



ViPNet Coordinator KB 4

Справочник команд и
конфигурационных файлов

Версия продукта: 4.3.3

© АО «ИнфоТеКС», 2024

ФРКЕ.465614.001РЭЗ

Версия продукта 4.3.3, документ обновлен 28.02.2024

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.

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

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.....	12
О документе.....	13
Соглашения документа	14
Обратная связь.....	15
 Глава 1. Справочник команд	16
Команды группы admin.....	17
admin config delete.....	17
admin config list.....	17
admin config load	18
admin config save	19
admin export dnsd log	20
admin export keys binary-encrypted usb	21
admin export logs usb.....	22
admin export packetdb usb	23
admin export-and-clear logs usb.....	24
admin keys remove.....	25
admin keys update.....	25
admin passwd	26
admin show check integrity status	27
admin show dnsd log.....	28
admin show dsdrnet.....	29
admin ssh reset-key.....	29
admin ssh reset-key local	30
admin ssh show-key	32
admin update-dsdr	33
admin upgrade software usb.....	34
Команды группы alg	35
alg module process off.....	35
alg module process on	35
alg restart.....	36
alg show	37
Команды группы failover.....	38
failover config edit	38
failover config mode	38

failover show active-mac-address.....	39
failover show config.....	40
failover show info	41
failover start	42
failover stop	43
failover view	43
Команды группы firewall.....	45
firewall add	45
firewall add name	48
firewall change append.....	49
firewall delete	51
firewall move rule	52
firewall object delete	53
firewall object show	53
firewall rules show	54
firewall show	56
Команды группы inet.....	58
inet bonding add mode slaves.....	58
inet bonding delete	60
inet clear mac-address-table	61
inet dgd configuration default	61
inet dgd configuration interval-time	62
inet dgd configuration response-time	63
inet dgd configuration retries-count	64
inet dgd configuration syslog-level	64
inet dgd mode	65
inet dgd next-hop add	66
inet dgd next-hop delete	67
inet dgd rule add action-priority.....	68
inet dgd rule add match-next-hop.....	69
inet dgd rule clear	70
inet dgd rule delete action-priority	70
inet dgd rule delete match-next-hop.....	71
inet dhcp client route-default-metric.....	72
inet dhcp client route-distance	72
inet dhcp relay add backup-interface	73
inet dhcp relay add external-interface	74
inet dhcp relay add listen-interface.....	75
inet dhcp relay delete backup-interface.....	76

inet dhcp relay delete external-interface	77
inet dhcp relay delete listen-interface.....	77
inet dhcp relay mode	78
inet dhcp relay reset.....	79
inet dhcp relay start.....	80
inet dhcp relay stop	80
inet dhcp server add default-lease-time	81
inet dhcp server add dns	82
inet dhcp server add domain.....	83
inet dhcp server add host.....	84
inet dhcp server add interface.....	85
inet dhcp server add max-lease-time.....	86
inet dhcp server add ntp	87
inet dhcp server add option	88
inet dhcp server add range.....	89
inet dhcp server add relay-interface	90
inet dhcp server add router.....	91
inet dhcp server add subnet-mask.....	92
inet dhcp server add tftp	93
inet dhcp server add voip.....	94
inet dhcp server add wins	94
inet dhcp server delete default-lease-time	95
inet dhcp server delete dns	96
inet dhcp server delete domain	97
inet dhcp server delete host.....	98
inet dhcp server delete interface.....	99
inet dhcp server delete max-lease-time	100
inet dhcp server delete ntp.....	100
inet dhcp server delete option	101
inet dhcp server delete range.....	102
inet dhcp server delete relay-interface	103
inet dhcp server delete router	104
inet dhcp server delete subnet-mask	105
inet dhcp server delete tftp	105
inet dhcp server delete voip.....	106
inet dhcp server delete wins.....	107
inet dhcp server mode.....	108
inet dhcp server reset	109
inet dhcp server start	109

inet dhcp server stop.....	110
inet dns clients add.....	110
inet dns clients delete.....	111
inet dns clients list.....	112
inet dns forwarders add	112
inet dns forwarders delete	113
inet dns forwarders list.....	114
inet dns mode	114
inet dns start.....	115
inet dns stop.....	116
inet ifconfig address.....	116
inet ifconfig address add	117
inet ifconfig address delete	118
inet ifconfig bonding add.....	119
inet ifconfig bonding ad-select.....	119
inet ifconfig bonding delete.....	120
inet ifconfig bonding lacp-rate	121
inet ifconfig bonding miimon.....	122
inet ifconfig bonding primary.....	122
inet ifconfig bonding xmit-hash-policy	123
inet ifconfig class	124
inet ifconfig dhcp.....	125
inet ifconfig dhcp route-metric.....	126
inet ifconfig down	127
inet ifconfig mtu.....	128
inet ifconfig reset.....	129
inet ifconfig speed.....	130
inet ifconfig speed auto	131
inet ifconfig up.....	132
inet ifconfig vlan add	132
inet ifconfig vlan delete.....	133
inet ntp add	134
inet ntp delete.....	134
inet ntp list.....	135
inet ntp mode	136
inet ntp orphan.....	136
inet ntp start	137
inet ntp stop	138
inet ospf mode.....	138

inet ospf network add.....	138
inet ospf network delete.....	139
inet ospf redistribute add.....	140
inet ospf redistribute delete.....	141
inet ping	141
inet policy active	142
inet policy rule add match	143
inet policy rule add	145
inet policy rule clear	146
inet policy rule delete match	147
inet policy rule delete	148
inet route add	149
inet route clear.....	150
inet route delete.....	151
inet show dgd configuration.....	152
inet show dgd next-hop	153
inet show dgd rule	154
inet show dhcp client	155
inet show dhcp relay	156
inet show dhcp server.....	156
inet show dhcp server lease	157
inet show dns	158
inet show interface.....	159
inet show mac-address-table	160
inet show ntp.....	161
inet show ospf configuration	162
inet show ospf database.....	163
inet show ospf neighbour	164
inet show policy rule	165
inet show routing.....	166
inet show snmp	167
inet show snmp community	167
inet show vlan	168
inet snmp community ro	169
inet snmp community trap	169
inet snmp debug-level.....	170
inet snmp mode.....	171
inet snmp start.....	171
inet snmp stop.....	172

inet snmp trapsink.....	172
inet ssh.....	173
inet vlan comment add	174
inet vlan comment delete.....	174
Команды группы iplir.....	176
iplir adapter add.....	176
iplir adapter delete.....	177
iplir adapter traffic.....	177
iplir config.....	178
iplir info.....	179
iplir option get.....	180
iplir option set antispoofing	181
iplir option set block-fragmented-packets.....	182
iplir option set block-other-protocols.....	182
iplir option set cleanup-interval.....	183
iplir option set connection-ttl-ip	184
iplir option set connection-ttl-tcp	184
iplir option set connection-ttl-udp.....	185
iplir option set dynamic-ports.....	186
iplir option set dynamic-timeouts.....	186
iplir option set max-connections.....	187
iplir ping	188
iplir set l2overip interface.....	189
iplir set l2overip local-port.....	189
iplir set l2overip mac-ttl.....	190
iplir set l2overip mode.....	191
iplir set l2overip remote-port	191
iplir set l2overip remote-port delete	192
iplir set l2overip unsolicited-frames.....	193
iplir set thread-count	193
iplir show adapter.....	194
iplir show adapters.....	195
iplir show config.....	196
iplir show firewall status.....	196
iplir show key-info.....	198
iplir show keys-upgrade-log	199
iplir show l2overip	199
iplir show thread-count.....	200
iplir start	201

