 192.168.43.110  netmask 255.255.255.0 broadcast 192.168.43.255
               ether 6c:1d:eb:4b:fa:e2 txqueuelen 1000 (Ethernet)
               RX packets 54 bytes 4916 (4.8 KiB)
               RX errors 0 dropped 1 overruns 0 frame 0
               TX packets 59 bytes 6759 (6.6 KiB)
               TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


wlan0     IEEE 802.11 ESSID:"myNetwork"
               Mode:Managed Frequency:2.437 GHz Access Point: 04:D4:C4:A7:33:B3
               Bit Rate=1 Mb/s  Tx-Power=18 dBm
               Retry short limit:9  RTS thr=2347 B  Fragment thr=2346 B
               Encryption key:off
               Power Management:on
               Link Quality=25/70 Signal level=-85 dBm
               Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
               Tx excessive retries:0 Invalid misc:0 Missed beacon:0

               Configured by DHCP: yes
               Information requested from DHCP server: IP address, routes, DNS servers,
               NTP servers
               DHCP route metric: default (70)
               Class: access
```

inet show interface state

Просмотреть, разрешено или заблокировано прохождение IP-трафика через сетевой интерфейс.

Синтаксис

```
inet show interface state [<интерфейс>]
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса.

Значения по умолчанию

Без указания имени интерфейса команда выполняется для всех интерфейсов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображается:

- имя интерфейса;
- 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        internal     enabled

eth2        internal     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 IG (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 нём.

  - 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 IG (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;
  - `o` — 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 получения ответа;
- `offset` — смещение в миллисекундах между ViPNet Coordinator IG и NTP-серверами;
- `jitter` — абсолютное значение в миллисекундах с указанием среднеквадратичного отклонения смещения относительно ViPNet Coordinator IG;
- `refid` — код ошибки или идентификатор NTP-сервера.

Пример использования

```
hostname> inet show ntp
NTP server autostart is off
NTP server is RUNNING
NTP orphan mode support is off
  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 доступна только 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` — из таблицы маршрутизации:
        - `<номер таблицы>` — номер пользовательской таблицы маршрутизации;
        - `<имя таблицы>` — имя пользовательской таблицы маршрутизации;
        - `default` — из таблицы 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 IG).
- Чтобы завершить выполнение команды, нажмите **Ctrl**+**C**.
- В кластере команда доступна 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 2025
```

inet show usb-modem

Просмотреть настройки модема.

Синтаксис

```
inet show usb-modem
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде на экран выводится следующая информация:

- Состояние службы управления модемом (`starting`/`working`/`stopped`/`error`).
- Тип и производитель модема.
- Тип мобильной сети.
- Уровень сигнала.
- Статус SIM-карты (`OK`/`error`/`not inserted`).
- PIN-код SIM-карты.
- Режим определения оператора мобильной связи (`Auto`/`Manual`).
- Имя оператора мобильной связи.
- Коды MCC и MNC.
- Настройки активного профиля:
  - Имя или адрес точки доступа к интернету (APN).
  - Имя пользователя и пароль.
  - Номер телефона.
- Настройки маршрутизации:
  - Создаётся ли новый маршрут по умолчанию, в котором используется шлюз, полученный при подключении через модем (параметр, заданный командой inet usb-modem route).
  - Создаётся ли DNS-сервер, полученный от мобильного оператора по протоколу DHCP при установлении соединения (параметр, заданный командой inet usb-modem set dns (см. inet usb-modem dns)).
  - Метрика для маршрута по умолчанию, который формируется на основе информации от сервера оператора связи по протоколу PPP. Метрика по умолчанию обозначена `default`.
- Имя сетевого интерфейса, с помощью которого установлено модемное соединение.

Пример использования

```
hostname> inet show usb-modem

Modem software: is working

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

Modem hardware: 3G/4G

Vendor model: Quectel UC20
```

```
Mobile network type: 3G
Signal strength: -85 dBm [great]
SIM-card: OK
PIN code: is not set
PIN verification: N/A
----------------------------------------
Cellular provider define: Auto
Provider country: ru
Cellular provider name: MTS
Multiple APN detected, check your auto settings!
MCC, MNC: 250, 01
APN: internet.mts.ru
Username: mts
Password: mts
Dial number: *99***1#
----------------------------------------
Use DHCP response information: gateway(yes) DNS(yes)
Route metric: default (70)
Connection interface: ppp0
```

inet show usb-modem ip-gw

Просмотреть IP-адрес, заданный командой inet usb-modem ip-gw и используемый в качестве статического адреса шлюза мобильного оператора при настройке резервного канала доступа в интернет.

Синтаксис

```
inet show usb-modem ip-gw
```

Режимы командного интерпретатора

- Режим просмотра
- Режим настройки.

Пример использования

```
hostname> inet show usb-modem ip-gw
```

```
Gateway address: not configured
```

inet show usb-modem provider

Просмотреть предустановленный список мобильных операторов и настройки подключения к мобильным сетям.

Синтаксис

```
inet show usb-modem provider {<код страны> | all} [name {<имя оператора> | all} [type {<точка доступа> | all}]]
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи. Используйте ключевое слово `all`, чтобы посмотреть операторов мобильной связи всех стран.
- `<имя оператора>` — имя оператора мобильной связи. Опустите данный параметр, чтобы посмотреть операторов мобильной связи со всеми именами.
- `<точка доступа>` — доменное имя или IP-адрес сервера мобильного оператора, через который осуществляется подключение к мобильной сети (APN). Опустите данный параметр, чтобы посмотреть операторов мобильной связи со всеми именами точек доступа.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Сначала выводится информация из пользовательского списка операторов (`user`), затем из предустановленного (`common`). Информация выводится в алфавитном порядке по именам операторов.
- Для завершения просмотра нажмите **Q**.

Пример использования

```
hostname> inet show usb-modem provider us name Verizon

Provider country: us

Cellular provider name: Verizon, 4G_LTE_Contract

Cellular provider database: common

MCC, MNC: 310, 995

MCC, MNC: 311, 480

APN: vzwims
```

```
Username: N/A
Password: N/A
Dial number: *99***1#
---------------------------------------
Provider country: us
Cellular provider name: Verizon, 4G_LTE_Contract
Cellular provider database: common
MCC, MNC: 310, 995
MCC, MNC: 311, 480
APN: vzwinternet
Username: N/A
Password: N/A
Dial number: *99***1#
---------------------------------------
Provider country: us
Cellular provider name: Verizon, 4G_LTE_Contract
Cellular provider database: common
MCC, MNC: 310, 995
MCC, MNC: 311, 480
APN: vzwapp
Username: N/A
Password: N/A
Dial number: *99***1#
hostname>
```

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

Просмотреть настройки модуля Wi-Fi.

Синтаксис

```
inet show wifi
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.

Пример использования

```
hostname> inet show wifi

WiFi service autostart is on

The WiFi service role is client
```

```
ssid=TEST
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_passphrase="12345"
wpa_pairwise=TKIP
```

inet show wifi log signal

Просмотреть периодичность записи уровня сигнала Wi-Fi в системный журнал.

Синтаксис

```
inet show wifi log signal
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Команда доступна только на аппаратных платформах со встроенным модулем Wi-Fi.

Пример использования

```
hostname> inet show wifi log signal
WiFi signal strength logging time interval: 5 min
```

inet snmp autostart

Включить или выключить автоматический запуск SNMP-агента при загрузке ViPNet Coordinator IG.

Синтаксис

```
inet snmp autostart {on | off}
```

Параметры и ключевые слова

- `on` — включить запуск SNMP-агента при загрузке ViPNet Coordinator IG.
- `off` — выключить запуск SNMP-агента при загрузке ViPNet Coordinator IG.

Значения по умолчанию

Запуск SNMP-агента при загрузке ViPNet Coordinator IG 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 IG:

```
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, 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

- Community задаётся в процессе выполнения команды.
- Допустимая длина community — от 6 до 18 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.
- Команда доступна только на активном узле кластера. При этом с помощью параметра `<IP-адрес>` задаётся community для доступа к каждому узлу кластера отдельно.

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. Разрешённые символы — прописные и строчные буквы латинского алфавита и цифры.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда доступна только на активном узле кластера. При этом с помощью параметра `<IP-адрес>` задаётся контекст для доступа к каждому узлу кластера отдельно.

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 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, заданные на узлах кластера (если не задан, отображается `Not set`), если указан параметр `community`.
- Команда доступна 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, 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 (пароль) для чтения SNMP-параметров ViPNet Coordinator IG.

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.
- Допустимая длина community — от 6 до 18 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.
- Максимальное количество community — 16.

Пример использования

Чтобы задать community со значением `MyCommunity`:

```
hostname# inet snmp community add
Type new community string: MyCommunity
RO community MyCommunity created
```

inet snmp community change

Изменить community для чтения SNMP-параметров ViPNet Coordinator IG.

Синтаксис

```
inet snmp community change
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда поддерживается в протоколах SNMPv1 и SNMPv2c.
- Для задания нового значения community сначала требуется ввести текущее.
- Допустимая длина community — от 6 до 18 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `( . * / - : _ ? = @ , &)`.

Пример использования

Чтобы изменить community 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, используемый для чтения SNMP-параметров ViPNet Coordinator IG.

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.
- При вводе команды не поддерживается контекстная подсказка.

Пример использования

Чтобы удалить community 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 для чтения SNMP-параметров ViPNet Coordinator IG.

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 IG.

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 IG:

  ```
  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 IG — 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 IG.

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 IG 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 IG — запуск включен (`ON`) или выключен (`OFF`).
- Статус работы по протоколам SNMPv1 и SNMPv2c и статус отправки SNMP-уведомлений по протоколам SNMPv1 и SNMPv2c — разрешена (`ON`) или запрещена (`OFF`).
- Статус работы по протоколу SNMPv3 и статус отправки SNMP-уведомлений по протоколу SNMPv3 — разрешена (`ON`) или запрещена (`OFF`).
- Информация о ViPNet Coordinator IG, 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 IG.

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 IG.

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 IG.

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. Разрешённые 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 IG 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`).

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 IG.

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. Разрешённые 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 IG 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 задаёт 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 IG:

```
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 IG.

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. Разрешённые 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 IG 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 IG:

```
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 IG будет отправлять уведомления.

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 уведомления.
- `v1` — отправлять уведомления типа TRAP по протоколу SNMPv1.
- `inform` — отправлять уведомления типа INFORM по протоколу SNMPv2c.

Значения по умолчанию

- Если порт не задан, используется порт UDP 162.
- Если тип уведомлений 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, заданный на сетевом узле, получающем SNMP-уведомления (trap community).
- Максимальное количество сетевых узлов для SNMP-агента ViPNet Coordinator IG — 16.
- Допустимая длина community — от 6 до 18 символов. Разрешённые символы — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `. * / - : _ ? = @ , &`.
- При указании параметра `v1` отправка уведомлений INFORM невозможна.
- Если вы хотите задать порт, отличный от UDP 162, перед выполнением команды добавьте сетевой фильтр, разрешающий передачу SNMP-уведомлений на данный порт (firewall add).

Пример использования

Чтобы SNMP-агент ViPNet Coordinator IG отправлял уведомления 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 IG отправляет уведомления.

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 IG заданы сетевые узлы с одинаковым IP-адресом и портом, но с разными community — удаляются все такие сетевые узлы.

Пример использования

Чтобы удалить сетевой узел с IP-адресом 10.0.0.1, принимающий SNMP-уведомления 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 уведомления.

Синтаксис

```
inet snmp trapsink list [secure]
```

Параметры и ключевые слова

`secure` — отображать trap community.

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 уведомления:

```
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 уведомления, включая trap community:

```
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 IG.

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. Разрешённые 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, введённые символы отредактировать нельзя.
- Допустимая длина пароля — от 8 до 32 символов. Разрешённые символы пароля — прописные и строчные буквы латинского алфавита, цифры и специальные символы: `! @ # $ % ^ & * () - _ + = ; : ' " , . < > / ? \ | ` ~ [ ] { }`.
- Максимальное количество пользователей на SNMP-агенте — 32.
- Пользователь создаётся 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 IG.

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 IG.

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
```

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-уведомлений;

параметры отправки SNMP-уведомлений.

inet snmp user set key

Создать, изменить или удалить ключ шифрования пользователя SNMP-агента ViPNet Coordinator IG.

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, введённые символы отредактировать нельзя.
- Допустимая длина ключа шифрования — от 8 до 32 символов. Разрешённые 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 удалён:

```
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 IG.

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. Разрешённые символы имени пользователя — прописные и строчные буквы латинского алфавита и цифры.
- При успешном выполнении команды:
  - Пароль пользователя остаётся без изменений.
  - Если для пользователя настроено шифрование данных (см. inet snmp user set key), ключ шифрования остаётся без изменений.
  - Если для пользователя выполнены настройки отправки уведомлений, 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 IG.

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, введённые символы отредактировать нельзя.
- Допустимая длина пароля — от 8 до 32 символов. Разрешённые 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 IG.

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-уведомлений 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 уведомлений запрещена (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда поддерживается в протоколе SNMPv3.

Пример использования

Чтобы разрешить отправку уведомлений 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 IG будет отправлять уведомления 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 уведомления.
- `inform` — отправлять уведомления 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 IG — 16.
- Если вы хотите задать порт, отличный от UDP 162, перед выполнением команды добавьте сетевой фильтр, разрешающий передачу SNMP-уведомлений на данный порт.

Пример использования

Чтобы SNMP-агент ViPNet Coordinator IG отправлял уведомления 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 IG отправляет уведомления 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 IG перестал отправлять уведомления 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), включить или выключить отправку SNMP-уведомлений 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-уведомлений:
  - `on` — включить.
  - `off` — выключить.

Значения по умолчанию

- Чтение SNMP-параметров запрещено (`off`).
- Отправка SNMP-уведомлений выключена (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

До выполнения команды `inet snmp v2 traps on`, которая включает отправку SNMP-уведомлений, 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 включить отправку SNMP-уведомлений:

```
hostname# inet snmp v2 traps on
Sending traps via SNMPv1 and SNMPv2c is ON
```

inet snmp v3

Разрешить или запретить чтение SNMP-параметров (OID), включить или выключить отправку SNMP-уведомлений 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-уведомлений:
  - `on` — включить.
  - `off` — выключить.

Значения по умолчанию

- Чтение SNMP-параметров запрещено (`off`).
- Отправка SNMP-уведомлений выключена (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

До выполнения команды `inet snmp v3 traps on`, которая включает отправку SNMP-уведомлений, 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 включить отправку SNMP-уведомлений:

```
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 автозаполнение и подсказка, данные для подсказки берутся из списка связей ViPNet Coordinator IG.
- 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 IG 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 пользовательский список мобильных операторов.

Синтаксис

```
inet usb-modem add provider <код страны> name <имя оператора> [apn <точка доступа>]
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи.
- `<имя оператора>` — имя оператора мобильной связи.

- `<точка доступа>` — доменное имя или IP-адрес сервера мобильного оператора (APN), через который осуществляется подключение к мобильной сети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.
- При добавлении оператора мобильной связи у модема запрашиваются коды MCC и MNC, которые затем записываются в пользовательский список мобильных операторов в качестве уникального идентификатора оператора. При дублировании кодов старая запись стирается.
- В результате выполнения команды в пользовательском списке мобильных операторов будет создана запись с заданными параметрами: код страны, имя оператора, точка доступа (если была введена лексема `apn`) и коды MCC и MNC (если вставлена SIM-карта). Все остальные параметры будут содержать пустые значения.
- Чтобы использовать добавленного оператора, необходимо выбрать его в качестве активного мобильного оператора с помощью команды `inet usb-modem select provider`.

Пример использования

Чтобы добавить оператора `tele2`:

```
hostname# inet usb-modem add provider ru name tele2
Provider 'tele2' was added successfully
```

inet usb-modem clear provider-base

Удалить все записи из пользовательского списка мобильных операторов.

Синтаксис

```
inet usb-modem clear provider-base
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.

- Команда требует подтверждение выполнения (введите `Yes` или `No`).

Пример использования

Чтобы удалить список мобильных операторов:

```
hostname# inet usb-modem clear provider-base

Are you sure you want to proceed?[Yes,No]

Yes

Provider base was cleared successfully
```

inet usb-modem delete provider

Удалить оператора из пользовательского списка мобильных операторов.

Синтаксис

```
inet usb-modem delete provider <код страны> name <имя оператора>
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи.
- `<имя оператора>` — имя оператора мобильной связи.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.
- Команда выполняется только для операторов из пользовательского списка мобильных операторов.

Пример использования

Чтобы удалить оператора мобильной связи `tele2` из пользовательского списка мобильных операторов:

```
hostname# inet usb-modem delete provider ru name tele2

provider tele2 was deleted successfully.
```

inet usb-modem dns

Разрешить или запретить обращение к DNS-серверу, информация о котором поступает от мобильного оператора по протоколу DHCP при установлении соединения.

Синтаксис

```
inet usb-modem dns {on | off}
```

Параметры и ключевые слова

- `on` — разрешить обращение к DNS-серверу.
- `off` — запретить обращение к DNS-серверу.

Значения по умолчанию

Разрешено обращение к DNS-серверу (`on`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.

Пример использования

Чтобы запретить обращение к DNS-серверу оператора связи:

```
hostname# inet usb-modem dns off
```

inet usb-modem ip-gw

Задать или удалить IP-адрес шлюза мобильного оператора. Команда используется при резервировании каналов доступа в интернет (подробнее см. в документе «Сценарии работы»).

Синтаксис

```
inet usb-modem ip-gw [<IP-адрес>]
```

Параметры и ключевые слова

`<IP-адрес>` — IP адрес шлюза мобильного оператора.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.
- Чтобы удалить заданный IP-адрес, выполните команду без параметра `<IP-адрес>`.

Пример использования

Чтобы задать IP-адрес шлюза мобильного оператора 10.64.64.64:

```
hostname# inet usb-modem ip-gw 10.64.64.64
address configured
```

Чтобы удалить заданный IP-адрес:

```
hostname# inet usb-modem ip-gw
address deleted
```

inet usb-modem mode

Включить или выключить использование модема.

Синтаксис

```
inet usb-modem mode {on | off}
```

Параметры и ключевые слова

- `on` — включить использование модема.
- `off` — выключить использование модема.

Значения по умолчанию

Использование модема выключено (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.

- В выключенном состоянии модем не будет использоваться для установления соединения, даже если он найден.

Пример использования

Чтобы включить использование модема:

```
hostname# inet usb-modem mode on
3G/4G connection is enabled
```

inet usb-modem pin

Задать или удалить PIN-код, с помощью которого ViPNet Coordinator IG получает доступ к SIM-карте.

Синтаксис

```
inet usb-modem pin [<PIN-код>] [sim <номер SIM-карты>]
```

Параметры и ключевые слова

- `<PIN-код>` — PIN-код для SIM-карты. Возможные значения — цифры, длина — от 4 до 8 цифр.
- `<номер SIM-карты>` — номер разъёма, в который установлена SIM-карта. Возможные значения: `1`, `2`. Параметр используется для исполнений ViPNet Coordinator IG, которые поддерживают 2 SIM-карты.

Значения по умолчанию

При выполнении команды без параметра `<PIN-код>` заданный PIN-код будет удалён из памяти ViPNet Coordinator IG. При этом PIN-код на SIM-карте не меняется.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Для исполнений ViPNet Coordinator IG с поддержкой двух SIM-карт параметр `sim <номер SIM-карты>` обязательный.
- Перед выполнением команды выключите модем.

Пример использования

Чтобы задать PIN-код 1234 для доступа к SIM-карте:

```
hostname# inet usb-modem pin 1234

PIN code was set.
```

inet usb-modem provider mc

Задать коды MCC и MNC мобильного оператора.

Синтаксис

```
inet usb-modem provider <код страны> name <имя оператора> mc <mcc> <mnc>
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи.
- `<имя оператора>` — имя оператора мобильной связи.
- `<mcc>` — MCC (Mobile Country Code). Состоит из трёх цифр.
- `<mnc>` — MNC (Mobile Network Code). Состоит из двух цифр.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.
- Вы можете выполнить команду только если коды MCC и MNC не были установлены ранее. Иначе, появится сообщение об ошибке.
- Команда выполняется только для операторов из пользовательского списка мобильных операторов.

Пример использования

Чтобы установить значение `909` для кода MCC и значение `234` для кода MNC мобильного оператора `tele2`:

```
hostname# inet usb-modem provider ru name tele2 mc 909 234

provider tele2 mcc & mnc was set to 909 234
```

inet usb-modem provider password

Задать пароль к точке доступа мобильного оператора.

Синтаксис

```
inet usb-modem provider <код страны> name <имя оператора> password <пароль>
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи.
- `<имя оператора>` — имя оператора мобильной связи.
- `<пароль>` — пароль к точке доступа оператора мобильной связи. При вводе можно использовать символы латинского алфавита, цифры, а также специальные символы: `- _ . @`. Длина пароля: от 1 до 32 символов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.
- Команда выполняется только для операторов из пользовательского списка мобильных операторов.

Пример использования

Чтобы задать пароль `Aa123456` для подключения к точке доступа оператора `mts`:

```
hostname# inet usb-modem provider ru name mts password Aa123456
provider mts password was set to Aa123456
```

inet usb-modem provider phone

Задать телефонный номер, используемый для соединения с мобильным оператором.

Синтаксис

```
inet usb-modem provider <код страны> name <имя оператора> phone <номер телефона>
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи.
- `<имя оператора>` — имя оператора мобильной связи.
- `<номер телефона>` — номер телефона. При вводе номера телефона вы можете использовать цифры и символы: `* #`. Длина номера: 3–10 символов.

Значения по умолчанию

Задан номер телефона: `*99***1#`

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.
- Команда выполняется только для операторов из пользовательского списка мобильных операторов.