iplir stop.....	201
iplir view	202
Команды группы machine	204
machine halt	204
machine reboot	204
machine self-test.....	205
machine set dailyreboot mode	206
machine set dailyreboot time	207
machine set date.....	208
machine set hostname	209
machine set loghost	210
machine set session-timeout	211
machine set timezone.....	211
machine show dailyreboot.....	212
machine show date	213
machine show dnssd log	213
machine show dnssd log usb.....	214
machine show hostname.....	214
machine show loghost.....	214
machine show logs.....	215
machine show memory	216
machine show session-timeout	217
machine show timezone	217
machine show uptime.....	218
machine swap mode	218
machine swap set	219
Команды группы mftp	221
mftp config.....	221
mftp info.....	222
mftp show config.....	223
mftp start	223
mftp stop.....	224
mftp view	224
Команды группы ups	226
ups set driver	226
ups set mode.....	226
ups set monitoring.....	227
ups show config	228
ups show status	228

ups start.....	229
ups stop.....	230
Прочие команды	231
debug off	231
debug on.....	231
enable.....	232
exit	233
version features list	233
version.....	234
webui status.....	235
webui restart.....	235
who.....	236
Глава 2. Справочник конфигурационных файлов.....	237
Файл failover.ini	238
Секция [channel]	238
Секция [debug]	240
Секция [misc]	240
Секция [network]	241
Секция [sendconfig].....	242
Файл iplir.conf	245
Секция [adapter]	245
Секция [debug]	246
Секция [dynamic].....	246
Секция [id]	247
Секция [misc].....	253
Секция [servers].....	255
Секция [virtualip].....	255
Секция [visibility].....	256
Секция [packet-settings].....	256
Секция [protection]	257
Файл iplir.conf- <интерфейс>	259
Файл mftp.conf	262
Секция [channel]	262
Специфические параметры для канала MFTP	263
Секция [transport]	264
Секция [mailtrans]	264
Секция [journal].....	265
Секция [misc].....	266

Секция [debug]	268
Секция [reserv]	269
Секция [upgrade]	269
Приложение А. Термины и сокращения	270



Введение

О документе	13
Соглашения документа	14
Обратная связь	15

О документе

Документ содержит описание команд, доступных для выполнения в командном интерпретаторе программно-аппаратного комплекса ViPNet Coordinator KB 4 (далее — ViPNet Coordinator KB). В нем приведены синтаксис команд, руководство по использованию, а также примеры команд. Команды сгруппированы по первому слову, список групп и список команд внутри каждой группы упорядочены по алфавиту.

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

- `iplir.conf` — конфигурационный [файл управляющей службы](#).
- `iplir.conf`-<интерфейс или группа интерфейсов> — конфигурационные файлы сетевых интерфейсов ViPNet Coordinator KB.
- `failover.ini` — конфигурационный [файл системы защиты от сбоев](#).
- `mftp.conf` — [конфигурационный файл транспортного модуля MFTP](#).

Параметры в конфигурационных файлах используются для настройки ViPNet Coordinator KB. Некоторые параметры задаются программным обеспечением ViPNet Coordinator KB 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 KB. Изменять такие параметры вручную не следует, в данном документе они называются нередактируемыми и описаны в специальных подразделах.

Все операции по администрированию ViPNet Coordinator KB выполняются с помощью командного интерпретатора, который представляет собой программный интерфейс взаимодействия с ViPNet Coordinator KB.

Работа в командном интерпретаторе возможна при локальном подключении к ViPNet Coordinator KB в двух режимах:

- Режим администратора, который позволяет изменять настройки ViPNet Coordinator KB.
- Режим пользователя, который позволяет контролировать параметры работы ViPNet Coordinator KB.

Командный интерпретатор запускается автоматически после успешной аутентификации на ViPNet Coordinator KB. После запуска командный интерпретатор находится в режиме пользователя (доступен ограниченный набор команд управления, обозначается символом «>» в приглашении интерпретатора). Для управления ViPNet Coordinator KB требуется перейти из режима пользователя в режим администратора.

Соглашения документа

Обозначение	Описание
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, путь, фрагмент кода или команда в командной строке



Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены в режиме администратора, содержат приглашение с символом #. Например:
`hostname# команда`
- Команды, которые могут быть выполнены в режиме пользователя, содержат приглашение с символом >. Например:
`hostname> команда`
- Обязательные параметры, которые должны быть заданы, заключены в угловые скобки. Например:
`команда <параметр>`
- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:
`команда <обязательный параметр> [необязательный параметр]`
- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой. Например:
`команда {вариант-1 | вариант-2}`

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 компании ИнфоТеКС регулируется [политикой ответственного разглашения](#).

1

Справочник команд

Команды группы admin	17
Команды группы alg	35
Команды группы failover	38
Команды группы firewall	45
Команды группы inet	58
Команды группы iplir	176
Команды группы machine	204
Команды группы mftp	221
Команды группы ups	226
Прочие команды	231

Команды группы admin

Управление копиями конфигурации VPN, обновление ПО и выполнение других административных задач.

admin config delete

Удалить копию конфигурации VPN.

Синтаксис

```
admin config delete <имя> [<версия>]
```

Параметры и ключевые слова

- <имя> — имя копии конфигурации VPN;
- <версия> — версия ПО ViPNet Coordinator KB, к которой относится копия конфигурации VPN. Указывается в формате Major.Minor.Subminor.

Режимы командного интерпретатора

Режим администратора.

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# admin config delete Config_*  
Configuration 'Config_2023123' (version 2.0.0) deleted
```

admin config list

Просмотреть список сохраненных копий конфигурации VPN.

Синтаксис

```
admin config list
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Список сохраненных копий конфигурации VPN отображается в следующем формате:

```
"Name", Version, Type, saved on Date at Time, loaded at Date-load at Time-load
```

где:

- **Name** — имя копии конфигурации VPN. Имя автоматически сохраненной копии начинается со слова `autosave`.
- **Version** — версия ПО ViPNet Coordinator KB, 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# admin config list
```

```
"Config_1", version 4.3.3, full, saved on 13.03.2023 at 20:06, never loaded
```

admin config load

Загрузить (восстановить) настройки ViPNet Coordinator KB из копии конфигурации VPN.

Синтаксис

```
admin config load <имя> [<версия>]
```

Параметры и ключевые слова

- **<имя>** — имя копии конфигурации VPN.
- **<версия>** — версия ПО ViPNet Coordinator KB, к которой относится копия конфигурации VPN. Указывается в формате `Major.Minor.Subminor`.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Перед выполнением команды остановите службы `failoverd`, `iplircfg`, `mftpd`. После выполнения запустите их.
- При вводе имени работают автодополнение и подсказка, данные для подсказки берутся из текущего списка сохраненных копий конфигурации VPN.
- Если версия не указана и при этом имеется несколько копий конфигурации VPN с совпадающими именами, но различными версиями, то выводится список таких копий конфигурации с предложением указать версию для загрузки.
- Перед загрузкой настроек из копии конфигурации VPN запрашивается подтверждение для сохранения копии текущей конфигурации VPN. В случае подтверждения введите имя, под которым будет сохранена копия текущей конфигурации.
- Если текущая версия ПО ViPNet Coordinator KB ниже версии, указанной в команде, дополнительно подтвердите загрузку настроек из копии конфигурации VPN.

Пример использования

Чтобы загрузить настройки из копии конфигурации VPN с именем `Rollback_config`, относящейся к версии 4.3.3:

```
hostname# admin config load Rollback_config 4.3.3
```

admin config save

Сохранить копию текущей конфигурации VPN.

Синтаксис

```
admin config save <имя>
```

Параметры и ключевые слова

<имя> — имя копии конфигурации VPN.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Перед выполнением команды остановите службы `failoverd`, `iplircfg`, `mftpd`.

- В имени можно использовать только символы латинского алфавита, цифры, знаки «дефис» и «подчеркивание».
- Если в списке сохраненных копий конфигурации VPN есть копия с указанным именем, то запрашивается подтверждение на перезапись.
- Сохраненная копия конфигурации VPN включает в себя следующие конфигурационные файлы ПО ViPNet Coordinator KB:
 - `iplir.conf` и все файлы с именем, соответствующим маске `iplir.conf`-<интерфейс или группа интерфейсов>;
 - `failover.ini`;
 - `mftp.conf`;
 - сетевые фильтры;
 - справочники и ключи.

Пример использования

Чтобы сохранить копии текущей конфигурации VPN под именем `Rollback_config`:

```
hostname# admin config save Rollback_config
```

admin export dnsd log

Сохранить журнал СКЗИ на жесткий диск ViPNet Coordinator KB для последующей выгрузки на USB-носитель.

Синтаксис

```
admin export dnsd log
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда недоступна при работе в удаленной SSH-сессии.
- Чтобы экспортировать журнал СКЗИ на USB-носитель, выполните `admin export logs usb`.

Пример использования

```
hostname# admin export dnsd log
```

admin export keys binary-encrypted usb

Экспортировать [справочники](#), [ключи](#) и настройки ViPNet Coordinator KB на USB-носитель. Ключевая информация с установленного ключевого блокнота ДСДР не экспортируется.

Синтаксис

```
admin export keys binary-encrypted usb
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда недоступна при работе в удаленной SSH-сессии.
- Имя файла экспорта формируется по следующему шаблону:
<название ViPNet Coordinator KB>-<идентификатор узла>-<дата экспорта>-<время экспорта>.vbe,

где <название ViPNet Coordinator KB> — наименование аппаратной платформы без последних двух символов.
- Во избежание получения неработоспособного файла экспорта рекомендуем предварительно провести регламентное тестирование ViPNet Coordinator KB.
- Перед выполнением команды требуется завершить работу служб `iplircfg` (см. [iplir stop](#)) и `mftpd` (см. [mftp stop](#)).
- Необходимо дождаться сообщения с разрешением извлечь устройство прежде, чем извлечь USB-носитель из разъема.

Пример использования

```
hostname# iplir stop
Shutting down IpLir

hostname# mftp stop
Shutting down MFTP daemon

hostname# admin export keys binary-encrypted usb
Configuration file will be saved to /tmp/vipnet/kb-15ea000b-2017-05-09-10-30-00.vbe
Put kb-15ea000b-2017-05-09-10-30-00.vbe file onto USB drive.
Insert USB drive and press Enter
1) General USB Flash Disk partition 3839Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc1 was successfully mounted on /usb.
File kb-15ea000b-2017-05-09-10-30-00.vbe to be copied onto the USB drive.
File kb-15ea000b-2017-05-09-10-30-00.vbe was successfully copied onto the USB drive.
You may remove the USB drive.
```

admin export logs usb

Экспортировать файлы журналов, хранящиеся на жестком диске ViPNet Coordinator KB, на USB-носитель.

Синтаксис

```
admin export logs usb
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда недоступна при работе в удаленной SSH-сессии.
- Имя файла экспорта — `logs.tar.gz`.
- При выполнении команды будет запрошен пароль для журналов СКЗИ.
- Для того, чтобы на USB-носитель можно было выгрузить журнал событий СКЗИ, предварительно его необходимо сохранить на жестком диске ViPNet Coordinator KB.
- При просмотре архива журнала в Windows время создания архива может отличаться от реального времени. При этом время событий в журналах будет правильным. Это связано с особенностями работы разных ОС с системным временем.

Пример использования

Ниже приведен пример выполнения команды:

```
hostname# admin export logs usb
```

```
1) /var/log/journal_2023_01_22_15_27_15.dnsd
```

```
Select dnsd journals (Example: 1,2,4 OR 0 export all journals): 1
```

```
Enter the password of the journal:
```

```
tar: Removing leading '/' from member names
```

```
/var/log/atop
```

```
/var/log/boot.log
```

```
/var/log/dmesg.boot
```

```
/var/log/everything.log
```

```
/var/log/lastlog
```

```
/var/log/lighttpd/
```

```
/var/log/lighttpd/accesss.log
```

```
/var/log/lighttpd/error.log
```

```
/var/log/news/
```

```
/var/log/ntpstats/
```

```
/var/log/wtmp
```

```
Put logs.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/sdb1 as is
Partition /dev/sdb1 was successfully mounted on /usb.
File logs.tar.gz to be copied onto the USB drive.
File logs.tar.gz was successfully copied onto the USB drive.
You may remove the USB drive.
hostname#
```

admin export packetdb usb

Экспортировать журнал регистрации [IP-пакетов](#) на USB-носитель.

Синтаксис

```
admin export packetdb usb <имя>
```

Параметры и ключевые слова

<имя> — имя файла экспорта.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- При удаленном подключении по протоколу SSH установите в настройках SSH-клиента тип терминала VT100+.
- Перед экспортом сохраните журнал IP-пакетов в файл (iplr view).
- При вводе имени файла работает автодополнение и подсказка, данные для подсказки берутся из списка существующих файлов экспорта.

Пример использования

Чтобы экспортировать файл `ippacket`, в который сохранены записи журнала IP-пакетов:

```
hostname# admin export packetdb 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.

admin export-and-clear logs usb

Экспортировать файлы системного журнала, хранящихся на ViPNet Coordinator KB, на USB-носитель с последующим удалением их с ViPNet Coordinator KB.

Синтаксис

```
admin export-and-clear logs usb
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда недоступна в удаленной SSH-сессии.
- При выполнении команды будет запрошен пароль для журналов СКЗИ. Пароль не отображается при вводе.
- Если файл архива журнала событий СКЗИ отсутствует на жестком диске ViPNet Coordinator KB, то вам будет предложено создать его.
- При просмотре архива журнала в Windows время создания архива может отличаться от реального времени. При этом время событий в журналах будет правильным. Это связано с особенностями работы разных ОС с системным временем.