Пример использования

Чтобы задать телефонный номер `*99***1#` для оператора мобильной связи `megafon`:

```
hostname# inet usb-modem provider ru name megafon phone *99***1#
provider megafon phone was set to *99***1#
```

inet usb-modem provider type

Задать точку доступа (APN) к сети мобильного оператора.

Синтаксис

```
inet usb-modem provider <код страны> name <имя оператора> type <точка доступа>
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи.
- `<имя оператора>` — имя оператора мобильной связи.
- `<точка доступа>` — доменное имя или IP-адрес сервера мобильного оператора (APN), через который осуществляется подключение к мобильной сети.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.
- Команда выполняется только для операторов из пользовательского списка мобильных операторов.

Пример использования

Чтобы задать точку доступа (APN) с именем `internet.mts.ru` для оператора `mts`:

```
hostname# inet usb-modem provider ru name mts type internet.mts.ru
Provider mts connection address was set to internet.mts.ru
```

inet usb-modem provider username

Задать имя пользователя, который используется для авторизации в точке доступа мобильного оператора.

Синтаксис

```
inet usb-modem provider <код страны> name <имя оператора> username <имя пользователя>
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи.
- `<имя оператора>` — имя оператора мобильной связи.
- `<имя пользователя>` — имя пользователя для точки доступа оператора мобильной связи. При вводе можно использовать символы латинского алфавита, цифры, а также следующие специальные символы: `.` `-` `_` `@`. Длина имени пользователя: от 1 до 32 символов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.

- Команда выполняется только для операторов из пользовательского списка мобильных операторов.

Пример использования

Чтобы задать имя пользователя `Ivanov` для подключения к точке доступа оператора `tele2`:

```
hostname# usb-modem provider ru name tele2 username Ivanov
provider tele2 user was set to Ivanov
```

inet usb-modem route

Разрешить или запретить использование шлюза, полученного от мобильного оператора, в маршруте по умолчанию.

Синтаксис

```
inet usb-modem route {on | off}
```

Параметры и ключевые слова

- `on` — включить использование адреса шлюза.
- `off` — выключить использование адреса шлюза.

Значения по умолчанию

Применение маршрута включено (`on`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Перед выполнением команды выключите модем.

Пример использования

Чтобы выключить применение маршрута по умолчанию:

```
hostname# inet usb-modem route off
```

inet usb-modem route-metric

Задать метрику маршруту по умолчанию, который формируется на основе IP-адреса шлюза по умолчанию, полученного от мобильного оператора по протоколу PPP.

Синтаксис

```
inet usb-modem route-metric {<метрика> | none}
```

Параметры и ключевые слова

- `<метрика>` — значение метрики. Допустимый диапазон: 1–255.
- `none` — удалить метрику.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Задание метрики возможно только при следующих условиях:
  - Выключено использование модема.
  - Разрешено применение маршрута по умолчанию от сервера провайдера при подключении через модем (см. inet usb-modem route).
- При удалении метрики будет использоваться метрика по умолчанию (см. inet dhcp client route-default-metric).

Пример использования

Чтобы для маршрутов, формируемых в процессе работы через модем, назначить метрику `100`:

```
hostname# inet usb-modem route-metric 100
Route metric for USB modem is set to 100
```

Чтобы удалить метрику:

```
hostname# inet usb-modem route-metric none
Route metric for USB modem is unset
```

inet usb-modem select provider

Выбрать мобильного оператора для подключения к мобильной сети 3G/4G.

Синтаксис

```
inet usb-modem select provider <код страны> name <имя оператора> [type <точка доступа>]
[sim <номер SIM-карты>]
```

Параметры и ключевые слова

- `<код страны>` — двухсимвольный код страны оператора мобильной связи.
- `<имя оператора>` — имя оператора мобильной связи.
- `<точка доступа>` — доменное имя или IP-адрес сервера мобильного оператора (APN), через который осуществляется подключение к мобильной сети.
- `<номер SIM-карты>` — номер разъема, в который установлена SIM-карта. Возможные значения: `1`, `2`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом.
- Лексема `sim` с параметром `<номер SIM-карты>` задаётся для исполнений ViPNet Coordinator IG, которые поддерживают 2 SIM-карты. Для таких исполнений параметр обязательный.
- Перед выполнением команды выключите модем.
- При выборе оператора из пользовательского списка мобильных операторов, он помечается как активный.
- При выборе оператора из предустановленного списка мобильных операторов, запись по выбранному оператору копируется в пользовательский список мобильных операторов. При этом коды MCC и MNC записываются:
  - полученные от модема, если они не равны 0 и отличаются от кодов из предустановленного списка мобильных операторов;
  - полученные из предустановленного списка мобильных операторов, если полученные от модема равны 0 или не отличаются от кодов в предустановленном списке.

  Оператор помечается как активный.

Пример использования

Чтобы в качестве активного оператора мобильной связи выбрать `mts`:

```
hostname# inet usb-modem select provider ru name mts

Cellular provider was set to mts [ru]
```

inet usb-modem sim

Выбрать SIM-карту, которая будет использоваться при включении модема.

Синтаксис

```
inet usb-modem sim <номер SIM-карты>
```

Параметры и ключевые слова

`<номер SIM-карты>` — номер разъема, в который установлена SIM-карта. Возможные значения: `1`, `2`.

Значения по умолчанию

Используется SIM-карта, установленная в разъем под номером 1.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда доступна только на аппаратных платформах со встроенным модемом и поддерживающих две SIM-карты.
- Перед выполнением команды выключите модем.

Пример использования

Чтобы модем использовал SIM-карту, установленную в разъем под номером 2:

```
hostname# inet usb-modem sim 2
Active SIM card successfully set.
```

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. Разрешённые символы: A–Z, a–z, 0–9, _ -. 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 IG 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 IG 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 IG, 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 IG в режиме клиента Wi-Fi.
- Задать тип защиты сети Wi-Fi — при работе ViPNet Coordinator IG 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 IG работает в режиме клиента Wi-Fi.
- `access-point` — ViPNet Coordinator IG 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 log signal

Включить или выключить запись уровня сигнала Wi-Fi в системный журнал.

Синтаксис

```
inet wifi log signal {<периодичность> | off}
```

Параметры и ключевые слова

- `<периодичность>` — интервал времени, через который уровень сигнала будет записываться в журнал (в минутах). Возможные значения: `1`, `2`, `3`, `4`, `5`, `6`, `10`, `12`, `15`, `20`, `30`.
- `off` — выключить запись уровня сигнала в журнал.

Значения по умолчанию

Запись уровня сигнала Wi-Fi в системный журнал выключена (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда доступна только в исполнениях ViPNet Coordinator IG со встроенным модулем Wi-Fi.

Пример использования

Чтобы настроить запись уровня сигнала Wi-Fi в системный журнал с периодичностью в 1 минуту:

```
hostname# inet wifi log signal 1
WiFi signal strength logging time interval has been changed to 1 min
```

Чтобы выключить запись уровня сигнала Wi-Fi в системный журнал:

```
hostname# inet wifi log signal off
wifi signal strength logging disabled
```

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 только на аппаратных платформах со встроенным модулем Wi-Fi.

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 IG 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 IG 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 ipf

Настройка фильтрации промышленных протоколов и управление службой фильтрации промышленных протоколов (далее – служба `IPF`).

ipf add rules

Создать набор правил фильтрации промышленного протокола. Каждый набор состоит из таблицы транспортного уровня и таблицы прикладного уровня.

Синтаксис

```
ipf {modbus | iec104} add rules <имя набора правил>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола. Может содержать символы латинского алфавита, цифры, а также специальные символы: `_ . -`. Максимальная длина — 128 символов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По команде будет создан пустой набор правил. Чтобы добавить правила фильтрации транспортного уровня см. команду ipf rules fw add. Чтобы добавить правила фильтрации прикладного уровня см. команду ipf rules rule add.
- Наборы правил создаются во включенном состоянии. Чтобы выключить или включить набор правил см. команды ipf rules disable и ipf rules enable.
- Невозможно создать два и более набора правил, в которых таблицы правил транспортного и прикладного уровней полностью совпадают, даже если эти наборы имеют разные имена. Например, нельзя создать два пустых набора правил.

Пример использования

Чтобы создать набор правил фильтрации Modbus с именем `Controllers_01`:

```
hostname# ipf modbus add rules Controllers_01
```

ipf change name rules

Переименовать набор правил фильтрации промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} change name rules <текущее имя набора правил> <новое имя набора правил>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<текущее имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<новое имя набора правил>` — имя, которое вы хотите присвоить набору правил фильтрации промышленного протокола. Может содержать символы латинского алфавита, цифры, а также специальные символы: `_ . -`. Максимальная длина — 128 символов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.
- Если новое имя уже принадлежит одному из наборов правил промышленного протокола, команда не будет выполнена.

Пример использования

Чтобы присвоить набору правил Modbus с именем `Modbus_rules_01` новое имя `Temp_sensors`:

```
hostname# ipf modbus change name rules Modbus_rules_01 Temp_sensors
```

ipf delete rules

Удалить набор правил фильтрации промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} delete rules <имя набора правил>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.
- При удалении набора правил, удаляются все правила фильтрации транспортного и прикладного уровней, содержащиеся в наборе правил.

Пример использования

Чтобы удалить набор правил Modbus с именем `RuleSet_01`:

```
hostname# ipf modbus delete rules RuleSet_01
Are you sure to delete rules table "RuleSet_01"? [Yes,No]: y
RuleSet_01 removed.
```

ipf iec104 rules iecformat set asdu

Задать размер поля, содержащего общий адрес ASDU, для фильтрации протокола МЭК 60870-5-104.

Синтаксис

```
ipf iec104 rules <имя набора правил> iecformat set asdu <размер>
```

Параметры и ключевые слова

- `<имя набора правил>` — имя набора правил фильтрации МЭК 60870-5-104.
- `<размер>` — размер поля, содержащего общий адрес ASDU, в байтах. Возможные значения: `1`, `2`.

Значения по умолчанию

Размер поля, содержащего общий адрес ASDU, — 2 байта (`2`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда изменяет формат протокола МЭК 60870-5-104 для выбранного набора правил.
- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.
- При уменьшении размера поля, содержащего общий адрес ASDU (размер поля влияет на диапазон адресов), производится проверка правил фильтрации в выбранном наборе правил МЭК 60870-5-104. Если в правилах встречаются значения, не входящие в изменяемый диапазон, команда не выполняется.

Пример использования

Чтобы задать размер поля, содержащего общий адрес ASDU, в 1 байт для набора правил с именем `For_rdu`:

```
hostname# ipf iec104 rules For_rdu iecformat set asdu 1
```

ipf iec104 rules iecformat set cot

Задать размер поля, содержащего причину передачи ASDU, для фильтрации протокола МЭК 60870-5-104.

Синтаксис

```
ipf iec104 rules <имя набора правил> iecformat set cot <размер>
```

Параметры и ключевые слова

- `<имя набора правил>` — имя набора правил фильтрации МЭК 60870-5-104.
- `<размер>` — размер поля, содержащего причину передачи ASDU, в байтах. Возможные значения: `1`, `2`.

Значения по умолчанию

Размер поля, содержащего причину передачи, — 2 байта (содержит адрес источника) (`2`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда изменяет формат протокола МЭК 60870-5-104 для выбранного набора правил.
- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы задать размер поля, содержащего причину передачи ASDU, в 1 байт для набора правил с именем `For_rdu`:

```
hostname# ipf iec104 rules For_rdu iecformat set cot 1
```

ipf iec104 rules iecformat set default

Сбросить настройки формата протокола МЭК 60870-5-104 на значения по умолчанию.

Синтаксис

```
ipf iec104 rules <имя набора правил> iecformat set default
```

Параметры и ключевые слова

`<имя набора правил>` — имя набора правил фильтрации МЭК 60870-5-104.

Значения по умолчанию

По команде устанавливаются следующие значения для заданного набора правил:

- Размер поля, содержащего общий адрес ASDU: 2 байта;
- Размер поля, содержащего адрес объекта информации: 3 байта;
- Размер поля, содержащего причину передачи ASDU: 2 байта;
- Максимальный размер APDU: 253 байта.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда изменяет формат протокола МЭК 60870-5-104 для выбранного набора правил.
- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы сбросить все настройки формата протокола МЭК 60870-5-104 на значения по умолчанию для набора правил с именем `For_rdu`:

```
hostname# ipf iec104 rules For_rdu iecformat set default
```

ipf iec104 rules iecformat set ioaddress

Задать размер поля, содержащего адрес объекта информации, для фильтрации протокола МЭК 60870-5-104.

Синтаксис

```
ipf iec104 rules <имя набора правил> iecformat set ioaddress <размер>
```

Параметры и ключевые слова

- `<имя набора правил>` — имя набора правил фильтрации МЭК 60870-5-104.
- `<размер>` — размер поля, содержащего адрес объекта информации, в байтах. Возможные значения: `1`, `2`, `3`.

Значения по умолчанию

Размер поля, содержащего адрес объекта информации, — 3 байта (`3`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда изменяет формат протокола МЭК 60870-5-104 для выбранного набора правил.
- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.
- При уменьшении размера поля, содержащего адрес объекта информации (размер поля влияет на диапазон адресов), производится проверка правил фильтрации в выбранном наборе правил МЭК 60870-5-104. Если в правилах встречаются значения, не входящие в изменяемый диапазон, команда не выполняется.

Пример использования

Чтобы задать размер поля, содержащего адрес объекта информации, в 2 байта для набора правил с именем `For_rdu`:

```
hostname# ipf iec104 rules For_rdu iecformat set ioaddress 2
```

ipf iec104 rules iecformat set max_length_apdu

Задать максимальный размер APDU для фильтрации протокола МЭК 60870-5-104.

Синтаксис

```
ipf iec104 rules <имя набора правил> iecformat set max_length_apdu <число>
```

Параметры и ключевые слова

- `<имя набора правил>` — имя набора правил фильтрации МЭК 60870-5-104.
- `<число>` — максимальный размер APDU в байтах. Возможные значения: число, входящее в диапазон 2-253 включительно.

Значения по умолчанию

Задан максимальный размер APDU — 253 байта (`253`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда изменяет формат протокола МЭК 60870-5-104 для выбранного набора правил.
- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы задать максимальный размер APDU в 4 байта для набора правил с именем `For_rdu`:

```
hostname# ipf iec104 rules For_rdu iecformat set max_length_apdu 4
```

ipf mode

Включить или выключить фильтрацию промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} mode {on | off}
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.

- `iec104` — протокол МЭК 60870-5-104.
- `on` — включить фильтрацию.
- `off` — выключить фильтрацию.

Значения по умолчанию

Фильтрация выключена (`off`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы включить фильтрацию протокола Modbus:

```
hostname# ipf modbus mode on
Modbus mode is on
Attention: All sets of rules with modbus are working.
```

ipf rules disable

Выключить набор правил фильтрации промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> disable
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы выключить набор правил фильтрации протокола Modbus с именем `Controllers_02`:

```
hostname# ipf modbus rules Controllers_02 disable
```

ipf rules enable

Включить набор правил фильтрации промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> enable
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы включить набор правил фильтрации протокола Modbus с именем `Controllers_02`:

```
hostname# ipf modbus rules Controllers_02 enable
```

ipf rules fw add

Создать правило фильтрации транспортного уровня в наборе правил промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> fw add [<номер правила>] table <тип> [client
<адрес клиента>] [server <адрес сервера>] [<протокол>] port <порт>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице транспортного уровня.
- `<тип>` — тип трафика, для фильтрации которого предназначено правило:
  - `local` — локальный трафик открытой сети;
  - `forward` — транзитный трафик открытой сети;
  - `tunnel` — туннелируемый трафик;
  - `vpn` — защищенный трафик.
- `<адрес клиента>` — адрес узла, который запрашивает TCP-соединение:
  - Для локального, транзитного и туннелируемого трафика — IP-адрес или доменное имя.
  - Для защищенного трафика (`vpn`) — идентификатор узла или сети ViPNet.
- `<адрес сервера>` — адрес узла, который ожидает TCP-соединение:
  - Для локального, транзитного и туннелируемого трафика — IP-адрес или доменное имя.
  - Для защищенного трафика (`vpn`) — идентификатор узла или сети ViPNet.
- `<протокол>` — транспортный протокол, по которому передаются IP-пакеты. Доступен только протокол TCP.
- `<порт>` — порт назначения IP-пакетов.

Значения по умолчанию

- Если номер правила не задан, ему присваивается последний номер в таблице транспортного уровня.
- Если адрес клиента не задан, используется значение «любой» (`@any`).
- Если адрес сервера не задан, используется значение «любой» (`@any`).
- Если транспортный протокол не задан, используется протокол TCP (`tcp`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил. Если не создано ни одного набора правил, создайте его с помощью команды ipf add rules.

- В качестве адреса клиента или сервера для локального, транзитного и туннелируемого трафика вы можете указать несколько значений: диапазон IP-адресов, список IP-адресов и доменных имен, маску адресов подсети, системную группу объектов `any`, `local` или `remote`, одну или несколько пользовательских групп IP-адресов.
- В качестве адреса клиента или сервера для защищенного трафика (`vpn`) вы можете указать несколько значений: список идентификаторов узлов или сетей ViPNet, системные группы объектов `any`, `allcoordinators`, `allclients`, `local` или `remote`.
- Защищенный трафик может быть только локальным, поэтому в качестве адреса клиента или адреса сервера укажите группу `local`.
- Вы можете задать несколько портов или диапазонов портов назначения через запятую (например, `port 443, 4444-4445`). Не указывайте порты, которые используются другими службами (используемые порты вы можете посмотреть в сетевых фильтрах с помощью команды `firewall <тип> show`).

Пример использования

Чтобы создать в наборе правил Modbus с именем `Controllers_02` правило фильтрации транзитного открытого трафика со следующими значениями параметров: адрес клиента 192.168.0.1, адрес сервера 89.135.15.2, протокол TCP, порт назначения 502:

```
hostname# ipf modbus rules Controllers_02 fw add table forward client 192.168.0.1 server 89.135.15.2 tcp port 502
```

ipf rules fw append

Добавить новые значения параметров в правило фильтрации транспортного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> fw append <номер правила> [client <адрес клиента>] [server <адрес сервера>] [port <порт>]
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице транспортного уровня.
- `<адрес клиента>` — адрес узла, который запрашивает TCP-соединение:
  - Для локального, транзитного и туннелируемого трафика — IP-адрес или доменное имя.
  - Для защищенного трафика (`vpn`) — идентификатор узла или сети ViPNet.

- `<адрес сервера>` — адрес узла, который ожидает TCP-соединение:
  - Для локального, транзитного и туннелируемого трафика — IP-адрес или доменное имя.
  - Для защищенного трафика (`vpn`) — идентификатор узла или сети ViPNet.
- `<протокол>` — транспортный протокол, по которому передаются IP-пакеты. Доступен только протокол TCP.
- `<порт>` — порт назначения IP-пакетов.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.
- Список возможных значений адреса клиента, адреса сервера, протокола и порта — тот же, что при создании правила фильтрации с помощью команды ipf rules fw add.

Пример использования

Чтобы добавить в правило фильтрации с порядковым номером 2, содержащееся в наборе правил МЭК 60870-5-104 с именем `For_rdu`, новый адрес клиента 192.168.0.11:

```
hostname# ipf iec104 rules For_rdu fw append 2 client 192.168.0.11
```

ipf rules fw change

Заменить правило фильтрации транспортного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> fw change <номер правила> table <тип> [client <адрес клиента>] [server <адрес сервера>] [<протокол>] port <порт>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице транспортного уровня.
- `<тип>` — тип трафика, для фильтрации которого предназначено правило:
  - `local` — локальный трафик открытой сети;

    - `forward` — транзитный трафик открытой сети;
    - `tunnel` — туннелируемый трафик;
    - `vpn` — защищенный трафик.
- `<адрес клиента>` — адрес узла, который запрашивает TCP-соединение:
    - Для локального, транзитного и туннелируемого трафика — IP-адрес или доменное имя.
    - Для защищенного трафика (`vpn`) — идентификатор узла или сети ViPNet.
- `<адрес сервера>` — адрес узла, который ожидает TCP-соединение:
    - Для локального, транзитного и туннелируемого трафика — IP-адрес или доменное имя.
    - Для защищенного трафика (`vpn`) — идентификатор узла или сети ViPNet.
- `<протокол>` — транспортный протокол, по которому передаются IP-пакеты. Доступен только протокол TCP.
- `<порт>` — порт назначения IP-пакетов.

Значения по умолчанию

- Если адрес клиента не задан, используется значение «любой» (`@any`).
- Если адрес сервера не задан, используется значение «любой» (`@any`).
- Если транспортный протокол не задан, используется протокол TCP (`tcp`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.
- Список возможных значений адреса клиента, адреса сервера, протокола и порта — тот же, что при создании правила фильтрации с помощью команды ipf rules fw add.

Пример использования

Чтобы заменить правило фильтрации с порядковым номером 2, содержащееся в наборе правил МЭК 60870-5-104 с именем `For_rdu`, на новое правило со следующими параметрами: адрес клиента 192.168.0.10, адрес сервера 89.135.15.4, порт назначения 503, выполните команду:

```
hostname# ipf iec104 rules For_rdu fw change 2 table forward client 192.168.0.10 server
89.135.15.4 tcp port 503
```

ipf rules fw delete

Удалить правило фильтрации транспортного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> fw delete <номер правила>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице транспортного уровня.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При удалении правила транспортного уровня, правила прикладного уровня не удаляются.
- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы удалить правило фильтрации с порядковым номером 2, содержащееся в наборе правил МЭК 60870-5-104 с именем `For_rdu`:

```
hostname# ipf iec104 rules For_rdu fw delete 2
```

ipf rules rule add

Создать правило фильтрации прикладного уровня в наборе правил промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> rule add [<номер правила>] [name <имя правила>] <параметры прикладного протокола> {pass | drop}
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.

- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице прикладного уровня, определяющий приоритет правила.
- `<имя правила>` — имя правила фильтрации.
- `pass` — пропускать трафик.
- `drop` — блокировать трафик.
- `<параметры прикладного протокола>` — параметры промышленного протокола, по которым выполняется фильтрация трафика на прикладном уровне:
  - для протокола Modbus:

    ```
    id <идентификаторы узлов> fc <коды функций> [r <диапазоны регистров чтения>] [w <диапазоны регистров записи>]
    ```

    Параметры:

    - `<идентификаторы узлов>` — идентификаторы Modbus-устройств. Допустимые значения: числа, диапазоны чисел, входящие в интервал 0–255.
    - `<коды функций>` — коды функций в командах Modbus. Допустимые значения: числа, диапазоны чисел, входящие в интервал 1–127.

    Примечание. При задании диапазонов следует учитывать: если в команде заданы регистры чтения или записи, то диапазон должен содержать только те коды функций, которые работают с указанными регистрами.

    - `<диапазоны регистров чтения>` — номера регистров чтения. Допустимые значения: числа, диапазоны чисел, входящие в интервал 0–65535.
    - `<диапазоны регистров записи>` — номера регистров записи. Допустимые значения: числа, диапазоны чисел, входящие в интервал 0–65535.
  - для протокола МЭК 60870-5-104:

    ```
    [asdu <общий адрес ASDU>] [ioa <адреса объектов информации>] [iot <идентификаторы типов объектов информации>]
    ```

    Параметры:

    - `<общий адрес ASDU>` — общие адреса станций ASDU. Допустимые значения: числа, диапазоны чисел, входящие в интервал:
      - 1–255 — при размере поля в 1 байт;
      - 1–65535 — при размере поля в 2 байта.

      Размер поля, содержащего общий адрес ASDU, задается командой ipf iec104 rules iecformat set asdu.
    - `<адреса объектов информации>` — адреса (идентификаторы) объектов информации. Допустимые значения: числа, диапазоны чисел, входящие в интервал:

- 0–255 — при размере поля в 1 байт;
- 0–65535 — при размере поля в 2 байта;
- 0–16777215 — при размере поля в 3 байта.

Размер поля, содержащего адрес объектов информации, задается командой ipf iec104 rules iecformat set ioaddress.



Примечание. Для фильтрации пакетов со структурированным адресом объекта информации необходимо приводить адрес к неструктурированному виду (десятичному числу).

- `<идентификаторы типов объектов информации>` — идентификаторы типов объектов информации. Допустимые значения: числа, диапазоны чисел, входящие в интервал 1–127.

Значения по умолчанию

- Если номер правила не задан, ему присваивается последний номер в таблице прикладного уровня.
- Если для протокола Modbus диапазон регистров чтения или записи не задан, используется весь диапазон (`@any`).
- Если любой из параметров протокола МЭК 60870-5-104 не задан, используется весь диапазон (`@any`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил. Если не создано ни одного набора правил, создайте его с помощью команды ipf add rules.
- Если номер правила меньше последнего номера в таблице, нумерация правил фильтрации, следующих за новым правилом, будет автоматически изменена (их номера будут увеличены на 1).

Пример использования

Чтобы создать в наборе правил `Controllers_02` правило фильтрации, разрешающее прохождение команд Modbus с кодами функций 1, 3 и 4, запрашивающих чтение регистров с номерами 30–50 от устройств с идентификаторами 2 и 6:

```
hostname# ipf modbus rules Controllers_02 rule add id 2,6 fc 1,3-4 r 30-50 pass
```

Чтобы создать в наборе правил `IECRuleSet1` правило фильтрации, разрешающее прохождение блоков данных со следующими параметрами протокола МЭК 60870-5-104: общие адреса ASDU 1, 3 и 4, адреса объектов информации в диапазоне 10000–15000, идентификатор типов объектов 36:

```
hostname# ipf iec104 rules IECRuleSet1 rule add asdu 1,3-4 ioa 10000-15000 iot 36 pass
```

ipf rules rule append

Добавить новые значения параметров в правило фильтрации прикладного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> rule append <номер правила> [<параметры прикладного протокола>]
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице прикладного уровня.
- `<параметры прикладного протокола>` — параметры промышленного протокола, по которым выполняется фильтрация трафика на прикладном уровне (см. ipf rules rule add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы добавить в правило фильтрации с порядковым номером 2, содержащееся в наборе правил МЭК 60870-5-104 с именем `For_rdu`, следующие значения параметров: общий адрес ASDU 1 и адреса объектов информации в диапазоне 15000-16000:

```
hostname# ipf iec104 rules For_rdu rule append 2 asdu 1 ioa 15000-16000
```

ipf rules rule change

Заменить правило фильтрации прикладного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> rule change <номер правила> [name <новое имя правила>] <параметры прикладного протокола> {pass | drop}
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице прикладного уровня.
- `<новое имя правила>` — имя, которое вы хотите присвоить правилу фильтрации.
- `<параметры прикладного протокола>` — параметры промышленного протокола, по которым выполняется фильтрация трафика на прикладном уровне (см. ipf rules rule add).
- `pass` — пропускать трафик.
- `drop` — блокировать трафик.

Значения по умолчанию

- Если для протокола Modbus диапазон регистров чтения или записи не задан, используется весь диапазон (`@any`).
- Если любой из параметров протокола МЭК 60870-5-104 не задан, используется весь диапазон (`@any`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы заменить правило фильтрации с номером 2, содержащееся в наборе правил Modbus с именем `Controllers_02`, и задать в нем следующие параметры: имя `NewRule`, идентификаторы устройств 1, 2, 5, коды функций 2–6, действие «пропустить»:

```
hostname# ipf modbus rules Controllers_02 rule change 2 name NewRule id 1,2,5 fc 2-6 pass
```

ipf rules rule delete

Удалить правило фильтрации прикладного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> rule delete <номер правила>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице прикладного уровня.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы удалить правило фильтрации прикладного уровня с порядковым номером 2 в наборе правил МЭК 60870-5-104 с именем `For_rdu`:

```
hostname# ipf iec104 rules For_rdu rule delete 2
```

ipf rules rule disable

Выключить правило фильтрации прикладного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> rule disable <номер правила>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.

- `<номер правила>` — порядковый номер правила фильтрации в таблице прикладного уровня.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы выключить правило фильтрации Modbus с номером 5, содержащееся в наборе правил `Controllers_02`:

```
hostname# ipf modbus rules Controllers_02 rule disable 5
```

ipf rules rule enable

Включить правило фильтрации прикладного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> rule enable <номер правила>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице прикладного уровня.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы включить правило фильтрации Modbus с номером 5, содержащееся в наборе правил `Controllers_02`:

```
hostname# ipf modbus rules Controllers_02 rule enable 5
```

ipf rules rule move

Изменить приоритет правила фильтрации прикладного уровня промышленного протокола.

Синтаксис

```
ipf {modbus | iec104} rules <имя набора правил> rule move <номер правила> to <новый номер правила>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.
- `<номер правила>` — порядковый номер правила фильтрации в таблице прикладного уровня.
- `<новый номер правила>` — порядковый номер, который вы хотите присвоить правилу фильтрации в таблице прикладного уровня.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если новый номер правила выходит за количество правил в таблице прикладного уровня, правилу задается порядковый номер, следующий за последним.
- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы переместить правило фильтрации с порядковым номером 2 на позицию 1 в таблице прикладного уровня, содержащейся в наборе правил Modbus `Controllers_02`:

```
hostname# ipf modbus rules Controllers_02 rule move 2 to 1
```

ipf set journal maxsize

Задать максимальный размер журнала пакетов промышленных протоколов.

Синтаксис

```
ipf set journal maxsize <размер>
```

Параметры и ключевые слова

`<размер>` — максимальный размер журнала пакетов промышленных протоколов, в Мбайтах. Возможные значения: 0–20.

Значения по умолчанию

Задан максимальный размер журнала 10 Мбайт (`10`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Значение `0` выключает ведение журнала. При этом, если до выключения журнала в нем были записи, просмотреть их будет невозможно.

Пример использования

```
hostname# ipf set journal maxsize 20
maxsize: 20
```

ipf set journal registerall

Включить или выключить регистрацию пропущенных пакетов в журнале пакетов промышленных протоколов.

Синтаксис

```
ipf set journal registerall {on | off}
```

Параметры и ключевые слова

- `<on>` — включить регистрацию пропущенных пакетов (регистрируются как пропущенные, так и заблокированные пакеты).

- `<off>` — выключить регистрацию пропущенных пакетов (регистрируются только заблокированные пакеты).

Значения по умолчанию

Регистрируются только заблокированные пакеты (`off`).

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# ipf set journal registerall on
registerall: on
```

ipf set syslog-level

Задать уровень важности событий службы `IPF`, записываемых в системный журнал.

Синтаксис

```
ipf set syslog-level <уровень важности>
```

Параметры и ключевые слова

`<уровень важности>` — уровень важности событий службы `IPF`, 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.

Значения по умолчанию

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

Режимы командного интерпретатора

Режим настройки.

Пример использования

Чтобы записывать в системный журнал события службы `IPF` не выше 4-го уровня:

```
hostname# ipf set syslog-level 4

ipf system log level successfully set.
```

ipf show

Просмотреть конфигурацию службы `IPF`, а также всех наборов правил фильтрации промышленного протокола.

Синтаксис

```
ipf show [{modbus | iec104}]
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.

Значения по умолчанию

Если промышленный протокол не указан, отображаются наборы правил всех поддерживаемых промышленных протоколов.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Столбец `T` в таблице вывода команды означает тип фильтруемого трафика:
  - `L` — локальный трафик открытой сети (local);
  - `F` — транзитный трафик открытой сети (forward);
  - `T` — туннелируемый трафик (tunnel);
  - `V` — защищенный трафик (vpn).
- Столбец `U` в выводе команды отображает статус правила фильтрации:
  - `+` — включено;
  - `-` — выключено.

Пример использования

Чтобы просмотреть информацию о конфигурации службы `IPF`:

```
hostname> ipf show
service is enabled

system log level: 3
journal max size: 10 MBytes
register all packages: off

modbus mode on
rules set name: Controllers_02              status: enabled
rules set name: Controllers_03              status: enabled
rules set name: Controllers_04              status: enabled

iec104 mode off
rules set name: For_rdu_02              status: enabled
rules set name: For_rdu_03              status: enabled
```

Чтобы просмотреть все наборы правил фильтрации протокола Modbus:

```
hostname> ipf show modbus
T - firewall table: L - local T - tunnel V - vpn F - forward
U - rule status: "+" - enabled "-" - disabled

rules set name: Controllers_02              Status: enabled
Fw rules
Current Rules Set Id: 6
```

Num	T	Protocol	Port	Client	Server
1	L	TCP	502, 503, 1000-2000	192.168.10.20	192.168.30.50

```
App rules
Current Rules Set Id: 6
```

Num	U	Name	ID	FC	Registers	Act

1	+	read01	1, 25-30	36, 30	R: 15, 124 W: 15, 124	pass
2	+	read02	2, 10-12	5-7, 8	R: 15, 124	pass

rules set name: Controllers_03 Status: enabled

Fw rules

Current Rules Set Id: 7

Num	T	Protocol	Port	Client	Server
1	L	TCP	502, 503, 1000-2000	192.168.10.20	192.168.30.50

App rules

Current Rules Set Id: 7

Num	U	Name	ID	FC	Registers	Act
1	+	read01	1, 25-30	36, 30	R: 15, 124 W: 15, 124	pass
2	+	read02	2, 10-12	5-7, 8	R: 15, 124	pass

ipf show iec104 rules iecformat

Просмотреть настройки формата МЭК 60870-5-104 в наборе правил фильтрации.

Синтаксис

```
ipf show iec104 rules <имя набора правил> iecformat
```

Параметры и ключевые слова

`<имя набора правил>` — имя набора правил фильтрации МЭК 60870-5-104.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.

Пример использования

Чтобы просмотреть настройки формата протокола МЭК 60870-5-104 для набора правил с именем `For_rdu`:

```
hostname> ipf show iec104 rules For_rdu iecformat
```

Options	Value	Units
asdu	2	<byte>
address	3	<byte>
cause of transmition	2	<byte>
max length apdu	253	<byte>

ipf show rules

Просмотреть набор правил фильтрации промышленного протокола.

Синтаксис

```
ipf show {modbus | iec104} rules <имя набора правил>
```

Параметры и ключевые слова

- `modbus` — протокол Modbus.
- `iec104` — протокол МЭК 60870-5-104.
- `<имя набора правил>` — имя набора правил фильтрации промышленного протокола.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введенного имени из списка существующих наборов правил.
- Столбец `T` в таблице вывода команды означает тип фильтруемого трафика:
  - `L` — локальный трафик открытой сети (local);
  - `F` — транзитный трафик открытой сети (forward);
  - `T` — туннелируемый трафик (tunnel);
  - `V` — защищенный трафик (vpn).

- Столбец `U` в выводе команды отображает статус правила фильтрации:
  - `+` — включено;
  - `-` — выключено.

Пример использования

Чтобы просмотреть набор правил фильтрации протокола МЭК 60870-5-104 с именем `For_rdu`:

```
hostname> ipf show iec104 rules For_rdu
T - firewall table: L - local T - tunnel V - vpn F - forward
U - rule status: "+" - enabled "-" - disabled


rules set name: For_rdu               Status: enabled
Fw rules
Current Rules Set Id: 6
```

Num	T	Protocol	Port	Client	Server
1	L	TCP	2404, 2407, 2509, 2609, 2709-2809	192.168.10.20-192.168.10.80	89.175.26.1-89.175.26.2
2	L	TCP	2405	192.168.10.90-192.168.10.95 89.175.26.1-89.175.26.2	89.175.26.10

```
App rules
Current Rules Set Id: 6
```

Num	U	Name	ASDU	IOA	IOT	Act
1	+	Analog_Discr	1, 25-30	1-10000	36, 30	pass
2	+	Comm_closed	1, 25-30		45	drop

ipf show stat

Просмотреть статистику службы `IPF`.

Синтаксис

```
ipf show stat
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> ipf show stat

quantity packets received: 252

total:

       packets passed: 204

       packets dropped: 46

       packets anomaly: 2

       active connection opening: 1

       connection resets received: 0

       connections established: 3


Modbus:

    packets passed: 204

    packets dropped: 46

    packets anomaly: 2

    active connection opening: 1

    connection resets received: 0

    connections established: 3


iec104:

    packets passed: 0

    packets dropped: 0

    packets anomaly: 0

    active connection opening: 0

    connection resets received: 0

    connections established: 0
```

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;
  - `pppoe` — группа интерфейсов для подключения к сети провайдера по PPPoE;
  - `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 IG.
- `<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 IG другими координаторами 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.

Особенности использования

Обнаружить ViPNet Coordinator IG в качестве шлюза по умолчанию могут:

- ViPNet Coordinator HW версии 5.3.0 и выше;
- ViPNet Coordinator IG версии 5.2.0 и выше.

Пример использования

```
hostname# iplir option be-default-gateway on
```

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 IG к VPN-сети.

Синтаксис

```
iplir option mode {dynamic <id_узла> [always-use-server] | static | auto}
```

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;
- `auto` — в соответствии с настройкой, заданной в ViPNet Prime.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Порт режима со статической трансляцией адресов по умолчанию — 55777.

Пример использования

```
hostname# iplir option mode dynamic 0x034A234D
```

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 IG, другими защищёнными 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 IG 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 IG — 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 server-ping-timeout

Задать период опроса состояния других координаторов со стороны ViPNet Coordinator IG.

Синтаксис

```
iplir option server-ping-timeout <период>
```

Параметры и ключевые слова

`<период>` — период опроса, секунды; число из диапазона 1–20000.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Значение по умолчанию — 900 секунд (15 минут).
- Если от какого-либо координатора, который должен обмениваться пакетами с ViPNet Coordinator IG, не было получено служебных пакетов в течение периода опроса, то такому координатору направляется специальный пакет, на который должен прийти ответ. Если ответ не приходит, то узел координатора считается недоступным.

Пример использования

```
hostname# iplir option server-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 (connection server – <ViPNet ID>)` — с динамической трансляцией адресов;
  - `static` — со статической трансляцией адресов;
- `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:
  - `off` — ведение системного журнала отключено;
  - `critical` — критические ошибки;
  - `error` — ошибки;
  - `warning` — предупреждения;
  - `info` — информационные;
  - `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;
- `Connection keepalive timeout` — период отправки IP-пакетов серверу соединений для поддержания активного соединения с ним и пропуска входящего трафика через межсетевой экран, секунды;

- `Sync time` — автоматическая синхронизация времени с сервером IP-адресов:
  - `on` — включена;
  - `off` — выключена;
- `Tunnel local networks` — режим туннелирования IP-адресов узлов, входящих в локальную подсеть ViPNet Coordinator IG:
  - `on` — обращаться к туннелируемым узлам через ViPNet Coordinator IG;
  - `off` — обращаться к туннелируемым узлам напрямую, минуя ViPNet Coordinator IG;
- `Allow being default gateway` — обнаружение ViPNet Coordinator IG другими координаторами 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

   Full iplir6 support: No

   Addresses:

      192.168.100.100

   Syslog level: info

   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: 255
```

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 off
```

iplir option syslog-level

Изменить 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.

Значения по умолчанию

Задан уровень важности `3`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Регистрируются события заданного уровня важности и более важные. Например, если задать уровень 2, то в системном журнале будут регистрироваться события с уровнями 0, 1 и 2.

Пример использования

```
hostname# iplir option syslog-level 2
```

iplir option udp-ports-count

Задать количество портов UDP.

Синтаксис

```
iplir option udp-ports-count <количество портов>
```

Параметры и ключевые слова

`<количество портов>` — количество портов UDP; 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 автозаполнение и подсказка, данные для подсказки берутся из списка связей ViPNet Coordinator IG с другими узлами.
- Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Чтобы проверить связь ViPNet Coordinator IG 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 подключён 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 IG.

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.

Значения по умолчанию

L2OverIP выключен (`none`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Невозможно включить L2OverIP в следующих случаях:

- ViPNet Coordinator IG входит в состав кластера и в момент выполнения команды находится в пассивном режиме.
- Заданы не все параметры, необходимые для работы L2OverIP.

Пример использования

Чтобы включить L2OverIP:

```
hostname# iplir set l2overip mode switch
```

iplir set l2overip remote-port

Добавить параметры удалённого сегмента сети в настройках L2OverIP.

Синтаксис

```
iplir set l2overip remote-port <порт> <IP-адрес>
```

Параметры и ключевые слова

- `<порт>` — номер порта удалённого сегмента.
- `<IP-адрес>` — актуальный IP-адрес видимости ViPNet Coordinator IG, к которому подключён удалённый сегмент сети (реальный или виртуальный адрес удалённого ViPNet Coordinator IG).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Указанный номер удалённого порта должен быть отличен от номера локального порта.
- Можно добавить не более 31 удалённого порта, так как число объединяемых сегментов сети не может быть больше 32.

- Можно указать номер порта, который уже был добавлен. В этом случае будет обновлён IP-адрес удалённого сегмента.

Пример использования

Чтобы добавить удалённый 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 удалённые порты и на порт с номером 0;
  - кадры, принятые от удалённого порта, пересылать на локальный порт и на порт с номером 0;
  - кадры, принятые от порта с номером 0, пересылать на все удалённые 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 add

Добавить IP-адрес доступа к координатору.

Синтаксис

```
iplir node <id_узла> access-point add <IP-адрес> [port <порт>] [metric <метрика>]
```

Параметры и ключевые слова

- `<id_узла>` — идентификатор сетевого узла координатора;
- `<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.

Значения по умолчанию

Если необязательные параметры не указаны, задаются значения:

- `<порт>` — 55777;
- `<метрика>` — назначается автоматически.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# iplir node 0x50248525 access-point add 13.1.0.24 port 55888 metric 5
```

iplir node access-point delete

Удалить IP-адрес доступа к координатору.

Синтаксис

```
iplir node <id_узла> access-point delete <IP-адрес>
```

Параметры и ключевые слова

- `<id_узла>` — идентификатор сетевого узла координатора;
- `<IP-адрес>` — IP-адрес доступа.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# iplir node 0x50248525 access-point delete 13.1.0.24
```

iplir node blockforward

Включить или выключить блокирование транзитных IP-пакетов, передаваемых через ViPNet Coordinator IG 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 связанного узла пропускаются.

Пример использования

```
hostname# iplir node 0x383d0002 blockforward on
```

iplir node add domain-name

Добавить доменное имя узла ViPNet.

Синтаксис

```
iplir node <id_узла> add domain-name <доменное имя>
```

Параметры и ключевые слова

- `<id_узла>` — идентификатор узла ViPNet;
- `<доменное имя>` — доменное имя.

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 delete domain-name

Удалить доменное имя узла ViPNet.

Синтаксис

```
iplir node <id_узла> delete domain-name {<доменное имя> | all}
```

Параметры и ключевые слова

- `<id_узла>` — идентификатор узла ViPNet;
- `<доменное имя>` — доменное имя;
- `<all>` — удалить все доменные имена узла ViPNet.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# iplir node 0x383d0002 delete domain-name all
```

iplir node list

Просмотреть сведения об узлах ViPNet, связанных с ViPNet Coordinator IG.