Пример использования

```
hostname# admin export-and-clear logs usb
1) /var/log/journal_dnspd_2020_07_22_15_27_15.dnspd
Select dnspd journals (Example: 1,2,4 OR 0 export all journals): 1
Enter the password of the journal:
You are about to export and remove logs from ViPNet Coordinator KB [Yes/No] :
Please insert the USB flash drive and press Y to continue [Yes/No] :
Insert the USB flash drive and press Enter
1) JetFlash Transcend 4GB partition 3825Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdb1 as vfat
Packing of log files in progress. Press -C to abort.
Stopping system log daemon: syslogd
vipnetsnmp [4197]: Failed to open...
Starting system log daemon: syslogd
Copying files logs_kb1000_... to /dev/sda1. Press -C to abort.
File logs_kb1000_...
Logs archive file integrity check successful.
Logs exported and removed from ViPNet Coordinator KB successfully.
```

admin keys remove

Удалить ключи, справочники и настройки ViPNet Coordinator KB, а также ключевой блокнот ДСДР.

Синтаксис

```
admin keys remove
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- После удаления ключевой информации выполните инициализацию ViPNet Coordinator KB.
- В удаленной SSH-сессии команда недоступна.
- Если на ViPNet Coordinator KB запущен DHCP-сервер, то его работа будет автоматически завершена.

Пример использования

```
hostname# admin keys remove
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 keys update

Обновить ключи и справочники на ViPNet Coordinator KB из дистрибутива ключей.

Синтаксис

```
admin keys update
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда используется, когда нет возможности обновить справочники и ключи удаленно из ViPNet Administrator.
- В удаленной SSH-сессии команда недоступна.
- Команда доступна для выполнения на активном и на пассивном узле кластера.

Пример использования

```
hostname# admin keys update
```

This command updates all VPN keys and cannot be reverted.

After VPN keys update all user sessions will be closed

All settings will be updated according to new dst file

All VPN service will be restarted

Are you sure you want to continue [Yes/No]: Yes

Warning! Failover is in cluster mode. If password in dst file and user password DO NOT MATCH - You MUST disable failover link and update keys on PASSIVE node first.

Would you like to install keys from USB or CD storage device [u/c] or press ctrl+C to abort : u

Insert USB storage device with DST file and press <Enter>

Try to mount /dev/sdc as vfat

Found several application initialization files:

1 - abn_0034.dst Coordinator

2 - abn_0012.dst Coordinator

Choose file by typing [1-2] or [q] to cancel. Or, press Enter to proceed to the next page:1

Type password:

Applying keys update.... Please wait.

Keys update completed.

admin passwd

Изменить пароль пользователя ViPNet Coordinator KB.

Синтаксис

```
admin passwd
```

Режимы командного интерпретатора

Администратор.

Особенности использования

- При выполнении команды требуется ввести текущий пароль пользователя или пароль администратора, затем дважды ввести новый пароль.
- При вводе пароля вводимые символы не отображаются.
- Минимальная длина нового пароля — 6 символов.
- Чтобы изменить пароль пользователя на ViPNet Coordinator KB, работающих в режиме кластера горячего резервирования, выполните команду сначала на узле, функционирующем в пассивном режиме, а затем на узле, функционирующем в активном режиме. Пароли, задаваемые на обоих узлах, должны совпадать.



Совет. Рекомендуется задавать сложные пароли, содержащие не менее 8 символов.

Пример использования

```
hostname# admin passwd
Enter either the current user password or the corrent administrator password:
Enter new user password:
Confirm the new user password:
The new password has been successfully set.
Dumping data files...
Data files were dumped successfully
hostname#
```

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 администратора.

Пример использования

```
hostname# admin show check integrity status
Sat Feb 13 02:18:31 2024
Periodic control passed successfully
```

admin show dnsd log

Просмотреть журнал СКЗИ.

Синтаксис

```
admin show dnsd log
```

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# admin show dnsd log

02-12-2023 10:28:37: Diagnose check on the periodical key, status: ok...
02-12-2023 10:27:44: Key event [checksums with PKKC checking]
02-12-2023 10:27:37: Diagnose check on the periodical key, status: ok...
02-12-2023 10:10:37: Key event [PKKC generation]
02-12-2023 10:10:31: Key event [random numbers generation]
02-12-2023 10:08:04: Key event [predefined generation]
02-12-2023 10:08:03: Diagnose check on the technological key, status: ok...
02-12-2023 10:06:04: Key event [checksums with TKKC generation]
02-12-2023 10:05:57: Diagnose check on the technological key, status: ok...
02-12-2023 10:05:50: Key event [TKKC generation]
02-12-2023 10:05:44: Key event [random numbers generation]
00-00-0 00:00:06: Diagnose check on the predefined key, status: ok...
00-00-0 00:00:00: DNSD module start
```

admin show dsdrnet

Вывести сведения о номере и серии [ключевых блокнотов ДСДР](#), используемых связанными узлами ViPNet Coordinator KB сети ViPNet.

Синтаксис

```
admin show dsdrnet
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Сведения отображаются следующем формате:

```
AAAAABBBBBB  CCCCCCCC
```

- AAAA — номер ключевого блокнота ДСДР.
- BBBBBB — номер серии ключевых блокнотов ДСДР.
- CCCCCCCC — идентификатор узла ViPNet Coordinator KB в сети ViPNet, на котором установлен ключевой блокнот ДСДР с номером AAAA из серии BBBBBB.

Пример использования

```
hostname# admin show dsdrnet
```

```
<SH_LOG> Command: admin show dsdrnet
```

```
0001888888  2890000C
```

```
0004888888  2890000D
```

```
0002888888  28900024
```

admin ssh reset-key

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

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 администратора.

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 KB.

Синтаксис

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

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# admin ssh reset-key local
```

```
command: admin ssh remove key local
```

```
Reseting DSA-Hostkey...
```

```
Generating public/private dsa key pair.
```

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

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

The key fingerprint is:

SHA256:TvshXJ9ybY3Rmoy2L8Pfut5JN0TpdLNuOkp3nuXaisw root@hostname

The key's randomart image is:

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

```
|          |
|          .|
|          *.|
|          . = =|
|          S. . + @.|
|          o .o + @ +|
|          o  = = Bo|
|          ..oBo*==*|
|          .oEBXO=|
```

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

Reseting RSA-Hostkey...

Generating public/private rsa key pair.

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

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

The key fingerprint is:

SHA256:Q6PlZVt8y5eEh+lnC3yuP5CS6u2P8H4CTkA3xyOFOEY root@hostname

The key's randomart image is:

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

```
|      .E. +.      |
|      = = =  +  |
|      o * * ++.o |
|      * + oooo..|
|      . S . .++=.|
|      + o o*..|
|      o.o . .o |
|      o+..... |
|      ..o*+o...|
```

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

admin ssh show-key

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

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 администратора.

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+JvG8GLQZvODJCnIKzWlJ2eUJi5/iVTOfBwHt9oXo+W+K4JaVwUaQq0uEHj6YbhPk6mIlV+TIBfCbSP5r9quQCFdnn4IKcVng7rVKudl8geMKW0GQGrotZl9pRAAAAFQC2iqrroLE+zS6qmAkM2x/iOCzeiQAAAIEAxBbdKDITotJDNykWYuCPnCgWZujXz0oUUxAOsp+dVYcsnevRN6IiM5lgTAUDRR5AKPkY7M5ma3EOXAZTrdKj+Y7NePt4smEQQat93L+nKgoNDjf+oUnQFh07XkK0eydX3/xCO0M+pn/VvICDjXP6DdpDmXr01Gy389wakaqHZX4AAACBAJYC9XgjKgnLRcKjmSVLuA/yZ/YFk3P0LJUmsRe4yzVl6v2uLlRH8rEfTGVllMWuDX47ZmRhpemoM3QbvKFAFMBkmbqZzrn8nFARLaoPlsyS2CO3gaEFkmeQ/d7rL7HRq05tH2e4gUX2ZxWJQHNYgprj8r5gKPWyN6zBCRJ0GF8U
```

Key type: ssh-rsa(ssh2)

Fingerprint: SHA256:Txn8IloRmfAbD+l/F6/UWah4DfwGu2cKXDGide5VXQk

Public key:

```
AAAAB3NzaC1yc2EAAAADAQABAAQDgRfTwzDnmXg3GCofsWFqOlh96opUuTz1zkPA1c70ncnyNtkW6kmaEXxMU3EM7r/yf3/e/U6JH5Pkc6bWcYbU70tEBY3db9ZDY/QdOBZdijIagUuWyiiHqAEWwC1vCXqQ1/0AZwh71DKTDPFIOcImTC3ahMJMtv1/X7SnWJVxVz3AMBqXnTqjMXOpHDXQnAgPw4kcTNqZMNT1OOvaYmcCGZ6Tko7HPygyln+ZUV/GajAlwTmCfKr0DT/O3ebi9OF7SK6A5eJeGCVBRv2BdOhL/uWzuaMSP6vMk+hiWkX01N16iOUIo4PCHW8kNm6FcaJAmG0MKVw8M2dDo0osTtUhZ
```

admin update-dsdr

Установить или обновить ключевой блокнот ДСДР.

Синтаксис

admin update-dsdr

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда недоступна при работе в удаленной SSH-сессии.
- Перед первичной установкой ключевого блокнота ДСДР на ViPNet Coordinator KB должен быть установлен [дистрибутив ключей](#). Установить ключевой блокнот ДСДР можно только в случае совпадения его серии и номера с информацией, указанной в справочнике, который был установлен в составе дистрибутива ключей. Подробнее о установке справочников и ключей см. в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора» в разделе «Установка справочников и ключей».
- Перед выполнением обновления ключевого блокнота ДСДР [администратор сети ViPNet](#) выпускает обновление справочников и ключей. В обновленном справочнике содержится информация о серии и номере нового ключевого блокнота ДСДР. Установить новый ключевой блокнот ДСДР можно только в случае совпадения его серии и номера с информацией, указанной в обновленном справочнике.

- В процессе выполнения команды связь с данным узлом будет потеряна. Связь восстановится после завершения обновления.

Пример использования

```
hostname# admin update-dsdr
```

```
DSDR will be updated. IPLIR and MFTP will be stopped Continue? [Yes, No]
```

admin upgrade software usb

Обновить ПО ViPNet Coordinator KB с USB-носителя.

Синтаксис

```
admin upgrade software usb
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда недоступна при работе в удаленной SSH-сессии.

Пример использования

```
hostname# admin upgrade software usb
Insert USB flash drive into empty USB slot and press <Enter>
Select file to use for software upgrade:
1 - /mnt/tmp/sdb1/driv.lzh
Enter file number [1-1] or [q] to cancel: 1
vupgrade    - Melted : o
This is kb platform
Stop VPN daemons
...
To apply upgrades reboot the computer
hostname#
```

Команды группы alg

Управление обработкой прикладных протоколов.

alg module process off

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

По умолчанию включена обработка всех прикладных протоколов.

Пример использования

Чтобы выключить обработку прикладного протокола DNS:

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

alg module process on

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

Синтаксис

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

Параметры и ключевые слова

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

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

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

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

alg restart

Перезапустить службу `algd`, отвечающую за обработку прикладных протоколов.

Синтаксис

```
alg restart
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

При запуске службы `algd` с помощью данной команды не происходит включение обработки протокола `DNS`, если она была выключена с помощью команды `alg module process off`. Включить обработку протокола `DNS` можно только с помощью команды `alg module process on`.

Пример использования

```
hostname> alg restart
Shutting down Alg daemon
Loading Alg daemon
```

alg show

Просмотреть текущие параметры обработки прикладных протоколов.

Синтаксис

```
alg show
```

Режимы командного интерпретатора

- Пользователь.
- Режим администратора.

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
SIP	TCP	5060,5080	ON
SIP	UDP	5060,5080	ON

```
hostname>
```

Таблица с параметрами обработки содержит следующие столбцы:

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

Команды группы failover

Настройка и управление системой защиты от сбоев ViPNet Coordinator KB.

failover config edit

Редактировать конфигурационный файл системы защиты от сбоев.

Синтаксис

```
failover config edit
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- По команде будет запущен текстовый редактор с конфигурационным файлом [failover.ini](#).
- После изменения файла `failover.ini` перезапустите службу `failoverd` с помощью команд [failover stop](#) и [failover start](#).

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

По умолчанию установлен одиночный режим (`single`).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- 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

Чтобы установить режим кластера:

```
hostname# failover config mode cluster
Installing ViPNet failover system
hostname#
```

failover show active-mac-address

Просмотреть информацию о доступности сетевого интерфейса активного узла кластера со стороны пассивного узла.

Синтаксис

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

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Команда доступна только в режиме кластера горячего резервирования и только на пассивном узле кластера.
- При доступности активного узла кластера будет выведен список активных интерфейсов кластера, описанных параметрами `device` и `activeip` секций `[channel]` конфигурационного файла `failover.ini`, и соответствующих им MAC-адресов.

Пример использования

- В случае доступности активного узла кластера команда будет иметь вывод:

```
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, команда будет иметь вывод:

```
hostname> failover show active-mac-address

eth0                10.0.2.10  NA
eth1                10.0.3.10  NA
```

- При попытке выполнить команду на активном узле кластера будет выведено сообщение об ошибке:

```
hostname> failover show active-mac-address

error: Use it on passive cluster node only
```

failover show config

Просмотреть файл конфигурации системы защиты от сбоев.

Синтаксис

```
failover show config
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

Для завершения просмотра конфигурационного файла используется клавиша **Q**.

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 пользователя.
- Режим администратора.

Особенности использования

По команде отображается следующая информация:

- версия ПО ViPNet Coordinator KB и версия службы failoverd;
- информация о сетевом узле;
- локальное время на узле;
- режим работы системы защиты от сбоев;
- информация об использовании процессора и оперативной памяти;
- информация о текущем состоянии служб mftpd, failoverd, algd и webgui.