Синтаксис

```
iplir node list [{clients | gateways}] [filter <фильтр>]
```

Параметры и ключевые слова

- тип связанного узла:
  - `clients` — клиенты;
  - `gateways` — координаторы.
- `<фильтр>` — строка текста, состоящая из идентификатора узла или сети, имени или части имени узла; может содержать до 50 символов: `A–z`, `0–9`, `. , () ! № - = _ @ ; .`

Значения по умолчанию

Отображается список всех узлов, связанных с ViPNet Coordinator IG, и сведения о них.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Список связанных узлов содержит:
  - `Node id` — идентификатор узла;
  - `Type` — тип узла:
    - `CL` — клиент;
    - `GW` — координаторы;
  - `Node name` — имя узла;
  - `Fil6s (Full iplir6 support)` — полная поддержка iplir версии 6.1:
    - `Yes` — есть;
    - `No` — нет;
  - `Networks` — номера сетей ViPNet, для которых ViPNet Coordinator IG — 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 filter 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 узла ViPNet.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются:

- `Node name` — имя узла;
- `Type` — тип узла:
  - `Client` — клиент;
  - `Gateway` — координатор;
- `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 IG);
- `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 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 IG. 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 IG.

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 просмотра.
- 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;
  - `pppoe` — группа интерфейсов для подключения к сети провайдера по PPPoE;

- `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 <ViPNet ID>}]
```

Параметры и ключевые слова

- `<warning>` — отображать сведения о ключах обмена, для которых:
  - срок действия ключа истёк;
  - 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 ViPNet-узлом;
- `<ViPNet ID>` — идентификатор связанного узла.

Значения по умолчанию

При выполнении команды без параметров отображаются сведения обо всех ключах обмена, в том числе срок действия которых истёк или скоро истечёт.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Отображаются следующие сведения о ключах обмена:

- `Peer` — идентификатор связанного ViPNet-узла;
- `Variant` — номер варианта ключей связанного узла;
- `StartDate` — дата начала срока действия ключа;
- `ExpiryDate` — дата окончания срока действия ключа;
- `KeyID` — идентификатор ключа в ViPNet Prime.

Пример использования

```
hostname# iplir show exchange-keys
|----------|---------|-----------|-------------------------|-----------------|
|   Peer   | Variant | StartDate |        ExpiryDate       |     KeyID       |
|----------|---------|-----------|-------------------------|-----------------|
|0x5ae00002|        0| 2024-11-04|  2026-01-28(  398 days) |0x0200e0...594170|
|0x5ae00001|        0| 2024-11-04|  2026-01-28(  398 days) |0x0100e0...a04000|
|0x5ae00004|        0| 2024-11-04|  2026-01-28(  398 days) |0x0400e0...6b21e7|
|----------|---------|-----------|-------------------------|-----------------|
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).
- `TCP SYN timeout` — таймаут установления TCP-соединения в секундах.
- `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           1000000
TCP SYN timeout           120
Connection ttl TCP        1800
Connection ttl UDP        300
ICMP timeout              30
Connection ttl IP         300
Total connections count   10
Local connections count   10
VPN connections count     0
Forward connections count 0
Tunnel connections count  0
```

iplir show key-info

Получить информацию о ключе защиты обновлений узла ViPNet Coordinator IG.

Синтаксис

```
iplir show key-info
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде на экран выводится следующая информация:

- о ключе защиты обновлений 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:
  - `Support systems` — поддерживаемые системы и их статус;
  - `Support crypto suites` — 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 tcptunnel-info

Просмотреть настройки TCP-туннеля на ViPNet Coordinator IG.

Синтаксис

```
iplir show tcptunnel-info
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

В результате выполнения команды отображается информация:

- `Current role` — текущая роль ViPNet Coordinator IG:

- `client` — клиент TCP-туннеля;
- `server` — сервер TCP-туннеля.

- Параметры сервера TCP-туннелей:
  - Состояние (включён, выключен);
  - `TCP server port` — номер порта для входящих TCP-соединений;
  - `Max TCP-tunnels` — максимально возможное количество TCP-туннелей;
  - `Current TCP-tunnels` — количество активных TCP-туннелей.
- Параметры клиента TCP-туннеля:
  - Состояние (включён, выключен);
  - `TCP-tunnel mode` — режим работы клиента TCP-туннеля:
    - `auto` — автоматическое включение TCP-туннеля при пропадании соединения по UDP и выключение при его появлении;
    - `forced` — TCP-туннель устанавливается всегда, когда возможно, даже при доступе к серверу соединения по UDP.
  - `TCP-tunnel server access port` — номер порта для исходящих TCP-соединений с сервером TCP-туннелей.

Пример использования

```
hostname> iplir show tcptunnel-info


Current role: server


TCP-tunnel server is running
TCP server port: 80
Max TCP-tunnels: 100
Current TCP-tunnels: 0


TCP-tunnel client is disabled
TCP-client mode: auto
TCP-tunnel server access port: 443
```

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 tcptunnel client mode

Изменить режим работы клиента TCP-туннеля.

Синтаксис

```
iplir tcptunnel client mode {auto | forced}
```

Параметры и ключевые слова

- `auto` — автоматическое включение TCP-туннеля при пропадании соединения по UDP и выключение при его появлении;
- `forced` — TCP-туннель устанавливается всегда, когда возможно, даже при доступе к серверу соединения по UDP.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если текущая роль — сервер TCP-туннелей, команда выполнится, когда будет назначена роль клиента TCP-туннеля.
- Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Устанавливать TCP-туннель всегда, когда возможно, даже при доступе к серверу соединения по UDP:

```
hostname# iplir tcptunnel client mode forced
TCP-client mode: forced
```

iplir tcptunnel client on/off

Включить или выключить работу клиента TCP-туннеля.

Синтаксис

```
iplir tcptunnel client {on | off}
```

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Включить работу клиента TCP-туннеля:

```
hostname# iplir tcptunnel client on
TCP-tunnel client is enabled
```

iplir tcptunnel client port

Задать порт для подключения ViPNet Coordinator IG к серверу TCP-туннелей.

Синтаксис

```
iplir tcptunnel client port <номер порта>
```

Параметры и ключевые слова

`<номер порта>` — номер TCP порта. Допустимые значения: 1–65535.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Задать порт 5252 для доступа к серверу TCP-туннелей:

```
hostname# iplir tcptunnel client port 5252
New TCP server port: 5252
```

iplir tcptunnel role

Назначить ViPNet Coordinator IG роль сервера TCP-туннелей или клиента TCP-туннеля.

Синтаксис

```
iplir tcptunnel role {server | client}
```

Параметры и ключевые слова

- `server` — роль сервера TCP-туннелей.
- `client` — роль клиента TCP-туннеля.

Значения по умолчанию

Задана роль сервера TCP-туннелей.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Роль можно назначить только для координаторов которые работают в режиме «С динамической трансляцией адресов».
- Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Назначить ViPNet Coordinator IG роль клиента TCP-туннеля:

```
hostname# iplir tcptunnel role client
New TCP-tunnel role: client
```

iplir tcptunnel server on/off

Запустить или остановить сервер TCP-туннелей.

Синтаксис

```
iplir tcptunnel server {on | off}
```

Параметры и ключевые слова

- `on` — запустить сервер TCP-туннелей.
- `off` — остановить сервер TCP-туннелей.

Значения по умолчанию

Сервер TCP-туннелей остановлен.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если текущая роль — клиент TCP-туннеля, команда выполнится, когда будет назначена роль сервера TCP-туннелей.
- Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Запустить сервер TCP-туннелей:

```
hostname# iplir tcptunnel server on
TCP-tunnel server is enabled
```

iplir tcptunnel server port

Задать порт для подключения клиентов TCP-туннеля к ViPNet Coordinator IG в роли сервера TCP-туннелей.

Синтаксис

```
iplir tcptunnel server port <номер порта>
```

Параметры и ключевые слова

`<номер порта>` — номер TCP порта. Допустимые значения 1–65535.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Служба `iplircfg` должна быть запущена (iplir start).

Пример использования

Задать порт 5252 для доступа к ViPNet Coordinator IG в роли сервера TCP-туннелей:

```
hostname# iplir tcptunnel server port 5252
New TCP server port: 5252
```

iplir view

Просмотреть журнал IP-пакетов.

Синтаксис

```
iplir view
```

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**.
- Действие команды аналогично `machine logs show network-traffic`.

Пример использования

```
hostname> iplir view
```

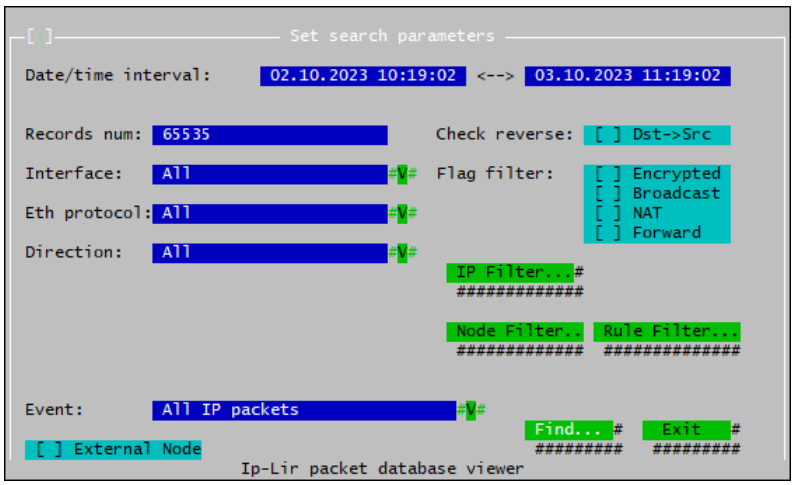


Рисунок 1. Задание параметров поиска записей в журнале IP-пакетов

iplir warning-threshold

Задать период оповещения о скором истечении срока действия:

- ключей обмена;
- ключа защиты обновлений;
- 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.

Пример использования

```
hostname# iplir warning-threshold 14
Key warnings will start displaying in 14 days before expiry date.
```

Команды группы machine

Выключение и перезагрузка ViPNet Coordinator IG, установка имени компьютера и системного времени, работа с системным журналом, а также регламентное тестирование ViPNet Coordinator IG.

machine backup

Включить или выключить автоматическое резервное копирование индивидуальной конфигурации ViPNet Coordinator IG на сервер ViPNet Prime.

Синтаксис

```
machine backup {on | off}
```

Параметры и ключевые слова

- `on` — включить автоматическое резервное копирование;
- `off` — выключить автоматическое резервное копирование.

Значения по умолчанию

Автоматическое резервное копирование выключено (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- После включения автоматического резервного копирования индивидуальная конфигурация ViPNet Coordinator IG будет копироваться ежедневно в случайное время из интервала 21:00–23:00. Чтобы настроить время резервного копирования, выполните команду: `machine backup schedule`.
- После выключения автоматического резервного копирования настроенное время резервного копирования удаляется.
- Команда используется только на активном узле кластера.

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 IG 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 доступна только 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 IG 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>`.

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 IG 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. Разрешённые символы: `A–Z`, `a–z`, `0–9`, специальные символы.
- Команда устанавливает глобальную блокировку управляющих запросов; текущие сессии пользователей сохраняются, новые сессии не открываются.
- В кластере команда доступна только 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 180KB free space and press Enter
General USB Flash Disk successfully mounted.
Copying ig10i2-40cd0004-20230720T152132Z.vbe to USB drive. Press ^+C to abort.
File successfully copied. Unmounting USB drive...
You may remove the USB drive.
```

machine config import

Импортировать настройки универсальной конфигурации или индивидуальную конфигурацию ViPNet Coordinator IG с USB-носителя.

Синтаксис

```
machine config import
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При импорте файла универсальной конфигурации (`vbe`) 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`).
    - `Modbus Gateway` — настройки и маршруты шлюза Modbus: с добавлением маршрутов для Modbus-устройств к текущим (`append`) или с их заменой (`replace`).
    - `Industrial protocol filtration settings` — правила фильтрации промышленных протоколов: с добавлением к текущим правилам (`append`) или с их заменой (`replace`).
    - `General-purpose input/output settings (GPIO)` — настройки интерфейса GPIO.
    - `Network-interface settings` — настройки сетевых интерфейсов.
    - `Static routing settings` — таблицы и политики статической маршрутизации: `append` или `replace`.
- Файл индивидуальной конфигурации (`ecf`) зашифрован на ключе обмена. Импортировать индивидуальную конфигурацию можно только на тот ViPNet Coordinator IG, на котором она была создана.

- По завершении импорта конфигурации отображаются статические IP-адреса сетевых интерфейсов. Возможность подключения к ViPNet Coordinator IG по этим интерфейсам определяется сетевыми фильтрами.
- Команда устанавливает глобальную блокировку управляющих запросов; текущие сессии пользователей сохраняются, новые сессии не открываются.
- По завершении импорта требуется перезагрузить ViPNet Coordinator IG.
- Команда выполняется на активном узле кластера.

Пример использования

Импорт настроек универсальной конфигурации:

```
hostname# machine config import
Insert USB drive and press Enter


Found ig-20210220T152132Z.vbe.
Product: ViPNet Coordinator IG
Platform: IG100 I1
Software version: 5.2.0-4424
Description: universal configuration


Enter configuration password:
Loading settings...


Select which settings you want to import:
Firewall [Yes/No] : y
Append firewall settings or replace them? [a/r] : a
Modbus Gateway [Yes/No] : y
Append Modbus Gateway routes or replace them? [a/r] : r
Industrial protocol filtration settings [Yes/No] : y
Append filtration rules or replace them? [a/r] : r
General-purpose input/output settings (GPIO) [Yes/No] : Yes
Network-interface settings [Yes/No] : y
Static routing settings [Yes/No] : 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
…
Settings successfully imported. You may remove the USB drive.
IMPORTANT: Please reboot the appliance to apply the settings.
```

Импорт индивидуальной конфигурации ViPNet Coordinator IG:

```
hostname# machine config import
Insert USB drive and press Enter

Found ig-20210220T152132Z.ecf.
...
After the import the device should be available with following parameters:
Web-interface port: 8080
SSH-port: 22
Obtained DHCP-addresses.
…
Settings successfully imported. You may remove the USB drive.
IMPORTANT: Please reboot the appliance to apply the settings.
```

machine halt

Завершить работу ViPNet Coordinator IG.

Синтаксис

```
machine halt
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда доступна только для исполнения ViPNet Coordinator IG1000 Q1.

Пример использования

```
hostname# machine halt

Shutting down in progress
```

machine hosts add

Добавить запись о соответствии IP-адреса доменному имени в файл hosts ViPNet Coordinator IG.

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 IG.

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 IG.

Синтаксис

```
machine hosts show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Для завершения просмотра нажмите **Q** или **Ctrl+C**.

Пример использования

```
hostname> machine hosts show
127.0.0.1 ig10i1-2c67000b localhost localhost.localdomain
11.1.0.23 nvs.prime
```

machine logs clear dns

Очистить журнал DNS-запросов.

Синтаксис

```
machine logs clear dns
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

В процессе очистки журнала DNS-запросов DNS-сервер останавливается.

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 журналов на USB-носитель.

Синтаксис

```
machine logs export usb
```

Режимы командного интерпретатора

- Режим просмотра.

- Режим настройки.

Особенности использования

- Имя архива файлов журналов — `logs_<id_узла>_<платформа><ревизия>_<версия>_<имя>_<гггг_мм_дд_чч_мм_сс>.tar.gz`:
  - `<id_узла>` — ViPNet ID узла;
  - `<платформа>` — аппаратная платформа;
  - `<ревизия>` — ревизия аппаратной платформы;
  - `<версия>` — версия ПО;
  - `<имя>` — имя узла;
  - `<гггг_мм_дд_чч_мм_сс>` — дата и время создания файла.
- 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 Linux и Windows с системным временем.

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/audit/
/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/hw_management_1.dblite
/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/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/startboot.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 612KB free space and press Enter
Generic Flash Disk successfully mounted.


Copying logs_40cd0005_ig10i2NONE_5.1.0-16_ig10i2-40cd0005_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 IG.

Синтаксис

```
machine logs export-and-clear usb
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Имя архива файлов журналов — `logs_<идентификатор узла>_<платформа><ревизия платформы>_<версия ПО>_<название узла>_<YYYY_MM_DD_HH_MM_SS>.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 Linux и Windows с системным временем.

Пример использования

```
hostname# machine logs export-and-clear usb
Are you sure to export and remove logs? [Yes/No] : Yes


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

acking of log files in progress. Press ^+C to abort.

Stopping system log daemon: syslogd.

Starting system log daemon: syslogd.

Insert USB drive with at least 620KB free space and press Enter

Generic Flash Disk successfully mounted.


Copying logs_40cd0005_ig10i2NONE_5.1.0-16_ig10i2-40cd0005_2023_01_24_12_59_09.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 IG10I2 successfully.
```

machine logs export ipf-traffic usb

Экспортировать журнал пакетов промышленных протоколов на USB-носитель.

Синтаксис

```
machine logs export ipf-traffic usb <имя>
```

Параметры и ключевые слова

`<имя>` — имя файла экспорта.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед экспортом необходимо сохранить журнал в файл (см. документ «Настройка с помощью командного интерпретатора», раздел «Экспорт журнала пакетов промышленных протоколов»).
- При вводе имени файла работает автодополнение и подсказка, данные для подсказки берутся из списка существующих файлов экспорта.

Пример использования

Чтобы экспортировать файл `ipflog`, в который сохранены записи журнала пакетов промышленных протоколов:

```
hostname# machine logs export ipf-traffic usb ipflog
Put ipflog.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 ipflog.tar.gz to be copied onto the USB drive.
File ipflog.tar.gz was successfully copied onto the USB drive.
You may remove the USB drive.
```

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 cef include

Добавить события в список событий журнала IP-пакетов, экспортируемых в формате CEF.

Синтаксис

```
machine logs settings cef <интерфейс> include <события>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса;
- `<события>` — номера событий, разделённые запятой.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда позволяет вернуть события в список событий, экспортируемых в формате CEF, которые были исключены из списка командой `machine logs settings cef exclude`.

Пример использования

```
hostname# machine logs settings cef eth0 include 2,121,33
```

machine logs settings cef event-type

Изменить 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;
- `<интерфейс>` — имя сетевого интерфейса.

Значения по умолчанию

- Если сетевой интерфейс не указан, тип событий задаётся для всех интерфейсов.
- По умолчанию задан тип событий `blocked`.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# machine logs settings cef event-type all


hostname# machine logs settings cef event-type blocked eth2
```

machine logs settings cef exclude

Исключить события из списка событий журнала IP-пакетов, экспортируемых в формате CEF.

Синтаксис

```
machine logs settings cef <интерфейс> exclude {<события> | none}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса;
- `<события>` — номера событий, разделённые запятой;
- `none` — отменить все исключения, созданные данной командой.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# machine logs settings cef eth0 exclude 2,121,33


hostname# machine logs settings cef eth0 exclude none
```

machine logs settings size

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.

Значения по умолчанию

Для обоих журналов задан максимальный размер — 50 Мбайт.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Если текущий размер журнала превышает 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 60 Мбайт:

```
hostname# machine logs settings crypto-audit size 60
```

machine logs settings network-traffic maxsize

Задать максимальный размер журнала IP-пакетов для 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 IG:

Таблица 4. Размер по умолчанию и максимальный размер журнала IP-пакетов, Мбайт

Исполнение	Размер по умолчанию	Макс. размер для физических интерфейсов	Макс. размер для виртуальных интерфейсов
ViPNet Coordinator IG10 I1	10	10	
ViPNet Coordinator IG10 I2	10	10	
ViPNet Coordinator IG100 I1	10	10	
ViPNet Coordinator IG100 I4	50	50	
ViPNet Coordinator IG100 I5	10	10	
ViPNet Coordinator IG1000 Q1	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 IG 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-соединения не регистрируется — в журнале IP-пакетов номер порта указывается равным нулю, что позволяет объединить события о попытках подключения к какому-либо порту ViPNet Coordinator IG 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 максимальный 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:

- Максимальный размер и процент заполнения журналов аудита и СКЗИ.
- Настройки экспорта журнала IP-пакетов в формате CEF:
  - статус экспорта:
    - `enabled` — включен;
    - `disabled` — выключен;
  - 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;
  - `Timedif` — 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.
  - `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  Timedif   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
```

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
2025 12:37:33 [hostname] [Single Mode] backup_dump [success] [System]
Details: finish
2025 12:37:38 [hostname] [Single Mode] CheckIntegrity [success] [System]
Details: failoverd: initializing (single)
2025 12:37:39 [hostname] [Single Mode] CheckIntegrity [success] [System]
Details: iplircfg: initializing
```

```
2025 12:37:42 [hostname] [Single Mode] backup_dump [success] [System]
Details: finish
2025 12:38:04 [hostname] [Single Mode] StartSession [failed] [System]
Details: userid:admin ticket:
2025 12:38:14 [hostname] [Single Mode] StartSession [success] [System]
Details: userid:admin ticket:AAA__17c91f_bd5b57_1c936a_9eb8e0
2025 12:38:52 [hostname] [Single Mode] Lock [success] [System]
...
```

Просмотреть записи журнала, в которых встречается строка `9eb8e0`:

```
hostname# machine logs show crypto-audit text 9eb8e0
2025 12:38:14 [hostname] [Single Mode] StartSession [success] [System]
Details: userid:admin ticket:AAA__17c91f_bd5b57_1c936a_9eb8e0
```

machine logs show ipf-traffic

Просмотреть журнал пакетов промышленных протоколов.

Синтаксис

```
machine logs show ipf-traffic
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- После ввода команды будет запущена программа просмотра журнала с эмуляцией графического интерфейса.
- В кластере команда доступна только на активном узле.
- Журнал может отображаться по-разному в зависимости от способа подключения к ViPNet Coordinator IG. Например, при локальном подключении через консоль с помощью программы PuTTY журнал отображается в чёрно-белом виде. Для отображения журнала в цветном виде, используйте:
  - SSH-подключение;
  - компьютер с Linux и стандартное приложение командной строки (терминал) или компьютер с Windows и приложение Git Bash.

  Для подключения выполните команды:

```
export TERM=xterm
ssh user@<IP-адрес>
```

где `<IP-адрес>` — IP-адрес сетевого интерфейса ViPNet Coordinator IG, к которому вы хотите подключиться по SSH.

Пример использования

```
hostname# machine logs show ipf-traffic
```

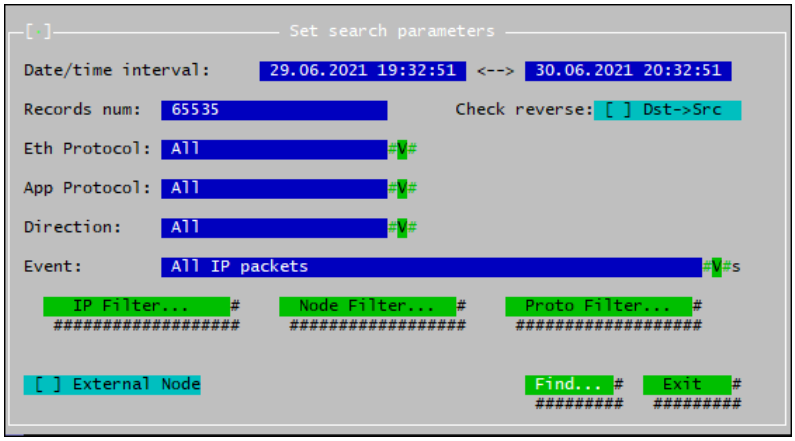


Рисунок 2. Задание параметров поиска записей в журнале пакетов промышленных протоколов

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 2025
-------------------------------------------------------------------------------
-----------------------------------------------------------------
| Envelope filename | Personal envelope name | Sender| Receiver            |Date-Time
 |     Event         |      Size   |      Description   |      Task          |
-----------------------------------------------------------------
| ~OJ)(#(A.RJ9      | ~OJ)(#(A.RJ9               | Admin    | xfva | 11.02.2025 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**.

Пример использования

```
hostname> machine logs show network-traffic
```

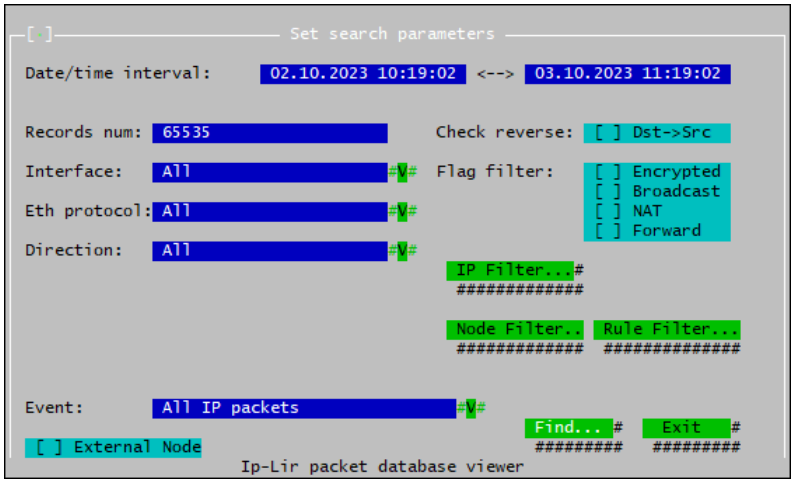


Рисунок 3. Задание параметров поиска записей в журнале IP-пакетов

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 IG;
- `string <строка>` — вывод записей, содержащих строку текста.

Значение по умолчанию

Без указания параметров отображаются все записи системного журнала.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Параметр `<время>` задаётся в формате `YYYY-MM-DD hh:mm:ss`.
- В параметре `<строка>` можно использовать буквы (`A-Z`, `a-z`), цифры (`0-9`), символы (`!#$%&()*+,-./:;<=>@[]_{|}~`) и пробел (в этом случае строку необходимо заключить в двойные кавычки).
- Для завершения просмотра нажмите клавишу **Q**.

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 2025 года, выводимых в обратном порядке:

```
hostname# machine logs show syslog reversed since 2025-02-22 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

2025 12:38:14 [hostname] [Single Mode] VPN:ViPNet:ShowWarningThreshold [success] [admin]

Details: Command:'certificate or keys expiration request '

2025 12:38:14 [hostname] [Single Mode] View the password protectioncounter [success]
[admin]

Details: Command:'Recorded failed authentication request '
```

```
2025 12:38:53 [hostname] [Single Mode] Edit firewall filters via Web Access [success]
[admin]

Details: Command:'firewall local add 'src' '@any' 'dst' '@any' 'pass' '

2025 12:38:53 [hostname] [Single Mode] Add firewall filter [success] [admin]

Details: Command:'firewall local add 'src' '@any' 'dst' '@any' 'pass' '

2025 12:39:05 [hostname] [Single Mode] Show network interface parameters [success] [admin]

Details: Command:'inet show interface eth0'

2025 12:39:58 [hostname] [Single Mode] Show idle session time-out [success] [admin]

Details:

2025 12:39:58 [hostname] [Single Mode] Show appliance info [success] [admin]

Details:

2025 12:39:58 [hostname] [Single Mode] Viewing license information[success] [admin]

Details:

...
```

Просмотреть записи журнала, начиная с 14:50 22 ноября 2025 года, выводимые в обратном порядке:

```
hostname# machine logs show user-audit reversed from 2025-11-22 14:50:00
```

Просмотреть записи журнала с 14:50 по 17:50 22 ноября 2025 года пользователя `admin` с неуспешным результатом выполнения запроса:

```
hostname# machine logs show user-audit result failed from 2025-11-22 14:50:00 to 2025-11-22
17:50:00 user admin
```

machine mode set

Переключить режим работы межсетевого экрана ViPNet Coordinator IG.

Синтаксис

```
machine mode set {normal | service | emergency}
```

Параметры и ключевые слова

- `normal` — штатный режим;
- `service` — режим регламентного обслуживания;
- `emergency` — специальный режим.

Значения по умолчанию

После инициализации ViPNet Coordinator IG и после смены типа межсетевого экрана на тип «Д» устанавливается штатный режим (`normal`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Выполнение команды возможно, если ViPNet Coordinator IG работает как межсетевой экран типа «Д».
- После ввода команды необходимо подтвердить изменение режима (`Yes/No`).

Пример использования

Чтобы переключать режим работы межсетевого экрана ViPNet Coordinator IG в специальный режим:

```
hostname# machine mode set emergency
Warning! Switching to emergency mode will change the following:
Software upgrade, key set update: disabled.
Firewall mode: emergency.
Continue? [Yes/No] Yes
Mode switched successfully!
emergency mode
Software upgrade, key set update: disabled.
Firewall mode: emergency.
```

machine mode show

Просмотреть текущий режим работы межсетевого экрана ViPNet Coordinator IG.

Синтаксис

```
machine mode show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Выполнение команды возможно, если ViPNet Coordinator IG работает как межсетевой экран типа «Д».

- Вывод команды содержит следующую информацию:
  - Режим работы межсетевого экрана:
    - `normal` — штатный режим;
    - `service` — режим регламентного обслуживания;
    - `emergency` — специальный режим.
  - Возможность обновления ПО и справочников и ключей в текущем режиме:
    - `enabled` — обновление возможно (для режима регламентного обслуживания);
    - `disabled` — обновление невозможно (для специального и штатного режимов).

Пример использования

```
hostname> machine mode show
normal mode
Software upgrade, key set update: disabled.
Firewall mode: normal.
```

machine reboot

Перезагрузить ViPNet Coordinator IG.

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 IG 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 IG 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 IG.

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 IG 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 IG.

Синтаксис

```
machine self-test [rbb]
```

Параметры и ключевые слова

`rbb` — запустить проверку дополнительной памяти с восстановлением повреждённых секторов перед запуском регламентного тестирования.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команду нельзя выполнить по SSH.
- После ввода команды подтвердите остановку всех служб. После успешного тестирования службы будут автоматически запущены.
- В процессе регламентного тестирования проводятся:
  - Проверка файловых систем на загрузочном носителе.
  - Проверка контрольных сумм исполняемых и конфигурационных файлов ПО ViPNet Coordinator IG.
  - 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.
  - Создаётся 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 IG. Если восстановление конфигурационного файла завершилось неудачно, ViPNet Coordinator IG 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 IG 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 IG не должны отличаться от даты и времени узлов сети ViPNet более чем на величину `timediff`. Иначе текущие управляющие соединения с ViPNet Coordinator IG 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 2025 года и время, равное 12 часам:

```
hostname# machine set date 2025-02-22 12:00:00
Do you really wish to change the date?
Continue? [Yes/No]: Yes
```

machine set hostname

Изменить имя сетевого узла ViPNet Coordinator IG.

Синтаксис

```
machine set hostname <имя>
```

Параметры и ключевые слова

`<имя>` — имя сетевого узла. Допустимые символы: `A-z`, `0-9`, `-`. Длина: 1–63 символа.

Значения по умолчанию

Имя сетевого узла задаётся при инициализации ViPNet Coordinator IG. По умолчанию оно сформировано по шаблону `<название>-<идентификатор>`, где `название` — наименование аппаратной платформы ViPNet Coordinator IG без последних двух символов, а `идентификатор` — идентификатор узла в защищённой сети. Например: `IG100-270E033A`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Имя сетевого узла используется, в том числе, в SNMP-параметрах:

- `sysDescr` (OID .1.3.6.1.2.1.1.1.0);
- `sysName` (OID .1.3.6.1.2.1.1.5.0) — если параметр `sysName` не задан при настройке SNMP-агента.

Если в момент выполнения команды SNMP-агент был запущен, значения этих параметров не изменятся. Чтобы значения обновились, перезапустите SNMP-агент:

```
hostname# inet snmp stop
hostname# inet snmp start
```

Пример использования

Чтобы изменить имя сетевого узла на `IG100`:

```
hostname# machine set hostname IG100
```

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 IG (локальное ведение журнала).
- `null` — выключить ведение журнала.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- По умолчанию системный журнал хранится на ViPNet Coordinator IG (`local`).
- Если системный журнал будет храниться на удалённом узле, этот узел должен быть доступен для ViPNet Coordinator IG. Если узел является открытым, то на ViPNet Coordinator IG 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 IG.

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 на обоих узлах.

Примеры использования

```
hostname> machine show backup

Remote backup is ON

Last successful remote backup: 2025-12-15 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 IG.

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 2025
```

machine show hostname

Просмотреть имя ViPNet Coordinator IG.

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 IG.
- 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, файла подкачки и дискового пространства.

Синтаксис

```
machine show memory
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Информация об использовании оперативной памяти и файла подкачки (в Мбайт) выводится в виде таблицы, где строки соответствуют видам физической памяти:
  - `Mem` — оперативная память ОЗУ;
  - `Swap` — использование файла подкачки.

  Столбцы таблицы соответствует категориям выделенной или используемой памяти:
  - `total` — суммарный объём памяти;
  - `used` — объём используемой памяти без учёта буферов ядра;
  - `free` — объём неиспользуемой памяти;
  - `shared` — объём разделяемой (shared) памяти
  - `buff/cache` — суммарное количество памяти, занятое операционной системой под буферы ядра и под страничный кеш;
  - `available` — объём памяти, доступный приложениям без использования файла подкачки.
- Информация об использовании дискового пространства выводится в виде таблицы, где строки соответствуют подключенным разделам файловой системы ViPNet Coordinator IG:
  - `root` — корневой раздел Linux;
  - `tmpfs` — раздел, выделенный под файл подкачки;
  - `overlay` — объединённая файловая система ViPNet Coordinator IG.

  Таблица включает следующие столбцы:

  `Filesystem` — имя раздела файловой системы;

  `Size` — размер раздела файловой системы;

  `Used` — объём использованного пространства;

  `Avail` — объём доступного пространства;

  `Use%` — процент использования раздела файловой системы;

  `Mounted on` — точка монтирования раздела файловой системы.

  По умолчанию значения доступного и используемого дискового пространства выводятся в Кбайт. Для сокращённого вывода некоторых величин используются модификаторы размера:
  - M — Мбайт;
  - G — Гбайт.

  Например, значение `2.0G` означает 2 Гбайт.

Пример использования

```
hostname> machine show memory
        total     used     free      shared     buff/cache      available
Mem:    245       93       20        85         131             59
Swap:   0         0        0

Filesystem              Size    Used    Avail   Use%  Mounted on
root                    123M    86M     38M     70%   /mnt/root
tmpfs                   123M    220K    123M    1%    /run
tmpfs                   123M    16K     123M    1%    /tmp
udev                    10M     0       10M     0%    /dev
ubil:VIPNET_HW_MAIN     393M    191M    198M    50%   /mnt/main
/dev/mmcblk0pl          14G     58M     14G     1%    /additional
overlay                 123M    86M     38M     70%   /
```

machine show priority-stats

Просмотреть статистику обработанных IP-пакетов с учётом приоритета в обслуживании (QoS).

Синтаксис

```
machine show priority-stats
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде выводятся значения:

- `queue n` — количество пакетов, обработанных очередью n.
- `total proccessed` — общее количество обработанных пакетов с учётом приоритета.

Пример использования

```
hostname> machine show priority-stats

queue 0 : 12

queue 1 : 202

queue 2 : 340
```

```
queue 3 : 10

queue 4 : 12

queue 5 : 21

queue 6 : 5

queue 7 : 9

total proccessed : 611
```

machine show timezone

Просмотреть информацию о временной зоне (часовом поясе), настроенной на ViPNet Coordinator IG.

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 IG после загрузки, а также среднее число процессов в очереди за ближайшее время.

Синтаксис

```
machine show uptime
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> machine show uptime
 18:04:29 up 44 min, 1 user, load average: 2.19, 2.18, 2.06
```

По команде отображается следующая информация:

- текущее время;
- время работы ViPNet Coordinator IG после загрузки;
- текущее число пользователей;
- среднее число процессов в очереди ожидания процессора за последние 1, 5 и 15 минут.

machine update-queue

Просмотреть очередь отложенных обновлений компонентов и настроек ViPNet Coordinator IG, 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 IG.
  - `License` — лицензия.
  - `Firewall` — политики безопасности.
  - `VPN node info` — справочники и ключи.
  - `Services` — настройки прикладных служб.
- `Sent` — время отправки обновления из ViPNet Prime.
- `Application time` — плановое время применения обновления на ViPNet Coordinator IG.

Пример использования

```
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 IG 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 консоль выводится не более 10000 записей о конвертах.
- Для просмотра очереди исходящих конвертов используйте навигационные клавиши.
- Чтобы завершить просмотр, нажмите **Q**.

Пример использования

```
hostname> mftp info

Running MFTP remote info

Workstation configured for ID 2C670001 (IG10i2)

Read ID Info for 9 nodes.

Waiting for data. It will take about 30 seconds...

Queue cash size: 25

0 "m~_w~lio.ctl 6.361K Type:"Control request" 02-02-2023 12:26:32 <2c670002, Control
Center>

       Receivers:

       <2c670016, ivanov-IG100I1>

1 "ms7br_2.ctl 7.199K Type:"Control request" 08-02-2023 14:11:11 <2c670002, Control
Center>

       Receivers:

       <2c670016, ivanov-IG100I1>
```

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.

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 poe

Настройка подачи питания и проверки доступности устройств с поддержкой технологии Power over Ethernet (PoE). Команды этой группы доступны только для исполнений ViPNet Coordinator IG с поддержкой PoE.

poe interface check-ip action add restart

Перезагружать устройство с поддержкой PoE в случае его недоступности.

Синтаксис

```
poe interface <интерфейс> check-ip action add restart <интервал>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса, к которому подключено устройство с поддержкой PoE.
- `<интервал>` — время в секундах, на которое будет отключено питание от устройства. По истечении этого времени, питание вновь будет подано на устройство. Диапазон допустимых значений: 1–120.

Значения по умолчанию

В случае недоступности устройства с поддержкой PoE в системный журнал записывается информация об этом событии.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- В результате выполнения команды будут выполняться два действия в случае недоступности устройства:
  - перезагрузка устройства;
  - запись события в системный журнал ViPNet Coordinator IG.

  Эти действия будут выполняться, если включена проверки доступности устройства (см. poe interface check-ip mode).

- Команда недоступна в кластере.

Пример использования

Чтобы настроить перезагрузку устройства, подключенного к интерфейсу `eth2`, на 15 секунд в случае его недоступности:

```
hostname# poe interface eth2 check-ip action add restart 15
```

poe interface check-ip action clean

Удалить все действия, заданные командной `poe interface check-ip action add` (см. poe interface check-ip action add restart).



Примечание. В ViPNet Coordinator IG версии 5.2.0 вы можете добавить только одно действие, которое будет выполняться при недоступности устройства с поддержкой PoE — перезагрузка устройства. Запись событий в системный журнал отключить нельзя.

Синтаксис

```
poe interface <интерфейс> check-ip action clean
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса, к которому подключено устройство с поддержкой PoE.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- После выполнения команды запись информации о недоступности устройства в системный журнал останется включенной (запись в журнал нельзя отключить).
- Команда недоступна в кластере.

Пример использования

Чтобы удалить все действия, которые должны быть выполнены при недоступности устройства с поддержкой PoE, подключенного к `eth2`:

```
hostname# poe interface eth2 check-ip action clean

no response actions: N/A
```

poe interface check-ip action del restart

Не перезагружать устройство с поддержкой PoE в случае его недоступности.

Синтаксис

```
poe interface <интерфейс> check-ip action del restart
```

Параметры и ключевые слова

`<интерфейс>` — имя сетевого интерфейса, к которому подключено устройство с поддержкой PoE.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- После выполнения команды запись информации о недоступности устройства в системный журнал останется включённой (запись в журнал нельзя отключить).
- Команда недоступна в кластере.

Пример использования

Чтобы устройство, подключённое к `eth2`, не перезагружалось в случае недоступности его IP-адреса с ViPNet Coordinator IG:

```
hostname# poe interface eth2 check-ip action del restart
```

poe interface check-ip address

Задать IP-адрес подключённого устройства с поддержкой PoE для проверки его доступности.

Синтаксис

```
poe interface <интерфейс> check-ip address <IP-адрес>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса, к которому подключено устройство с поддержкой PoE.

- `<IP-адрес>` — IP-адрес подключённого устройства.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- Чтобы включить проверку доступности устройства, используйте команду poe interface check-ip mode.
- Команда недоступна в кластере.

Пример использования

Задать IP-адрес 192.168.0.1 для проверки доступности устройства с поддержкой PoE, подключённого к `eth2`:

```
hostname# poe interface eth2 check-ip address 192.168.0.1
```

poe interface check-ip failed-attempts

Задать число проверок IP-адреса устройства с поддержкой PoE, при достижении которого устройство считается недоступным.

Синтаксис

```
poe interface <интерфейс> check-ip failed-attempts <число проверок>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса, к которому подключено устройство с поддержкой PoE.
- `<число проверок>` — число проверок, при достижении которого устройство с поддержкой PoE считается недоступным. Диапазон допустимых значений: 1–10.

Значения по умолчанию

Для каждого интерфейса задано число проверок — 2.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- Чтобы включить проверку доступности устройства, используйте команду poe interface check-ip mode.
- Команда недоступна в кластере.

Пример использования

Задать число проверок доступности устройства с поддержкой PoE, подключённого к `eth2`, равное трём:

```
hostname# poe interface eth2 check-ip failed-attempts 3
```

poe interface check-ip frequency

Задать период опроса подключённого устройства с поддержкой PoE для проверки его доступности.

Синтаксис

```
poe interface <интерфейс> check-ip frequency <период опроса>
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса, к которому подключено устройство с поддержкой PoE.
- `<период опроса>` — время в секундах, через которое выполняется проверка доступности подключённого устройства. Диапазон допустимых значений: 1–120.

Значения по умолчанию

Для каждого интерфейса задан период опроса — 10 секунд (`10`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- Чтобы включить проверку доступности устройства, используйте команду poe interface check-ip mode.
- Команда недоступна в кластере.

Пример использования

Задать период опроса устройства, подключённого к `eth2`, равный пяти секундам:

```
hostname# poe interface eth2 check-ip frequency 5
```

poe interface check-ip mode

Включить или выключить проверку доступности подключённого устройства с поддержкой PoE.

Синтаксис

```
poe interface <интерфейс> check-ip mode {on | off}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса, к которому подключено устройство с поддержкой PoE.
- `on` — включить проверку доступности устройства.
- `off` — выключить проверку доступности устройства.

Значения по умолчанию

- Проверка доступности устройств выключена (`off`).
- При включении проверки устанавливаются параметры:
  - период опроса — 10 секунд;
  - число проверок, при достижении которого устройство считается недоступным — 2;
  - действие, которое будет выполнятся в случае недоступности устройства — запись информации в системный журнал ViPNet Coordinator IG.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- Если на момент выполнения команды не задан IP-адрес проверяемого устройства, на экран будет выведено предупреждение.
- Параметры проверки доступности устройства с поддержкой PoE настраиваются с помощью команд:
  - poe interface check-ip address;

    - poe interface check-ip frequency;
    - poe interface check-ip failed-attempts;
    - poe interface check-ip action add restart.
- Команда недоступна в кластере.

Пример использования

Включить проверку доступности устройства, подключённого к `eth2`:

```
hostname# poe interface eth2 check-ip mode on
```

poe interface faststart

Разрешить подачу питания на устройства с поддержкой PoE до загрузки ПО ViPNet Coordinator IG.