Пример использования

```
hostname> failover show info
Running failover info
Versions: ViPNet 4.3.3(3555), daemon 1.5 (1)
Workstation configured for ID 15EA000B (KB100)
The workstation works in a single mode of protection against failures
Workstation time (utc: 1406806848) Tue Aug 4 15:40:48 2020
failover mode    * single
```

```
failover uptime * 0d 0:14
total cpu      * 3%
total memory   * 1943132 kB
free memory    * 1604324 kB
failover state * works
failover cpu   * 1%
iplir state    * works
iplir cpu      * 7%
mftp state     * works
mftp cpu       * 0%
alg state      * works
alg cpu        * 0%
webgui state   * works
webgui cpu     * 0%
```

failover start

Запустить службу `failoverd`, отвечающую за работу системы защиты от сбоев.

Синтаксис

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

Параметры и ключевые слова

- `active` — запустить службу в активном режиме (в кластере горячего резервирования).
- `passive` — запустить службу в пассивном режиме (в кластере горячего резервирования).

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Параметр доступен только в режиме кластера.
- Если в режиме кластера параметр не указан, служба `failoverd` будет запущена в том режиме, в котором она находилась до завершения работы.
- Перед запуском службы `failoverd` в активном режиме 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 и другим нежелательным последствиям.

Пример использования

Чтобы запустить службу `failoverd` в пассивном режиме:

```
hostname> failover start passive
```

failover stop

Завершить работы службы `failoverd`, отвечающей за работу системы защиты от сбоев.

Синтаксис

```
failover stop
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

При выполнении команды в удаленной SSH-сессии связь с удаленным узлом прервется.

Пример использования

```
hostname> failover stop
Shutting down failover daemon
```

failover view

Просмотреть журнал переключений кластера горячего резервирования 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 пользователя.
- Режим администратора.

Особенности использования

- Команда доступна только в режиме кластера горячего резервирования.
- Чтобы завершить просмотр журнала нажмите Q.

Пример использования

```
hostname> failover view 09.03.2023.08.00.00 23.03.2023.19.00.00
View journal of failover switching
Versions: ViPNet 4.3.3 (3935), daemon 1.5 (1)
Workstation configured for ID 1031F
The workstation works in a cluster mode of protection against failures
Workstation time (utc: 1174916969) Mon Mar 29 17:49:29 2023

09 Mar 2023 12:51:42      <P_START> Start failover daemon in passive mode
22 Mar 2023 12:27:27      <A_START> Start failover daemon in active mode
22 Mar 2023 14:10:35      <A_START> Start failover daemon in active mode
22 Mar 2023 15:30:46      <BOOT> Boot the system
23 Mar 2023 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>] <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 (правила трансляции) в таблице, определяющий его приоритет.
- <имя> — имя фильтра (правила трансляции).
- <отправитель> — ip-адрес или идентификатор отправителя IP-пакетов.
- <получатель> — ip-адрес или идентификатор получателя IP-пакетов.
- <протокол> — протокол, по которому передаются IP-пакеты.
- <расписание> — расписание применения фильтра (правила трансляции).
- <действие> — действие с IP-пакетами, соответствующими условиям фильтра (правила трансляции).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Для работы каждого сетевого фильтра от ViPNet Coordinator KB требуется выделение вычислительных ресурсов, поэтому для стабильного функционирования не должно быть создано суммарно более чем 200000 условий в фильтрах и правилах трансляции адресов.
- Если номер не указан, фильтр (правило трансляции) добавляется в конец соответствующей таблицы и будет применяться при анализе [IP-трафика](#) в последнюю очередь.
- Если указанный номер меньше последнего номера в таблице, нумерация фильтров (правил трансляции), следующих за новым фильтром (правилом трансляции), будет автоматически изменена (их номера будут увеличены на 1).
- В качестве адреса отправителя или получателя можно указать следующее:
 - для локальных фильтров открытой сети — IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску адресов подсети, доменное имя сети, системную группу объектов `any`, `local` или `remote`, одну или несколько пользовательских групп IP-адресов;
 - для транзитных фильтров открытой сети: то же, что для локальных фильтров открытой сети, но в таких фильтрах нельзя использовать системные группы объектов;
 - для фильтров защищенной сети — идентификатор узла или сети ViPNet, список идентификаторов узлов и сетей ViPNet, системные группы объектов `any`, `allcoordinators`, `allclients`, `local` или `remote`, одну или несколько пользовательских групп узлов ViPNet;
 - для фильтров туннелируемых узлов — то же, что для локальных фильтров открытой сети и фильтров защищенной сети, но в таких фильтрах можно использовать только системные группы объектов `any`, `allcoordinators`, `allclients` или `tunneledip`;
 - для правил трансляции адресов — IP-адрес или доменное имя узла, диапазон IP-адресов узлов, список IP-адресов и доменных имен узлов, маску адресов подсети, доменное имя сети, одну или несколько пользовательских групп IP-адресов.
- В качестве адреса отправителя для локальных, транзитных фильтров открытой сети и фильтров туннелируемых узлов также можно указать сетевой интерфейс собственного узла в виде:

```
src interface {<системное имя интерфейса> | @<имя группы интерфейсов> | byip {<IP-адрес> | <диапазон IP-адресов> | <маска подсети>}}
```
- В качестве адреса получателя также можно указать:
 - для локальных фильтров открытой сети — системную группу `broadcast` или `multicast`;
 - для фильтров защищенной сети — системную группу `broadcast`.
- Протокол можно указать, используя:
 - имена протоколов, написанные строчными буквами и разделенные пробелами. При этом можно также задать дополнительные параметры для протоколов:
 - TCP и UDP: `sport` (порт или диапазон портов источника пакета) и/или `dport` (порт или диапазон портов назначения пакета). При использовании обоих этих параметров сначала укажите параметр `sport`, затем — параметр `dport`. Возможно указать несколько портов или диапазонов портов, в этом случае укажите название протокола

(tcp или udp) перед каждым номером порта (диапазоном портов). Например: tcp sport 2525 tcp dport 443 tcp dport 4444-4445.

- ICMP: только параметр `type` (тип пакета) либо параметр `type` вместе с параметром `code` (код пакета). Если параметр `code` не задан, то под условие будут подпадать все ICMP-пакеты указанного типа;
- номера протоколов. При этом перед номером каждого протокола укажите ключевое слово `proto`;
- пользовательские группы протоколов в виде: `service @<имя группы>`.
- Расписание можно задать, используя одну из следующих лексем:
 - `daily <чч:мм>-<чч:мм>` — фильтр действует ежедневно в течение заданного интервала времени. Время указывается в 24-часовом формате: `чч` — часы, `мм` — минуты.
 - `weekly [mo] [tu] [we] [th] [fr] [sa] [su] [at <чч:мм>-<чч:мм>]` — фильтр действует еженедельно в заданные дни недели:
 - `mo` — понедельник,
 - `tu` — вторник,
 - `we` — среда,
 - `th` — четверг,
 - `fr` — пятница,
 - `sa` — суббота,
 - `su` — воскресенье.
 - `calendar <дд.мм.гггг>-<дд.мм.гггг> [at <чч:мм>-<чч:мм>]` — фильтр действует в заданные даты и интервал времени. Дата указывается в следующем формате:
 - `дд` — день,
 - `мм` — месяц,
 - `гггг` — год.
 - `schedule @<имя группы объектов>` — фильтр действует по расписанию, описанному группой объектов соответствующего типа.