Синтаксис

```
poe interface <интерфейс> faststart {on | off}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса, к которому подключено устройство с поддержкой PoE.
- `on` — разрешить подачу питания до загрузки ПО.
- `off` — запретить подачу питания до загрузки ПО.

Значения по умолчанию

Подача питания до загрузки ПО ViPNet Coordinator IG запрещена на всех интерфейсах (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Команда используется для ускорения загрузки подключённых устройств с поддержкой PoE.
- Питание на выбранный интерфейс будет подаваться при условии, что ранее была выполнена команда `poe interface power on`.
- При переключении системы защиты от сбоев из режима кластера в одиночный режим питание на интерфейс будет подано, если разрешена подача питания до загрузки ПО (`on`).
- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.

- Команда недоступна в кластере.

Пример использования

Разрешить подачу питания до загрузки ПО ViPNet Coordinator IG на интерфейс `eth2`:

```
hostname# poe interface eth2 faststart on
```

poe interface limit

Задать ограничение мощности, выделяемой на сетевой интерфейс по технологии PoE.

Синтаксис

```
poe interface <интерфейс> limit <ограничение>
```

Параметры и ключевые слова

- `<интерфейс>` — имя одного из сетевых интерфейсов, обозначенных на корпусе ViPNet Coordinator IG как **LAN**.
- `<ограничение>` — мощность в Ваттах. Диапазон допустимых значений: 0–60.

Значения по умолчанию

Установлено ограничение в 7 Вт для каждого интерфейса (`7`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- Если потребляемая мощность подключённого устройства с поддержкой PoE превышает заданное ограничение, сработает защита по току и устройство будет перезагружено.
- Если заданное ограничение для одного интерфейса превышает мощность, выделенную на питание всех устройств (15 Вт или 60 Вт — в зависимости от источника питания ViPNet Coordinator IG), питание не будет подано на устройство.
- Если сумма ограничений, заданных на всех интерфейсах, превышает мощность, выделенную на питание всех устройств, будет выведено предупреждение.
- Команда недоступна в кластере.

Пример использования

Задать ограничение мощности в 15 Ватт на интерфейсе `eth2`:

```
hostname# poe interface eth2 limit 15
```

poe interface power

Включить или выключить автоматическую подачу питания на сетевой интерфейс при подключении устройства, работающего по технологии PoE.

Синтаксис

```
poe interface <интерфейс> power {on | off}
```

Параметры и ключевые слова

- `<интерфейс>` — имя одного из сетевых интерфейсов, обозначенных на корпусе ViPNet Coordinator IG как **LAN**.
- `on` — включить автоматическую подачу питания.
- `off` — выключить автоматическую подачу питания.

Значения по умолчанию

Автоматическая подача питания на всех интерфейсах **LAN** выключена (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- Если при включении подачи питания к интерфейсу уже подключено устройство, питание на него будет подано после определения класса мощности устройства и при условии, что потребление мощности не превышает установленные ограничения.
- Команда недоступна в кластере.

Пример использования

Включить автоматическую подачу питания на интерфейс `eth2`:

```
hostname# poe interface eth2 power on
```

poe interface priority

Задать приоритет подачи питания на сетевой интерфейс по технологии PoE.

Синтаксис

```
poe interface <интерфейс> priority <приоритет>
```

Параметры и ключевые слова

- `<интерфейс>` — имя одного из сетевых интерфейсов, обозначенных на корпусе ViPNet Coordinator IG как **LAN**.
- `<приоритет>` — номер интерфейса в очереди на подачу питания по технологии PoE. Список возможных значений зависит от количества портов **LAN** в исполнении ViPNet Coordinator IG.

Значения по умолчанию

На всех сетевых интерфейсах установлен высший приоритет (`1`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При вводе команды работает автодополнение введённого имени интерфейса из списка интерфейсов **LAN**.
- Если задан одинаковый приоритет на интерфейсах, очерёдность подачи питания определяется порядковым номером в имени интерфейса, например, сначала `eth1`, затем `eth2`.
- Команда недоступна в кластере.

Пример использования

Чтобы питание сначала подавалось на устройство, подключённое к `eth2`, а затем (если хватит бюджета мощности PoE) на устройство, подключённое к `eth1`:

```
hostname# poe interface eth2 priority 1
hostname# poe interface eth1 priority 2
```

poe set syslog-level

Изменить уровень важности событий, записываемых в системный журнал и относящихся к службе управления питанием по технологии PoE.

Синтаксис

```
poe set 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` — предупреждения (warning);
- `3` — извещения (notice);
- `4` — информационные сообщения (info).

Каждый последующий уровень включает в себя предыдущие.

Значения по умолчанию

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

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда недоступна в кластере.

Пример использования

Чтобы записывать в системный журнал события не выше 2-го уровня:

```
hostname# poe set syslog-level 2
```

poe show

Просмотреть настройки и состояние службы управления питанием по технологии PoE, а также информацию о подключённых устройствах с поддержкой PoE.

Синтаксис

```
poe show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде выводится информация:

- `Service status` — состояние службы:
  - `running` — запускается;
  - `working` — запущена;
  - `error` — ошибка.
- `Log level` — уровень важности событий службы, записываемых в системный журнал ViPNet Coordinator IG;
- Информация о потребляемой и отдаваемой мощности:
  - `Power source` — источник питания ViPNet Coordinator IG:
    - `Power unit` — блок питания;
    - `PD (<сетевой интерфейс>)` — другое устройство по технологии PoE через порт **WAN**.
  - `System Power Budget [W]` — доступная мощность (Вт), которая может быть выделена с текущим источником питания (бюджет мощности PoE, зависит от `Power source`);
  - `Total allocated power [W]` — мощность (Вт), выделенная на порты **LAN**, на которые подано питание (зависит от `Power limit`);
  - `Total measured power [W]` — фактически потребляемая мощность (Вт), измеренная на портах **LAN**;
  - `Total allocated power limits [W]` — максимальная мощность (Вт), заданная пользователем (сумма `Power limit` всех интерфейсов);
  - `Budget deficit [W]` — недостаток мощности для питания устройств, заданных пользователем (разница между `Total allocated power limits` и `System Power Budget`).
- Информация о состоянии и настройках портов:
  - `PoE` — состояние функции PoE (`enabled` — включена, `disabled` — выключена);
  - `Power limit` — установленное ограничение мощности (мощность, которая может быть выделена на этот порт);
  - `Fast start` — подача питания до загрузки ПО ViPNet Coordinator IG (`on` — включена, `off` — выключена);
  - `Priority` — приоритет выделения мощности на порт.
- Информация о подключённом устройстве с поддержкой PoE:

`Type` — тип PoE и стандарт, которому соответствует устройство;

    - `Status` — состояние:
        - `Disabled` — устройство не подключено;
        - `Classification` — устройство в процессе классификации;
        - `Classification complete` — классификация завершена, определён класс мощности устройства, устройство ждёт подачи питания (питание может быть не подано, если установленное ограничение мощности превышает суммарную выделяемую мощность);
        - `Wait power enabled` — ожидание подачи питания;
        - `Power enabled` — питание подано;
        - `Error` — ошибка.
    - `Power class` — класс мощности устройства;
    - `Measured power [W]` — фактическая потребляемая мощность (Вт).
- Информация о проверке доступности подключённого устройства с поддержкой PoE:
    - `Status` — состояние:
        - `active` — устройство доступно;
        - `inactive since <последнее время успешной проверки>` — устройство недоступно;
        - `not checking` — доступность не проверяется.
    - `Address` — IP-адрес проверки;
    - `Frequency [sec]` — период опроса (с);
    - `Failed attempts until action` — количество неудачных попыток проверки;
    - `No response action` — действия, выполняемые при недоступности устройства:
        - `log` — запись события в системный журнал;
        - `restart (timeout restart waiting: <время>)` — перезагрузка.

Команда недоступна в кластере.

Пример использования

```
hostname> poe show

Service status: working

Log level: 3


Power source: PD (eth0)

System Power Budget [W]: 15

Total allocated power [W]: 14

Total measured power [W]: 11.2
```

```
Total allocated power limits [W]: 14
Budget deficit [W]: -1

eth1 ----------------------------------------
PoE: enabled
Power limit [W]: 7.0
Fast start: off
Priority: 1
Connected device:
    Type: IEEE 802.3af
    Status: Power Enabled
    Power class: 4 (30W)
    Measured power [W]: 4.6

Availability check:
    Status: active
    Address: 192.168.0.1
    Frequency [sec]: 10
    Failed attempts until action: 2
    No response action:
        log
        restart (Timeout restart waiting: 10)

eth2 ----------------------------------------
PoE: disabled
Power limit [W]: 7.0
Fast start: off
Priority: 1
Connected device:
    Type: N/A
    Status: Disabled
    Power class: N/A
    Measured power [W]: N/A
```

```
Availability check:
    Status: not checking
    Address:
    Frequency [sec]: 10
    Failed attempts until action: 2
    No response action:
        log
```

Команды группы service

Настройка и управление прокси-сервером, шлюзом Modbus, службой `piomonitor`, а также сертификатами, которые используются для доступа к веб-интерфейсу в исполнениях ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.

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 IG 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 удалён, протокол доступа к ViPNet Coordinator IG изменён 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 IG сертификат, закрытый ключ сертификата или список аннулированных сертификатов (CRL) с USB-носителя.

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-носителе файлов с расширениями PEM, CER и CRL. Затем предлагается выбрать сертификат, закрытый ключ сертификата или CRL.
- При импорте файлов с расширением CER и CRL выполняется их преобразование в формат PEM.
- При импорте проверяется уникальность сертификата по содержимому и по имени:
  - Если имя и содержимое уникальны — сертификат импортируется, имя остаётся 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 сертификаты, закрытые ключи 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 {md5 | sha1} subj [subj]
```

Параметры и ключевые слова

- `<имя>` — имя сертификата;
- `<длина ключа>` — длина создаваемого RSA-ключа в битах, можно задавать следующие значения: 1024, 1536, 2048, 3072, 4096;
- `md5` — алгоритм хэширования MD5;
- `sha1` — алгоритм хэширования SHA1;
- `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 учитывайте:
  - 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 **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 1024 бита, используя алгоритм шифрования MD5:

```
hostname# service cert request create name Cert1 bits 1024 digest md5
Generating a 1024 bit RSA private key
    ++++
writing new private key to '/etc/cert/Cert1_key.pem'
----
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 some 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]:RU
State or province Name (full name) [Some-State]:
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgets Pty Ltd]:Infotecs
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or IP-address or *.vipnet name, one value) []:infotecs.biz
Email Address []:post@infotecs.ru


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 *.vipnet name, several
value)[]:127.50.50.50
Creating request Cert1_req.pem is completed
```

- Чтобы создать запрос на сертификат с длиной ключа 1024 бита, используя алгоритм шифрования MD5 и дополнительные параметры запроса:

```
hostname# service cert request create name Cert1 bits 1024 digest md5 subj
"/C=RU/ST=Moscow/L=Moscow/O=Infotecs/OU=IT/CN=infotecs.ru/emailAddress=post@infote
cs.ru/subjectAltName=DNS:infotecs.biz,IP:127.50.50.50"
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-носитель.

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 IG.

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 сертификат, созданных в ViPNet Coordinator IG.

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 IG.

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 IG.

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 IG.

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 IG.

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 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.

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>]`, где:
  - `<адрес>` — IP-адрес или доменное имя;
  - `<порт>` — номер порта;
  - `<путь>` — путь на ICAP-сервере.

Значения по умолчанию

Если в адресе ICAP-сервера не указан порт, будет использоваться порт 1344.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите прокси-сервер (см. service http-proxy stop).
- Если в адресе ICAP-сервера не указан путь, IP-пакеты будут отправляться в корень URL.

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 удалён адрес доступа к ICAP-серверу для проверки исходящего трафика (запросы от пользователей сети к прокси-серверу);
- `respmod` — будет удалён 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.

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 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

Исполнение	Размер кеша по умолчанию, Мбайт	Макс. размер кеша, Мбайт
ViPNet Coordinator IG10 I1	10	10
ViPNet Coordinator IG10 I2	10	10
ViPNet Coordinator IG100 I1	10	10
ViPNet Coordinator IG100 I4	256	80% от объёма свободного места на диске
ViPNet Coordinator IG100 I5	10	10
ViPNet Coordinator IG1000 Q1	256	80% от объёма свободного места на диске

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).

Пример использования

Чтобы задать размер кеша 5 мегабайт:

```
hostname# service http-proxy cache 5
```

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 удалённого 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 номера 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 удалённого 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 номера 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, подключённого 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 неё 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 изменённым 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 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:
empty rule for Service:
================================================================================
Num   Name                                      Option  Schedule
Act   Protocol              Source              ->Destination
      DpiProtocol           DpiApp                DomainUser
================================================================================
7     HTTP-Proxy auto                           User
pass  tcp: to 1024          @HttpProxyUsers     ->192.168.203.174
      @any                  @any                  @any
--------------------------------------------------------------------------------
8     HTTP-Proxy auto                           User
pass  tcp: to 80, tcp: to 21 192.168.203.174    ->@InternetIP
      @any                  @any                  @any
--------------------------------------------------------------------------------
...
```

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 приёма 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 автодополнение 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 IG.

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 mbgw add

Добавить шлюз Modbus на последовательном интерфейсе.

Синтаксис

```
service mbgw add name <имя шлюза> serial <последовательный интерфейс> port <TCP-порт>
```

Параметры и ключевые слова

- `<имя шлюза>` — произвольное имя шлюза. Длина: 1–8 символов. Разрешённые символы: `A–Z`, `a–z`, `0–9`, `пробел - _ , .`
- `<последовательный интерфейс>` — имя последовательного интерфейса из списка доступных. Если на интерфейсе уже настроен шлюз Modbus, интерфейс не отображается в списке.
- `<TCP-порт>` — TCP-порт, на котором будет работать шлюз Modbus.

Значения по умолчанию

После выполнения команды добавляется шлюз Modbus со следующими настройками:

- Режим работы: TCP to RTU;
- Время ожидания запроса: 1500 мс;
- Время ожидания ответа: 1500 мс;
- Скорость TTY: 115200 бод;
- Контроль чётности: even;
- Задержка до отправки: 100 мс (для RS-485);
- Задержка после отправки: 0 мс (для RS-485).

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service mbgw add name electric serial rs232 port 502
```

service mbgw after-send-delay

Изменить интервал задержки, действующий после отправки посылки с последовательного интерфейса шлюза Modbus типа RS-485.

Синтаксис

```
service mbgw name <имя шлюза> after-send-delay <интервал>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `<интервал>` — интервал времени в миллисекундах, в течение которого происходит задержка после отправки посылки с последовательного интерфейса шлюза Modbus. Разрешённые значения: `0–10000`.

Значения по умолчанию

После добавления шлюза Modbus устанавливается значение 0 мс (см. service mbgw add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).
- Значение параметра `<интервал>` сохраняется в настройках шлюза Modbus, но используется только если шлюз Modbus работает на интерфейсе с типом RS-485.

Пример использования

```
hostname# service mbgw name electric after-send-delay 1
```

service mbgw baudrate

Изменить скорость последовательного интерфейса шлюза Modbus.

Синтаксис

```
service mbgw name <имя шлюза> baudrate <скорость>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.

- `<скорость>` — скорость работы последовательного интерфейса шлюза Modbus, в бодах. Возможные значения:
  - `1200`;
  - `1800`;
  - `2400`;
  - `4800`;
  - `9600`;
  - `19200`;
  - `38400`;
  - `57600`;
  - `115200`.

Значения по умолчанию

После добавления шлюза Modbus устанавливается значение 115200 (см. service mbgw add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric baudrate 57600
```

service mbgw before-send-delay

Изменить интервал задержки, действующий перед отправкой посылки с последовательного интерфейса шлюза Modbus типа RS-485.

Синтаксис

```
service mbgw name <имя шлюза> before-send-delay <интервал>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.

- `<интервал>` — интервал времени в миллисекундах, в течение которого происходит задержка перед отправкой посылки с последовательного интерфейса шлюза Modbus. Разрешённые значения: `1–10000`.

Значения по умолчанию

После добавления шлюза Modbus устанавливается значение 100 мс (см. service mbgw add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).
- Значение параметра `<интервал>` сохраняется в настройках шлюза Modbus, но используется только если шлюз Modbus работает на интерфейсе с типом RS-485.

Пример использования

```
hostname# service mbgw name electric before-send-delay 10
```

service mbgw delete

Удалить шлюз Modbus на последовательном интерфейсе.

Синтаксис

```
service mbgw delete name <имя шлюза>
```

Параметры и ключевые слова

`<имя шлюза>` — имя шлюза Modbus.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw delete name electric
```

service mbgw mode

Включить или выключить автоматический запуск одного или всех шлюзов Modbus при загрузке ViPNet Coordinator IG.

Синтаксис

```
service mbgw [name <имя шлюза>] mode {on | off}
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus;
- `on` — включить автоматический запуск;
- `off` — выключить автоматический запуск.

Значения по умолчанию

- Если имя шлюза не указано, настройка автоматического запуска будет выполнена для всех шлюзов Modbus.
- После инициализации ViPNet Coordinator IG автоматический запуск шлюзов Modbus выключен (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выключением автоматического запуска шлюза остановите его работу (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric mode on
Modbus gateway electric serial rs232 is mode on
```

service mbgw parity

Изменить режим работы с битом контроля чётности последовательного интерфейса шлюза Modbus.

Синтаксис

```
service mbgw name <имя шлюза> parity <режим>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `<режим>` — выбор режима работы с битом контроля чётности. Возможные значения:
  - `off` — режим, при котором проверка бита чётности не производится;
  - `even` — режим, при котором биты данных и бит чётности всегда должны составлять чётное число единиц;
  - `odd` — режим, при котором биты данных и бит чётности всегда должны составлять нечётное число единиц;
  - `mark` — режим, при котором бит чётности всегда принимает значение 1;
  - `space` — режим, при котором бит чётности всегда принимает значение 0;
  - `none` — режим, при котором бит чётности отсутствует.

Значения по умолчанию

После добавления шлюза Modbus устанавливается значение even (см. service mbgw add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric parity off
```

service mbgw port

Изменить TCP-порт для шлюза Modbus.

Синтаксис

```
service mbgw name <имя шлюза> port <TCP-порт>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `<TCP-порт>` — TCP-порт, на котором будет работать шлюз Modbus.

Значения по умолчанию

Устанавливается при добавлении шлюза Modbus (см. service mbgw add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Нельзя выбрать TCP-порт, который уже используется другим шлюзом Modbus.
- Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric port 501
```

service mbgw request-timeout

Изменить время ожидания запроса от ведущего Modbus-устройства.

Синтаксис

```
service mbgw name <имя шлюза> request-timeout <интервал>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `<интервал>` — интервал времени в миллисекундах, выделенный на получение посылки с запросом от ведущего Modbus-устройства. Интервал отсчитывается с момента начала получения посылки. Если до истечения интервала посылка не будет получена до конца, шлюз Modbus запишет сообщение об ошибке в системный журнал. Разрешённые значения: `1–10000`.

Значения по умолчанию

После добавления шлюза Modbus устанавливается значение 1500 мс (см. service mbgw add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric request-timeout 1800
```

service mbgw response-timeout

Изменить время ожидания ответа от ведомого Modbus-устройства.

Синтаксис

```
service mbgw name <имя шлюза> response-timeout <интервал>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `<интервал>` — интервал времени в миллисекундах, выделенный на ожидание ответа от ведомого Modbus-устройства. Интервал отсчитывается с момента передачи ведомому устройству шлюзом Modbus посылки от ведущего устройства. Если до истечения интервала шлюзом Modbus не будет получена ответная посылка от ведомого устройства, шлюз Modbus запишет сообщение об ошибке в системный журнал. Разрешённые значения: `1–10000`.

Значения по умолчанию

После добавления шлюза Modbus устанавливается значение 1500 мс (см. service mbgw add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric response-timeout 1800
```

service mbgw routing add

Добавить маршрут для маршрутизации устройства Modbus RTU в сети Ethernet.

Синтаксис

```
service mbgw name <имя шлюза> routing add <адрес устройства> ip <IP-адрес> [port <TCP-порт>]
[description <комментарий>] [request-timeout <интервал>] [response-timeout <интервал>]
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `<адрес устройства>` — адрес устройства Modbus, которое необходимо маршрутизировать в сети Ethernet (SlaveID). Разрешённые значения: `1–247`. Вы можете задать несколько адресов и (или) их диапазонов через запятую.
- `<IP-адрес>` — IP-адрес шлюза Modbus.
- `<TCP-порт>` — TCP-порт шлюза Modbus.
- `<комментарий>` — произвольный комментарий для описания подключения к Modbus-устройству. Длина: 1–64 символа. Разрешённые символы: `A–Z`, `a–z`, `0–9`, `- _ , .`
- `request-timeout <интервал>` — интервал времени в миллисекундах, выделенный на получение запроса от ведущего Modbus-устройства.
- `response-timeout <интервал>` — интервал времени в миллисекундах, выделенный на ожидание ответа от ведомого Modbus-устройства.

Значения по умолчанию

- Если TCP-порт не указан, используется TCP-порт, заданный для шлюза Modbus.
- Если интервал времени не указан, используется интервал, заданный для шлюза Modbus.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Маршрутизация используется при работе шлюза Modbus в режиме RTU to TCP.
- Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric routing add 12 ip 192.168.0.2 port 501 description
Node_1 request-timeout 1200 response-timeout 1800
```

service mbgw routing change

Изменить маршрут для устройства Modbus RTU.

Синтаксис

```
service mbgw name <имя шлюза> routing change <адрес устройства> [ip <IP-адрес>] [port
<TCP-порт>] [description <комментарий>] [request-timeout <интервал>] [response-timeout
<интервал>]
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `<адрес устройства>` — адрес устройства Modbus, маршрут которого необходимо изменить. Вы можете задать несколько адресов и (или) их диапазонов через запятую.
- `<IP-адрес>` — IP-адрес шлюза Modbus.
- `<TCP-порт>` — TCP-порт шлюза Modbus.
- `<комментарий>` — произвольный комментарий для описания подключения к Modbus-устройству. Длина: 1–64 символа. Разрешённые символы: `A-Z, a-z, 0-9, - _ , .`
- `request-timeout <интервал>` — интервал времени в миллисекундах, выделенный на получение запроса от ведущего Modbus-устройства.
- `response-timeout <интервал>` — интервал времени в миллисекундах, выделенный на ожидание ответа от ведомого Modbus-устройства.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Маршрутизация используется при работе шлюза Modbus в режиме RTU to TCP.
- Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).
- Если адреса устройств Modbus, указанные в параметре `<адрес устройства>`, уже входят в один из существующих маршрутов, эти адреса будут удалены из него и добавлены в изменяемый данной командой маршрут.

Пример использования

```
hostname# service mbgw name electric routing change 12 ip 192.168.0.2 port 501 description
Node_1 request-timeout 1200 response-timeout 1800
```

service mbgw routing delete

Удалить маршрут для устройства Modbus RTU.

Синтаксис

```
service mbgw name <имя шлюза> routing delete <адрес устройства>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.

- `<адрес устройства>` — адрес устройства Modbus, маршрут которого необходимо удалить. Вы можете задать несколько адресов и (или) их диапазонов через запятую.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Маршрутизация используется при работе шлюза Modbus в режиме RTU to TCP.
- При удалении адреса из диапазона адресов маршрут будет разделён на два маршрута до и после удалённого адреса устройства.
- Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric routing delete 14
```

service mbgw routing show

Просмотреть список маршрутизируемых устройств шлюза Modbus, работающего в режиме RTU to TCP.

Синтаксис

```
service mbgw name <имя шлюза> routing show
```

Параметры и ключевые слова

`<имя шлюза>` — имя шлюза Modbus.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service mbgw name electric routing show
Modbus gateway: electric
Serial Port: rs232
TCP port: 501
Request timeout (ms): 1500
```

```
Response timeout (ms): 1500

Slave ID    IP Address        TCP Port     Request    Response    Description

1           192.168.1.101     Default      Default    Default     TCP Slave 1
```

service mbgw serial

Выбрать другой последовательный интерфейс для шлюза Modbus.

Синтаксис

```
service mbgw name <имя шлюза> serial <последовательный интерфейс>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `<последовательный интерфейс>` — имя последовательного интерфейса из списка доступных. Если на интерфейсе уже настроен шлюз Modbus, интерфейс не отображается в списке.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Нельзя выбрать последовательный интерфейс, который уже используется другим шлюзом Modbus.
- Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric serial rs485
```

service mbgw show

Просмотреть настройки одного или всех шлюзов Modbus.

Синтаксис

```
service mbgw [name <имя шлюза>] show
```

Параметры и ключевые слова

`<имя шлюза>` — имя шлюза Modbus.

Значения по умолчанию

Если имя шлюза не указано, на экран будут выведены настройки всех шлюзов Modbus.

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> service mbgw show

Modbus gateway: "electric" is running

Modbus gateway autostart (mode): off

Modbus gateway type: tcp-to-rtu

Syslog level: 3

Serial Port: rs232

TCP Port: 501

TTY device speed: 115200

TTY device parity: even

Response timeout(ms): 1500

Request timeout(ms): 1500


Modbus gateway: "water001" is stopped

Modbus gateway autostart (mode): on

Modbus gateway type: tcp-to-rtu

Syslog level: 3

Serial Port: rs485

TCP Port: 502

TTY device speed: 115200

TTY device parity: even

Response timeout(ms): 1500

Request timeout(ms): 1500

Before send delay(ms): 10

After send delay(ms): 0
```

service mbgw start

Запустить один или все шлюзы Modbus.

Синтаксис

```
service mbgw [name <имя шлюза>] start
```

Параметры и ключевые слова

`<имя шлюза>` — имя шлюза Modbus.

Значения по умолчанию

Если имя шлюза не указано, будут запущены все шлюзы Modbus.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service mbgw name electric start
Modbus gateway electric serial rs232 is started
```

service mbgw stop

Остановить работу одного или всех шлюзов Modbus.

Синтаксис

```
service mbgw [name <имя шлюза>] stop
```

Параметры и ключевые слова

`<имя шлюза>` — имя шлюза Modbus.

Значения по умолчанию

Если имя шлюза не указано, будут остановлены все шлюзы Modbus.

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service mbgw name electric stop

Modbus gateway electric serial rs232 is stopped
```

service mbgw syslog-level

Изменить уровень важности событий, записываемых в системный журнал, для одного или всех шлюзов Modbus.

Синтаксис

```
service mbgw [name <имя шлюза>] syslog-level <уровень важности>
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus;
- `<уровень важности>` — уровень важности событий, записываемых в системный журнал. Возможные значения:
  - `0` — критические события (critical);
  - `1` — ошибки (error);
  - `2` — предупреждения (warning);
  - `3` — важные события (notice);
  - `4` — информационные события (info);
  - `5` — отладочные события (debug).

  Каждый последующий уровень включает в себя предыдущие.

Значения по умолчанию

- В системный журнал записываются события не выше 3-го уровня (`3`).
- Если имя шлюза не указано, настройка выполняется для всех шлюзов Modbus.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед изменением уровня важности для шлюза Modbus остановите его работу (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric syslog-level 2

Syslog-level 2 successfully set for Modbus gateway electric serial rs232.
```

service mbgw type

Изменить режим работы шлюза Modbus.

Синтаксис

```
service mbgw name <имя шлюза> type {tcp-to-rtu | rtu-to-tcp}
```

Параметры и ключевые слова

- `<имя шлюза>` — имя шлюза Modbus.
- `tcp-to-rtu` — режим работы TCP to RTU.
- `rtu-to-tcp` — режим работы RTU to TCP.

Значения по умолчанию

После добавления шлюза Modbus устанавливается режим TCP to RTU (см. service mbgw add).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды остановите работу шлюза Modbus (см. service mbgw stop).

Пример использования

```
hostname# service mbgw name electric type rtu-to-tcp
```

service piomonitor mode

Включить или выключить автоматический запуск службы `piomonitor` при загрузке ViPNet Coordinator IG.

Синтаксис

```
service piomonitor mode {on | off}
```

Параметры и ключевые слова

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

Значения по умолчанию

Автоматический запуск выключен (`off`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу сервиса GPIO (см. service piomonitor stop).

Пример использования

Чтобы включить автоматический запуск службы `piomonitor`:

```
hostname# service piomonitor mode on
```

service piomonitor reset

Отключить отслеживание пользовательских событий на контактах интерфейса GPIO.

Синтаксис

```
service piomonitor reset
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- После выполнения команды на всех контактах будет отключено отслеживание события типа `custom` и будет задан уровень сигнала, противоположный заданному командой service piomonitor set activelevel.
- Если на выходных контактах с включенным отслеживанием события `custom` также включено отслеживание других событий, то будет задан уровень сигнала, соответствующий всем событиям, для которых включено отслеживание.

Пример использования

Чтобы отключить отслеживание пользовательских событий на всех контактах интерфейса GPIO:

```
hostname# service piomonitor reset
```

service piomonitor set activelevel

Задать активный уровень сигнала для контакта GPIO, который будет определять срабатывание обработчика.

Синтаксис

```
service piomonitor set {In | Out} activelevel { 0 | 1 }
```

Параметры и ключевые слова

- `In` — входные контакты GPIO;
- `Out` — выходные контакты GPIO;
- `0` — обработчик будет срабатывать при изменении уровня сигнала на контакте GPIO с 1 на 0;
- `1` — обработчик будет срабатывать при изменении уровня сигнала на контакте GPIO с 0 на 1.

Значения по умолчанию

- Для входных контактов (`In`) значение по умолчанию равно `0`.
- Для выходных контактов (`Out`) значение по умолчанию равно `1`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу сервиса GPIO (см. service piomonitor stop).

Пример использования

Чтобы задать активный уровень сигнала `1` для входного контакта GPIO:

```
hostname# service piomonitor set In activelevel 1
```

service piomonitor set In custom

Настроить пользовательскую обработку входящего сигнала на интерфейс GPIO от внешнего устройства.

Синтаксис

```
service piomonitor set In custom {button | switch}
```

Параметры и ключевые слова

- `button` — если внешнее устройство — кнопка;
- `switch` — если внешнее устройство — двухпозиционный переключатель.

Значения по умолчанию

Настроена обработка сигнала от внешнего источника типа «кнопка» (`button`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу сервиса GPIO (см. service piomonitor stop).

Пример использования

Чтобы включить обработку сигнала, входящего на контакт `In` от внешнего устройства типа «кнопка»:

```
hostname# service piomonitor set In custom button
```

service piomonitor set In emergency

Настроить обработку сигнала от внешнего устройства для перевода ViPNet Coordinator IG в специальный режим работы.

Синтаксис

```
service piomonitor set In emergency {button | switch}
```

Параметры и ключевые слова

- `button` — если внешнее устройство, которое вы используете для перевода ViPNet Coordinator IG в специальный режим работы, — кнопка;
- `switch` — если внешнее устройство, которое вы используете для перевода ViPNet Coordinator IG в специальный режим работы, — двухпозиционный переключатель.

Значения по умолчанию

Настроена обработка сигнала от внешнего устройства типа «кнопка» (`button`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Выполнение команды возможно только в том случае, если ViPNet Coordinator IG работает как межсетевой экран типа «Д».
- Перед выполнением команды завершите работу сервиса GPIO (см. service piomonitor stop).

Пример использования

Чтобы включить обработку входящего сигнала на контакт `In` от внешнего устройства типа «кнопка» для перевода ViPNet Coordinator IG в специальный режим работы:

```
hostname# service piomonitor set In emergency button
```

service piomonitor set In tamper

Настроить обработку интерфейсом GPIO сигнала от датчика вскрытия внешнего шкафа.

Синтаксис

```
service piomonitor set In tamper
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу сервиса GPIO (см. service piomonitor stop).

Пример использования

Чтобы настроить для контакта `In` обработку сигнала от датчика вскрытия внешнего шкафа:

```
hostname# service piomonitor set In tamper
```

service piomonitor set Out cluster

Настроить отправку на контакт GPIO исходящего сигнала, соответствующего текущему режиму работы ViPNet Coordinator IG в кластере.

Синтаксис

```
service piomonitor set Out cluster
```

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Если команда выполняется на активном узле кластера, то на выходном контакте будет задан сигнал, соответствующий заданному командой service piomonitor set activelevel.
- Если команда выполняется на пассивном узле кластера, то на выходном контакте будет задан сигнал, противоположный заданному командой service piomonitor set activelevel.
- Команда не может быть выполнена при включенном контроле событий ViPNet Coordinator IG (см. service piomonitor set Out event).
- Перед выполнением команды завершите работу сервиса GPIO (см. service piomonitor stop).

Пример использования

Чтобы включить отправку исходящего сигнала, соответствующего текущему режиму работы ViPNet Coordinator IG в кластере, на контакт `Out`:

```
hostname# service piomonitor set Out cluster
```

service piomonitor set Out event

Настроить отправку сигнала на контакт GPIO о наступлении одного из событий, отслеживаемых ViPNet Coordinator IG.

Синтаксис

```
service piomonitor set Out event {on | off} { custom | restricted | service | emergency
| tamper }
```

Параметры и ключевые слова

- `on` — отправлять сигнал о наступлении события.
- `off` — не отправлять сигнал о наступлении события.
- `custom` — поступление на входной контакт GPIO любых необрабатываемых сигналов.
- `restricted` — переход в режим ограниченного функционирования.
- `service` — переход в режим регламентного обслуживания.
- `emergency` — переход в специальный режим работы.
- `tamper` — срабатывание датчика вскрытия внешнего шкафа.

Значения по умолчанию

Включена сигнализация (`on`) о поступлении на входной контакт GPIO любых необрабатываемых сигналов (`custom`).

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- При каждом выполнении команды вы можете включить или выключить сигнализацию только одного события. Чтобы включить сигнализацию нескольких событий, выполните команду последовательно несколько раз.
- Выполнение команды невозможно, если настроена отправка сигнала, соответствующего текущему режиму ViPNet Coordinator IG в кластере (см. service piomonitor set Out cluster).
- Перед выполнением команды завершите работу службы piomonitor (см. service piomonitor stop).

Пример использования

Чтобы включить отправку сигнала о срабатывании датчика вскрытия внешнего шкафа:

```
hostname# service piomonitor set Out event on tamper
```

service piomonitor set syslog-level

Изменить уровень важности событий интерфейса GPIO, записываемых в системный журнал.

Синтаксис

```
service piomonitor set 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);
- `5` — детализированные отладочные события (deep).

Каждый последующий уровень включает в себя предыдущие.

Значения по умолчанию

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

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу сервиса GPIO (см. service piomonitor stop).

Пример использования

Чтобы записывать в системный журнал события интерфейса GPIO не выше 4-го уровня:

```
hostname# service piomonitor set syslog-level 4
```

service piomonitor show

Просмотреть параметры настройки интерфейса GPIO.

Синтаксис

```
service piomonitor show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

Если работа сервиса GPIO остановлена (см. service piomonitor stop), то значения параметров `piomonitor active events` и `Pin current state` не выводятся.

Пример использования

Чтобы просмотреть текущие параметры настройки интерфейса GPIO:

```
hostname# service piomonitor show
piomonitor status: running
piomonitor mode: on
piomonitor syslog level: 3
piomonitor pins configuration:
------------------------------
Pin name: In
Pin type: in
Pin active level: 1
Pin mode: emergency button
------------------------------
Pin name: Out
Pin type: out
Pin active level: 1
Pin mode: event
Pin events: custom, service
------------------------------
```

service piomonitor start

Запустить службу `piomonitor`.

Синтаксис

```
service piomonitor start
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service piomonitor start
```

service piomonitor stop

Остановить службу `piomonitor`.

Синтаксис

```
service piomonitor stop
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service piomonitor stop
```

service usbmodem set syslog-level

Изменить уровень важности событий для службы управления модемом, записываемых в системный журнал.

Синтаксис

```
service usbmodem set 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.

Значения по умолчанию

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

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Перед выполнением команды завершите работу сервиса управления модемом.

Пример использования

Чтобы записывать в системный журнал события службы управления модемом не выше 4-го уровня:

```
hostname# service usbmodem set syslog-level 4
System log level successfully set.
```

service usbmodem show config

Просмотреть уровень важности событий службы управления модемом, записываемых в системный журнал.

Синтаксис

```
service usbmodem show config
```

Режимы командного интерпретатора

Режим настройки.

Пример использования

```
hostname# service usbmodem show config
System log level: 4
```

service usbmodem show status

Просмотреть состояние модема, объём переданного трафика и другие параметры.

Синтаксис

```
service usbmodem show status
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- В исполнениях ViPNet Coordinator IG, поддерживающих две SIM-карты, выводится информация только по текущей используемой SIM-карте.
- По команде на экран выводится следующая информация:
  - Состояние модема.
  - Производитель и модель модема.
  - Идентификатор устройства (PID) и идентификатор производителя (VID).
  - Номер SIM-карты.
  - Международный идентификатор мобильного оборудования (IMEI).
  - Коды MCC и MNC.
  - Частота, на которой работает модем.
  - Тип мобильной сети.
  - Качество сигнала.
  - Температура модема.
  - Напряжение.
  - Оператор мобильной связи.
  - Объём переданного трафика.
  - Количество перезагрузок модема по причине сбоя модема или большого количества попыток соединения.
  - Количество перезагрузок модема по причине отсутствия ответного трафика.
  - Идентификатор SIM-карты.
  - Количество попыток ввода PIN-кода до блокировки SIM-карты.
  - Страна оператора мобильной связи.
  - Наименование оператора мобильной связи.
  - Интерфейс модема.
  - Ошибка (при наличии).

Пример использования

```
hostname> service usbmodem show status
Modem software: stopped
Manufacturer/Model: Quectel UC20
Modem PID and VID: 05c6:9003
SIM 1
IMEI: 35-419002-389644-3
MCC/MNC: 250/02
band used: WCDMA 2100
Mobile network type: 3G
Signal Quality: -89 dBm [great]
Temperature : 49.5 C
Voltage: 3.5 V
Fact of operator network connection: MegaFon
How many bytes were transmitted (Rx/Tx): 65/101
Resets and Communication Breaks: 5
Traffic Breaks: 0
Modem active SIM IMSI:
SIM password enteres left: 3
SIM country: ru
SIM provider: Megafon
Modem network interface: ppp0
Modem error code: 0
```

service vpn mode

Включить или выключить автозапуск подсистемы VPN при перезагрузке ViPNet Coordinator IG.

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 IG.

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 IG 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 IG с источником бесперебойного питания (ИБП).



Примечание. Команды группы `ups` доступны только для исполнения ViPNet Coordinator IG1000 Q1.

ups set driver

Выбрать драйвер `UPS`.

Синтаксис

```
ups set driver <драйвер>
```

Параметры и ключевые слова

`<драйвер>` — название драйвера. В текущей версии ViPNet Coordinator IG 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 IG 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 IG 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 IG 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 IG 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 IG с ИБП.

Синтаксис

```
ups stop
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Пример использования

```
hostname> ups stop
```

Команды группы user

Управление доступом локального аудитора `user`.

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 PIN-код администратора USB-токена, затем введите и подтвердите PIN-код пользователя (требования к PIN-кодам 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 IG 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 достаточно изменить пароль только на активном узле. Если узлы кластера переключились до того, как активный узел передал новый пароль на пассивный, доступ на узел, который стал активным, вы можете получить по старому паролю.

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 достаточно сбросить пароль только на активном узле. Если узлы кластера переключились до того, как активный узел передал информацию на пассивный, выполните команду на узле, который стал активным.

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
```

Команды группы vpn

Управление копиями конфигураций VPN.

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 IG, 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 IG, 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 5.2.0, full, saved on 13.03.2025 at 20:06, never loaded
```

vpn config load

Загрузить настройки ViPNet Coordinator IG из копии конфигурации VPN.

Синтаксис

```
vpn config load <имя> [<версия>]
```

Параметры и ключевые слова

- `<имя>` — имя копии конфигурации VPN.
- `<версия>` — версия ПО ViPNet Coordinator IG, к которой относится копия конфигурации VPN. Указывается в формате `Major.Minor.Subminor`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

- Перед выполнением команды остановите службы `iplircfg`, `failoverd`, `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.

Пример использования

Чтобы загрузить настройки из копии конфигурации VPN с именем `Rollback_config`, относящейся к версии `5.2.0`:

```
hostname# vpn config load Rollback_config 5.2.0
```

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 `iplircfg`, `failoverd`, `mftpd`.
- В имени можно использовать только символы латинского алфавита, цифры, знаки «дефис» и «подчёркивание».
- Если в списке сохранённых копий конфигурации VPN есть копия с указанным именем, то запрашивается подтверждение на перезапись.

- Копия конфигурации VPN содержит 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
```

Команды группы webui

Настройка и управление службой веб-интерфейса ViPNet Coordinator IG.

webui https-cert

Выбрать сертификат для доступа к ViPNet Coordinator IG 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

- Команда доступна только для исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.
- Если в хранилище нет указанного сертификата, отображается список доступных для выбора сертификатов.
- Если в момент установки сертификата для доступа к ViPNet Coordinator IG 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

- Команда доступна только для исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.
- По команде выводятся:
  - Статус службы — запущена или остановлена.
  - Протокол для доступа к ViPNet Coordinator IG 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 webuicert.pem
Port 8080
```

webui port

Задать TCP-порт для доступа к ViPNet Coordinator IG 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

- Команда доступна только для исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.
- Если TCP-порт используется другой службой ViPNet Coordinator IG — выводится сообщение `Port in use. Release port or select another.`
- После изменения TCP-порта:
  - Измените в сетевом фильтре `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 IG 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

- Команда доступна только для исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.
- До переключения протокола с HTTP на HTTPS установите сертификат.

- 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 IG:
  - 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

- Команда доступна только для исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.
- Новый сертификат назначается действующим для подключения к веб-интерфейсу ViPNet Coordinator IG 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 неё 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.

Особенности использования

Команда доступна только для исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.

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>
```

hardware-status show

Просмотреть информацию о состоянии процессора, модема и памяти.

Синтаксис

```
hardware-status show
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Команда доступна для исполнений ViPNet Coordinator IG10 и ViPNet Coordinator IG100.
- По команде отображаются:
  - Дата и время последнего перегрева процессора.
  - Дата и время последнего перегрева модема.
  - Количество повреждённых блоков основной памяти, дата и время последнего повреждения.
  - Количество аномальных отключений дополнительной памяти, дата и время последнего отключения.
- Время отображается в системе UTC.

Пример использования

```
hostname> hardware-status show
Temperature of the processor is exceeded: true (Last Date: 21.04.2020 02:23:22)
Temperature of the modem is exceeded: true (Last Date: 21.04.2020 02:23:22)
Main disk bad-blocks: 12323 (Last Date: 07.08.2018 02:23:22)
Second disk failures: 10 (Last Date: 07.08.2018 02:23:22)
```

hardware-status show memory

Просмотреть состояние дисковой памяти ViPNet Coordinator IG.