Также для задания расписания можно использовать соответствующие пользовательские группы объектов.

- Действие задается одной из следующих лексем:
 - для сетевых фильтров:
 - `pass` — пропускать IP-пакеты;
 - `drop` — блокировать IP-пакеты;
 - для правил трансляции адресов:

- `change src {<адрес> | auto}` — заменять адрес отправителя пакетов на указанный внешний адрес координатора или автоматически на публичный адрес внешнего сетевого интерфейса координатора;
- `change dst <адрес>:[<порт>]` — перенаправлять пакеты на указанные адрес и порт.

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

Пример использования

- Чтобы 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, выполните:

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

- Чтобы создать фильтр, разрешающий отправку IP-пакетов от [защищенного узла](#) с идентификатором 0x1234abab туннелируемому узлу с адресом 192.168.0.1 ежедневно в интервал с 8 утра до 8 вечера, выполните:

```
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
```



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

firewall add name

Создать группу объектов заданного типа.

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Примеры использования

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

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

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

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

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

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

firewall change append

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

Синтаксис

```
firewall <тип> change append <номер> [src <адрес отправителя>] [dst <адрес  
получателя>] [<протокол>] [<расписание>]
```

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 (правила трансляции) в таблице.
- <адрес отправителя> — добавляемый адрес отправителя IP-пакетов.
- <адрес получателя> — добавляемый адрес получателя IP-пакетов.
- <протокол> — добавляемый протокол, по которому передаются IP-пакеты.
- <расписание> — добавляемое расписание применения фильтра (правила трансляции).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

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

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

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

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

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 администратора.

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 осуществляется по строгому совпадению с заданными параметрами.
- Номера фильтров или правил трансляции, следующих за удаленным фильтром или правилом трансляции, автоматически уменьшаются на 1.

Пример использования

Чтобы удалить локальный фильтр открытой сети с номером 7:

```
hostname# firewall local delete 7
=====
Num  Name                               Option      Schedule
Act  Protocol      Source      >Destination
=====
```

```
7      Allow DNS                               User
pass udp: to 53,  @local      >@any
      tcp: to 53
```

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 администратора.

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 администратора.

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

Вывести для просмотра все группы объектов.

Синтаксис

```
firewall object show
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Для возвращения к командной строке введите с клавиатуры символ q.
- Для команды не поддерживается автодополнение.

Пример использования

```
hostname> firewall object show
```

```
Ip Objects
```

```
+====+=====+=====+
|Num |Name                               |Creation type |
+----+-----+-----+
|Inclusion                               |Exclusion      |
+====+=====+=====+
|1   |PrivateNetworkIP                     |User          |
+----+-----+-----+
|10.0.0.0/255.0.0.0, 172.16.0.0/   |              |
|255.0.0.0, 192.168.0.0/255.0.0.0 |              |
+====+=====+=====+
|...                               |              |
+====+=====+=====+
...
hostname>
```

Группы каждого типа объектов выводятся в отдельной таблице, содержащей следующие столбцы:

- Num — порядковый номер группы.
- Name — имя группы.
- Creation Type — вид группы: для групп из ViPNet Policy Manager — Policy, для пользовательских групп — User.
- Inclusion — объекты, входящие в группу.
- Exclusion — объекты, не входящие в группу.

firewall rules show

Просмотреть все сетевые фильтры и правила трансляции адресов.

Синтаксис

```
firewall rules show
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

Каждый тип сетевых фильтров и правила трансляции адресов выводятся в отдельной таблице, содержащей следующие столбцы:

- Num — порядковый номер фильтра (правила трансляции) в таблице;
- Name — имя фильтра (правила трансляции);
- Option — категория фильтра (правила трансляции);
- Schedule — расписание применения фильтра (правила трансляции);
- Act — действие фильтра (правила трансляции);
- Source — адрес отправителя IP-пакетов;
- Destination — адрес получателя IP-пакетов;
- Protocol — протокол, по которому передаются IP-пакеты.

Пример использования

```
hostname> firewall rules show
```

Local Rules:

Num	Name	Option	Schedule
1	Allow DHCP Service	User	
pass	@any	@any	udp: from 67 to 68
...			

empty rule for Forward Rules:

empty rule for Nat Rules:

Каждый тип сетевых фильтров и правила трансляции адресов выводятся в отдельной таблице, содержащей следующие столбцы:

- Num — порядковый номер фильтра (правила трансляции) в таблице.
- Name — имя фильтра (правила трансляции).
- Option — категория фильтра (правила трансляции).
- Schedule — расписание применения фильтра (правила трансляции).
- Act — действие фильтра (правила трансляции).

- `Source` — адрес отправителя IP-пакетов.
- `Destination` — адрес получателя IP-пакетов.
- `Protocol` — протокол, по которому передаются IP-пакеты.

firewall show

Просмотр конкретных групп объектов, сетевых фильтров заданного типа, а также правил трансляции адресов.

Синтаксис

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

Параметры и ключевые слова

- `<тип>` — тип групп объектов или сетевых фильтров, правила трансляции адресов:
 - `ip-object` — группы IP-адресов;
 - `vpn-object` — группы узлов ViPNet;
 - `interface-object` — группы интерфейсов;
 - `service-object` — группы протоколов;
 - `schedule-object` — группы расписаний;
 - `local` — локальный фильтр открытой сети;
 - `forward` — транзитный фильтр открытой сети;
 - `tunnel` — фильтр туннелируемых узлов;
 - `vpn` — фильтр защищенной сети;
 - `nat` — правило трансляции адресов.
- `<параметр>` — параметры фильтров (правил трансляции), отбираемых для просмотра. Можно указать следующие параметры: порядковый номер, имя, адрес отправителя, адрес получателя, протокол, действие фильтра или правила.

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Указать параметры для групп объектов нельзя.

- Синтаксис адреса отправителя, адреса получателя, протокола и расписания — тот же, что при создании фильтра (правила трансляции) с помощью команды `firewall add` (см. [firewall add](#)).
- Можно указать несколько параметров.
- Поиск фильтров (правил трансляции) осуществляется по строгому совпадению с указанными параметрами.
- В результате выполнения команды отображается таблица, содержащая соответствующие типы групп объектов (см. [firewall object show](#)), сетевых фильтров или правил трансляции адресов (см. [firewall rules show](#)).
- Для команды не поддерживается автодополнение.

Пример использования

Для просмотра локальных фильтров для протокола UDP выполните:

```
hostname> firewall local show udp
User:
=====+=====+=====+=====+
|Num|Name                               |Option      |Schedule    |
+----+-----+-----+-----+-----+
|Act|Source   |Destination |Protocol    |
+----+-----+-----+-----+
|1  |Allow DHCP Service   |User        |            |
+----+-----+-----+-----+
|pass|@any        |@any        |udp: from 67 to 68 |
+----+-----+-----+-----+
|...                               |
+----+-----+-----+-----+
hostname>
```

Команды группы inet

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

inet bonding add mode slaves

Настроить агрегированный интерфейс.