Синтаксис

```
hardware-status show memory
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

- Команда доступна для исполнений ViPNet Coordinator IG10 и ViPNet Coordinator IG100.
- Команда отображает состояние основной и дополнительной памяти. Некоторые аппаратные платформы могут содержать только основную память (подробнее см. документ «Описание аппаратных платформ»).
- Перечень отображаемых параметров зависит от типа памяти:
  - NAND:

Наименование	Описание
capacity	Объём
bad-blocks	Количество повреждённых блоков, дата и время последнего повреждения

  - eMMC:

Наименование	Описание
capacity	Объём
Device Life Time Estimation (MLC) [269]	Здоровье карты MLC
Device Life Time Estimation (SLC) [268]	Здоровье карты SLC
Pre EOL information (EOL - End Of Limit) [267]	Процент использования зарезервированных блоков

  - SD:

Наименование	Описание
capacity	Общий объём, количество и объём секторов
Flash ID	Идентификатор устройства
IC version	Версия интегральной схемы
FW Version	Версия прошивки
CE Number	Идентификатор CE

Наименование	Описание
card classes	Класс карты
erase_size	Размер блока записи
version	Версия
manufacturer	Производитель карты
product	Идентификатор продукта
serial	Серийный номер
manfacturing date	Дата производства
Bad Block Replace Maximum	Допустимое количество повреждённых блоков (если поддерживается SD-картой)
Bad Block count per Die	Количество повреждённых блоков (указано для каждой из 8-ми или 16-ти микросхем памяти)
Good Block Rate (%)	Процент неповреждённых блоков
Total Erase Count	Общее количество циклов стирания
Endurance (Remain Life) (%)	Остаточный ресурс
Power Up Count	Количество включений
Abnormal Power Off Count	Количество выключений с ошибками
Total Refresh Count	Общее количество обновлений

Пример использования

Для исполнения ViPNet Coordinator IG с основной памятью типа NAND и дополнительной памятью типа SD:

```
hostname> hardware-status show memory
Main disk:
type: 'NAND'
capacity: 512M
bad-blocks: 12323 (Last Date: 07.08.2018 02:23:22)

Secondary disk:
type: 'SD'
capacity: 3.7G

Read S.M.A.R.T  Data Section
#Attribute_name: Value
Flash ID: 45-DE-94-98-72-51-00-00-00
IC version: 2702
FW Version: 0613
CE Number: 02
card classes: 10 switch, 8 application specific, 4 block write, 2 block read, 0 basic,
```

```
erase_size: 512
version: SD 3.0x
manufacturer: 'TRANSCEND'
product: 'USDU1' 2.0
serial: 0x28010943
manfacturing date: 2018 mar
Bad Block Replace Maximum: 0
Bad Block count per Die: 8 0 0 0 0 0 0 0
Good Block Rate(%): 100
Total Erase Count: 689576
Endurance (Remain Life) (%): 97
Power Up Count: 304
Abnormal Power Off Count: 1
Total Refresh Count: 65278
```

Для исполнения ViPNet Coordinator IG с основной памятью типа NAND и дополнительной памятью типа eMMC:

```
Main disk:
type: 'NAND'
capacity: 16G
bad-blocks: 12323 (Last Date: 07.08.2018 02:23:22)


Secondary disk:
type: 'eMMC'
capacity: 14G
Read S.M.A.R.T  Data Section

Device Life Time Estimation (MLC) [269]: 0x01 0% - 10% device life time used
Device Life Time Estimation (SLC) [268]: 0x01 0% - 10% device life time used
Pre EOL information [267]: 0x03 Urgent
```

license

Просмотреть лицензии ViPNet Coordinator IG.

Синтаксис

```
license
```

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде выводятся сведения:

- Лицензия:
  - Наименование исполнения ViPNet Coordinator IG, например `Coordinator IG10`, — основная лицензия.
  - `VPN` — лицензия на VPN.
  - `Failover` — лицензия на работу системы защиты от сбоев в режиме кластера.
  - `IPF` — лицензия на фильтрацию промышленных протоколов на прикладном уровне.
  - `Modbus Gateway` — лицензия на шлюз Modbus.
- Максимальная версия ПО ViPNet Coordinator IG, поддерживаемая лицензией.
- Состояние лицензии:
  - `active` — действует.
  - `expired` — не действует.
- Дата окончания действия лицензии в формате `YYYY-MM-DD`.

Пример использования

```
hostname> license

License object          Version    Status    Expiration date

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

IPF                     5.99       active    2024-01-11

VPN                     5.99       active    2024-01-11

Failover                5.99       active    2024-01-11

Modbus Gateway          5.99       active    2024-01-11

Coordinator IG100       5.99       active    2024-01-11
```

serial

Записать серийный номер в память ViPNet Coordinator IG.

Синтаксис

```
serial <серийный номер>
```

Параметры и ключевые слова

`<серийный номер>` — серийный номер, указанный на этикетке вашего ViPNet Coordinator IG. Длина: 4–18 символов. Разрешённые символы: `A–Z`, `a–z`, `0–9`, `-`.

Режимы командного интерпретатора

Режим настройки.

Особенности использования

Команда доступна на ViPNet Coordinator IG, серийный номер которых не был записан в память при производстве. Команду можно использовать повторно для корректировки введённого значения.

Пример использования

```
hostname# serial 431-24758

Appliance serial number successfully set.
```

version

Просмотреть текущую версию ViPNet Coordinator IG и его компонентов.

Синтаксис

```
version [full]
```

Параметры и ключевые слова

`full` — просмотр текущей версии всех компонентов, а также других параметров (набор функций, архитектура процессора).

Режимы командного интерпретатора

- Режим просмотра.
- Режим настройки.

Особенности использования

По команде отображаются название продукта и аппаратной платформы, серийный номер, лицензия и версия ПО.

Пример использования

```
hostname> version full

Product: ViPNet Coordinator IG

Platform: IG100 I1

Serial number: 202006027

License: IG100
```

```
Software version: 5.2.0-4060


WebGUI software version: 3.0.0.2270
VPN software version: 5.4.0-1
Iplir driver software version: 4.1.3
Watchdog driver software version: 1.0.5
Crypto driver version: NA
Crypto core version: NA
Feature set: base
Architecture: armv71
```

version features list

Просмотреть список функциональных модулей, входящих в состав текущей версии ViPNet Coordinator IG.

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 учётной 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 540

Файл iplir.conf-<интерфейс или группа интерфейсов> 553

Файл failover.ini 556

Файл mftp.conf 565

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 IG могут создаваться динамические интерфейсы, например, при подключении ViPNet Coordinator IG к сети 3G или Wi-Fi. В ViPNet Coordinator IG 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 IG 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 журнала службы `iplircfg` 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.

  Не рекомендуется задавать уровень важности выше `3` для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов ИнфоТеКС.

- `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: `off` (по умолчанию) или `on`. Если этот параметр установлен в значение `off`, то остальные параметры в данной секции игнорируются.
- `forward_id` — идентификатор сервера соединений для ViPNet Coordinator IG. С помощью сервера соединений ViPNet Coordinator IG 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 IG. Каждому узлу, с которым у ViPNet Coordinator IG есть связь, соответствует своя секция `[id]`. Первая секция соответствует собственным настройкам ViPNet Coordinator IG (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 IG.

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>`, где:



Примечание. Вручную в параметре `accessiplist` можно указать только IP-адрес узла или IP-адрес узла и метрику, остальные значения определяются системой автоматически в процессе работы управляющей службы.

- `<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 IG.
  - `manual` — задан администратором вручную (редактированием файла конфигурации VPN).
  - `addrdoc` — взят из справочников, полученных из ViPNet Prime.

- `blockforward` — включение или выключение блокирования транзитных пакетов, передаваемых через ViPNet Coordinator IG узлу ViPNet, связанному с ним. Используется только в секциях `[id]`, описывающих настройки узлов ViPNet, связанных с ViPNet Coordinator IG. 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` — доменное имя координатора, которое используется для восстановления соединения в случае смены его IP-адреса доступа (параметр `firewallip`). В собственной секции `[id]` параметр используется для задания доменного имени ViPNet Coordinator IG, а в любой секции `[id]`, кроме собственной — для задания доменного имени координатора, связанного с ViPNet Coordinator IG. Значение параметра присваивается автоматически ViPNet Prime и может быть изменено вручную администратором ViPNet Coordinator IG. При этом, если впоследствии администратор сети ViPNet изменит значение параметра в ViPNet Prime, оно будет присвоено несмотря на изменения, сделанные администратором ViPNet Coordinator IG.

Доменное имя, заданное в параметре, должно быть зарегистрировано на DNS-сервере (корпоративном или любом другом, публично доступном). Чтобы ViPNet Coordinator IG был доступен по доменному имени, назначьте ему дополнительное доменное имя в ViPNet Prime и затем отправьте на ViPNet Coordinator IG 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` — режим работы узла, находящегося за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр. Возможные значения:
  - в собственной секции:
    - `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» (если в собственной секции `[id]` параметр `usefirewall` установлен в `on`);
  - в любой секции `[id]`, кроме собственной:
    - `0xfffffffe` — при работе в режимах «Со статической трансляцией адресов» или «С динамической трансляцией адресов», если ViPNet Coordinator IG является сервером соединений для узла;
    - идентификатор координатора — при работе в режиме «С динамической трансляцией адресов». Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`.
- `tcptunnelport` — порт координатора для входящих соединений по протоколу TCP. Возможные значения: от 0 до 65535, значение по умолчанию 443. Заданный порт используется для работы TCP-туннеля (см. параметр `tcptunnel_establish` секции `[misc]` (см. Секция [misc])).

Если параметр задан, то он автоматически рассылается на клиенты, для которых данный координатор служит сервером соединений.



Примечание. Если порт 80 уже используется, в параметре `tcptunnelport` рекомендуется указать другой порт. Иначе TCP-туннель будет выключен.

- `tunnel` — адреса узлов, туннелируемых ViPNet Coordinator IG (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>`. Они используются вместо реальных адресов туннелируемых узлов, если на узле, который к ним обращается, настроена видимость по виртуальным адресам. Например, в случае, когда 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]` (см. Секция [misc]), который может принимать одно из двух значений:

- `auto` — параметры `<ip1>` и `<ip2>` задаются администратором сети ViPNet в ViPNet Prime или вручную на ViPNet Coordinator IG.

  Например, чтобы в автоматическом режиме указать, что координатор туннелирует адреса с 192.168.0.1 по 192.168.0.100, сделайте следующую запись:

  ```
  tunnel = 192.168.0.1-192.168.0.100
  ```

- `manual` — 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, сделайте 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]` (см. Секция [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` — 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
  ```

  Используется в любой секции `[id]`, кроме собственной. В одной секции 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` — позволяет исключать IP-адреса узлов, туннелируемых другим координатором, из списка туннелируемых адресов, известных ViPNet Coordinator IG. В результате ViPNet Coordinator IG будет обращаться к таким узлам, как к открытым. Параметр задаётся в секциях `[id]` координаторов, связанных с ViPNet Coordinator IG. Возможные значения:
  - `on` (по умолчанию) — обращаться к узлам, туннелируемым другим координатором, через координатор, который их туннелирует.
  - `off` — обращаться к узлам, туннелируемым другим координатором, как к открытым. Рекомендуется использовать, если туннелируемый узел другого координатора находится в одной подсети с ViPNet Coordinator IG, и на туннелируемом узле не настроена маршрутизация до ViPNet Coordinator IG через туннелирующий координатор.
- `tunnelvisibility` — тип видимости для всех узлов, туннелируемых координатором:
  - `real` — всегда обращаться к туннелируемым узлам по их реальным адресам;
  - `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.

  Значение данного параметра по умолчанию определяется параметром `tunneldefault` секции `[visibility]` (см. Секция [visibility]).
- `usetunnel` — включает или выключает туннелирование незащищенных узлов координатором. Возможные значения: `on` (по умолчанию) или `off`. Если этот параметр на координаторе имеет значение `off`, то при соединении ViPNet Coordinator IG с узлами, которые туннелирует данный координатор, трафик шифроваться не будет. Используется в любой секции `[id]`, кроме собственной.
- `visibility` — тип видимости узла:
  - `real` — всегда обращаться к данному узлу по его реальному адресу.
  - `virtual` — всегда обращаться к данному узлу по его виртуальному адресу.

Примечание. Для узлов ViPNet, расположенных на мобильных устройствах, параметру `visibility` 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. Используйте параметр `visibility` 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 IG. Может принимать значение одного из реальных или виртуальных IP-адресов, в зависимости от физической топологии сети, режимов подключения к внешней сети ViPNet Coordinator IG 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 или установлено его значение `0.0.0.0`. В каждой секции `[id]` может быть только один такой параметр.
- `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:

- `be_dg_coordinator` — обнаружение ViPNet Coordinator IG другими координаторами в качестве шлюза по умолчанию:
  - `on` — включить;
  - `off` — выключить (по умолчанию);
  - `auto` — в соответствии с настройкой, заданной в ViPNet Prime.

  Обнаружить ViPNet Coordinator IG в качестве шлюза по умолчанию могут:
  - ViPNet Coordinator HW версии 5.3.0 и выше;
  - ViPNet Coordinator IG версии 5.2.0 и выше.
- `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 (alias) интерфейсов.
- `cef_port` — порт UDP для передачи сообщений CEF. Значение по умолчанию — `514`.
- `client_pollinterval` — период опроса координатора ViPNet Coordinator IG 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 IG). 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.

- `ompnumthreads` — количество ядер процессора, используемое для обработки служебных сообщений (по умолчанию — `1`).
- `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 только, 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_client` — включение или выключение функции TCP-клиента. Возможные значения: `on` или `off` (по умолчанию). Используется только если координатору назначена роль TCP-клиента.
- `tcptunnel_client_mode` — режим работы TCP-клиента. Возможные значения:
  - `auto` (по умолчанию) — автоматическое включение TCP-туннеля при пропадании UDP связи и выключение при её появлении.
  - `forced` — TCP-туннель устанавливается всегда, когда возможно, даже при доступе к серверу соединения по UDP.

  Используется только если координатору назначена роль TCP-клиента.
- `tcptunnel_client_port` — TCP-порт сервера, на который будут отправляться пакеты. Используется только если координатору назначена роль TCP-клиента. Значение по умолчанию: `443`.
- `tcptunnel_establish` — включение или выключение функции сервера TCP-туннелей. Возможные значения: `on` или `off` (по умолчанию). Для входящих соединений по протоколу TCP по умолчанию используется порт `443` — параметр `tcptunnelport` секции `[id]`.
- `tcptunnel_role` — роль координатора для функции TCP-туннеля. Возможные значения: `server` (сервер TCP-туннелей) или `client` (TCP-клиент). По умолчанию установлена роль `server`.
- `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]`.
- `udp_ports_count` — количество портов UDP. По умолчанию — 255 портов. Начальный порт диапазона задан в параметре `port` собственной секции `[id]` (по умолчанию — 55777).

`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 защищённых сетевых узлов, с которыми связан ViPNet Coordinator IG. В отличие от параметра `visibility`, с помощью которого в секциях [id] задаётся 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. Задаётся 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 служба iplircfg при запуске автоматически создает такой файл с параметрами по умолчанию.



Примечание. В ViPNet Coordinator IG по умолчанию разрешена работа динамических интерфейсов, которые входят в одну из следующих групп интерфейсов:

- `ppp` — группа интерфейсов для встроенных модемов;
- `wifi` — группа интерфейсов для WiFi.

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 ведётся свой журнал, 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 накапливаются в журнале IP-пакетов до тех пор, пока не будет достигнут максимальный размер журнала, 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, и затем при просмотре журнала можно узнать, сколько раз было зафиксировано событие, описываемое этой записью.

Секция `[db]` содержит следующие параметры:

- `maxsize` — максимальный размер журнала, Мбайт. Значение по умолчанию зависит от исполнения ViPNet Coordinator IG (см. machine logs settings network-traffic maxsize).

  Реальный размер журнала из-за наличия в нем служебного заголовка получается примерно на 1 Кбайт больше. Каждый раз при запуске управляющей службы 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 нём были записи, то просмотреть их будет невозможно.

- `timedif` — интервал времени, в течение которого одинаковые события объединяются в журнале в одну запись. Задаётся 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 IP-пакетах, проходящих через интерфейс. Возможные значения:

  - `off` — регистрируются только блокированные пакеты, а также изменение адресов сетевых узлов;
  - `on` — регистрируются все пакеты.

  Если параметр `registerall` отсутствует, включена регистрация IP-пакетов по сетевым фильтрам. Чтобы выключить регистрацию IP-пакетов по сетевым фильтрам, добавьте параметр `registerall` со значением `off` или `on`.

- `registerbroadcast` — включение или выключение регистрации записей о широковещательных пакетах. Возможные значения: `off` (по умолчанию) или `on`.

- `omittcpclientport` — включение или выключение скрытия информации о порте VPN-клиента 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 «События журнала IP-пакетов». Возможные значения: `off` или `on` (по умолчанию).

Секция [cef]

Секция `[cef]` содержит параметры:

- `event` — формирование сообщений CEF при регистрации IP-пакетов, проходящих через интерфейс:
  - `all` — для всех IP-пакетов;
  - `blocked` — для блокированных IP-пакетов (значение по умолчанию);
- `exclude` — формирование сообщений CEF, заданных в `event`, за исключением указанных номеров типов событий. Допускается перечисление номеров типов событий в любом порядке через запятую.

Файл failover.ini

Настройка параметров работы системы защиты от сбоев выполняется 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 в режиме кластера, должен быть описан секцией `[channel]`. Это необходимо для своевременного обнаружения прекращения работы интерфейса и переключения кластера.

Примечание. Параметры секций `[channel]` интерпретируются только при работе системы защиты от сбоев в режиме кластера.

Чтобы выключить контроль работоспособности какого-либо интерфейса, необходимо удалить из файла `failover.ini` соответствующую секцию `[channel]`.

Секция `[channel]` содержит следующие 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.

Для сетевого интерфейса с динамическим IP-адресом в качестве значения параметра необходимо указать ключевое слово `dynamic`.

- `channelgroup` — текстовая строка, идентифицирующая группу сетевых интерфейсов на узле кластера, которые используются в функции MultiWAN (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка функции MultiWAN»). Если на узле кластера настроено резервирование канала доступа в интернет, то для сетевых интерфейсов основного и резервного каналов должно быть задано одинаковое значение `channelgroup` в секциях `[channel]`. Система защиты от сбоев будет считать интерфейс работоспособным пока работает хотя бы один интерфейс с таким же параметром `channelgroup`. Иначе, при недоступности основного канала доступа в интернет, узлы кластера переключатся раньше, чем будет задействован резервный канал доступа в интернет.
- `checkonlyidle` — указание на необходимость проверки только неактивных интерфейсов. Возможные значения:
  - `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]`. Не поддерживается для беспроводных интерфейсов. 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 IG. Чтобы сбросить MAC-адреса, перезагрузите ViPNet Coordinator IG 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 службы `failover` 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.

  Не рекомендуется задавать уровень важности выше `3` для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов ИнфоТеКС.

- `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. Возможные значения:
  - `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.

Условия для синхронизации сессий прикладных протоколов:

- исполнение ViPNet Coordinator IG100 или ViPNet Coordinator IG1000;
- `syncalgtcp = yes` на обоих узлах кластера;
- `syncconnections = yes` на обоих узлах кластера.

- `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;
    - защищённые соединения по TCP-туннелям;
    - локальные соединения (открытые и защищённые соединения, в которых сетевой узел ViPNet Coordinator IG 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.

  Условия для синхронизации сетевых соединений в кластере:
  - исполнение ViPNet Coordinator IG100 или ViPNet Coordinator IG1000;
  - `syncconnections = 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 передаёт 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).

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`.

  Внимание! Не задавайте значение параметра `synctime` меньше `3`. Иначе ViPNet Coordinator IG не будет успевать обрабатывать пакеты синхронизации.
- `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 ViPNet Prime Policy Management);
  - 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.
- `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;
  - файл журнала пакетов промышленных протоколов;
  - 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`.

Секция [events]

Секция `[events]` определяет параметры световой индикации в ViPNet Coordinator IG. Редактировать эту секцию крайне не рекомендуется, так как это может привести к неработоспособности световой индикации ViPNet Coordinator IG.

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 IG может обмениваться данными с другими узлами. Каждому узлу, зарегистрированному за ViPNet Coordinator IG в ViPNet Prime (координатор является сервером IP-адресов), а также каждому координатору, с которым есть межсерверный канал связи, соответствует своя секция `[channel]`.



Внимание! Секции `[channel]` добавляются и удаляются 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.

  Не рекомендуется задавать уровень важности выше `3` для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов ИнфоТеКС.

- `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.2025.09.23`.

- `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 сохраняться 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 IG.
- `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 IG.

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

Термины и сокращения

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг интернета.

TCP-туннель настраивается на координаторе, который является для клиента сервером соединений.

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 Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в нее устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

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.

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.

Динамический сетевой интерфейс

Разновидность сетевого интерфейса, который добавляется в процессе работы при наступлении некоторого события (например, при подключении встроенного модема, предоставляющего данный интерфейс).

Динамические интерфейсы объединяются в группы по типу интерфейса. Поэтому иногда может встречаться термин «групповой динамический интерфейс».

Существуют следующие группы динамических интерфейсов:

- `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
- `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi через встроенный интерфейс `wlan0` (для исполнений ViPNet Coordinator IG со встроенным модулем Wi-Fi).

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных ViPNet Coordinator IG, один из которых (активный) выполняет функции координатора сети ViPNet, а другой (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet Coordinator IG на активном ViPNet Coordinator IG, пассивный ViPNet Coordinator IG переключается в активный режим для выполнения функций. При этом сбойный ViPNet Coordinator IG перезагружается и становится пассивным.

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 обновлений

Ключи защиты обновлений обеспечивают безопасное удаленное обновление ключей обмена из ключевого центра ViPNet Prime и их хранение в ViPNet Coordinator IG.

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 IG 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.

Открытый узел

Узел без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенный в сети «за координатором».

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.

Реальный IP-адрес

IP-адрес, назначенный сетевому интерфейсу компьютера в локальной сети или интернете.

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 функцию сервера соединений выполняет координатор, назначенный 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 защищённых узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

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 программного обеспечения ViPNet, предназначенный для обмена информацией в 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.

Шлюз Modbus

Программно-аппаратная функциональность, выполняющая преобразование трафика интерфейса Ethernet в интерфейсы RS-232 и RS-485 и обратно для обеспечения взаимодействия Ethernet- и Modbus-устройств.

Шлюзовой координатор

Координатор, через который происходит 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.