Синтаксис

```
inet bonding add <номер> mode <режим> slaves <интерфейс 1> [<интерфейс 2>] [<интерфейс 3>]
```

Параметры и ключевые слова

- <номер> — номер добавляемого агрегированного интерфейса. Возможные значения 0, 1, 2.
- <режим> — режим работы агрегированного интерфейса. Можно указать один из следующих режимов:
 - `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 этом режиме агрегированный интерфейс работает следующим образом:
 - 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, при 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. При этом 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 3>` — физические интерфейсы, подчиненные создаваемому агрегированному интерфейсу.

Значения по умолчанию

Агрегированные интерфейсы не заданы.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Можно задать до трех агрегированных интерфейсов.
- В результате выполнения команды создается агрегированный интерфейс с именем `bond<номер>`.
- Задаваемые подчиненные физические интерфейсы должны относиться к классу `slave`.
- При добавлении агрегированного интерфейса задайте хотя бы один подчиненный ему физический интерфейс. Вы можете задать до трех подчиненных ему физических интерфейсов 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`, организовать на этом канале защиту соединения по технологии `L2OverIP` невозможно.
- Для работы агрегированного интерфейса в режиме `balance-tlb` подключите все подчиненные физические интерфейсы к сети через коммутатор.

- Максимальное количество интерфейсов в ViPNet Coordinator KB (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 KB нельзя использовать в одном агрегированном интерфейсе.

Пример использования

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

```
hostname# inet ifconfig eth0 class slave
```

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

and then restart them.

```
eth0 set to slave class.
```

```
hostname# inet ifconfig eth1 class slave
```

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

and then restart them.

```
eth1 set to slave class.
```

```
hostname# inet bonding add 1 mode balance-rr slaves eth0 eth1
```

```
New bond interface bond1 was created
```

inet bonding delete

Удалить агрегированный интерфейс.

Синтаксис

```
inet bonding delete <номер>
```

Параметры и ключевые слова

<номер> — номер удаляемого агрегированного интерфейса.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Имена агрегированных интерфейсов имеют вид `bond<номер>`.

- Если вы хотите удалить агрегированный интерфейс класса `trunk`, 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 администратора.

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 администратора.

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 администратора.

Особенности использования

- Служба DGD должна быть запущена (см. [inet dgd mode](#)).
- Значение, заданное командой, действует для всех шлюзов, добавленных с помощью команды [inet dgd next-hop add](#).

- При нестабильном соединении (например, при использовании сети 3G или Wi-Fi) рекомендуется увеличить интервал проверки соединения со шлюзом.

Пример использования

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

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

inet dgd configuration response-time

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию время ожидания ответа составляет 3 секунды.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

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

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

inet dgd configuration retries-count

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию проверка работоспособности шлюза выполняется 3 раза.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

Чтобы считать шлюз нерабочим после 5 проверок:

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

inet dgd configuration syslog-level

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

Синтаксис

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

Параметры и ключевые слова

<уровень важности> — уровень важности событий, записываемых в системный журнал.

Возможные значения:

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

Каждый последующий уровень включает в себя предыдущие.

Значение -1 отключает регистрацию событий службы DGD.

Значения по умолчанию

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

Режимы командного интерпретатора

Режим администратора.

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 mode

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

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 администратора.

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 KB (и немедленно запустить службу DGD):

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

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 текстовое имя удаленного шлюза. Может содержать символы латинского алфавита, цифры и дефис («-»). Максимальная длина — 63 символа.
- `<адрес шлюза>` — уникальный IP-адрес удаленного шлюза.
- `<интерфейс>` — имя сетевого интерфейса ViPNet Coordinator KB. Данный параметр следует использовать только для сетевых интерфейсов, получающих IP-адрес по протоколу DHCP. Возможные значения:
 - `eth0`, `eth1`, `eth2` и так далее;
 - `wlan0`;
 - `modem` (для динамических rpp-интерфейсов).
- `<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 уникальный IP-адрес шлюза.

Не используйте одинаковые IP-адреса для проверки шлюзов DGD и для параметров `testip` при работе в кластере горячего резервирования — это может привести к циклической перезагрузке обоих узлов кластера.

- `check` — включить проверку состояния заданного шлюза.
- `no-check` — отключить проверку состояния заданного 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 администратора.

Особенности использования

- Служба DGD должна быть запущена (см. [inet dgd mode](#)).
- Если вы задали проверку шлюза с использованием TCP-соединения и порта 80 или 443, 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 администратора.

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 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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 «внутренней петли» (`loopback`, `localhost`);
 - виртуальные интерфейсы, созданные после назначения дополнительных IP-адресов физическим интерфейсам (алиасы).

Пример использования

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

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

inet dhcp relay add listen-interface

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Режим администратора.

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 «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 администратора.

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 администратора.

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 администратора.

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 KB.

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 администратора.

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 KB, 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 администратора.

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 администратора.

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 администратора.

Пример использования

Чтобы завершить работу копии 2 процесса DHCP-relay:

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

inet dhcp server add default-lease-time

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

Синтаксис

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

Параметры и ключевые слова

- <время> — время аренды в секундах (от 1 до 4294967294).
- <интерфейс> — название сетевого интерфейса в системе, для которого задается время аренды (лизинга) IP-адресов по умолчанию.
- <подсеть> — IP-адрес удаленной подсети, клиентам которой будет передаваться время аренды IP-адресов по умолчанию. Удаленная подсеть должна быть предварительно задана командой [inet dhcp server add relay-interface](#).
- <маска> — маска удаленной подсети.

- `<имя узла>` — имя узла сети ViPNet, для которого задается время аренды IP-адресов по умолчанию (в параметрах секции `[id]` указанного узла файла `iplir.conf`). Для узла должен быть предварительно зарезервирован IP-адрес с помощью команды [inet dhcp server add host](#).

Значения по умолчанию

По умолчанию время аренды составляет 864000 секунд.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

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

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

inet dhcp server add dns

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

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

```
hostname# inet dhcp server add dns 192.168.15.41 interface eth1
```
- Чтобы задать IP-адрес DNS-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server add dns 192.168.15.41 remote subnet 192.168.1.0 mask 255.255.255.0
```
- Чтобы задать IP-адрес DNS-сервера 192.168.15.41 для узла сети ViPNet с именем host123:

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

inet dhcp server add domain

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

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

```
hostname# inet dhcp server add domain dc.corp interface eth1
```
- Чтобы задать доменное имя dc.corp для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server add domain dc.corp remote subnet 192.168.1.0 mask 255.255.255.0
```
- Чтобы задать доменное имя dc.corp для узла сети ViPNet с именем host123:

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

inet dhcp server add host

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

Синтаксис

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

Параметры и ключевые слова

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

- <маска> — маска удаленной подсети.

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 рабочего можно указать физический, VLAN- или агрегированный сетевой 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 узла сети ViPNet, для которого задается время аренды IP-адресов (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Значения по умолчанию

Время аренды составляет 864000 секунд.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

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

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

inet dhcp server add ntp

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

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

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

```
hostname# inet dhcp server add ntp 192.168.15.41 interface eth1
```
- Чтобы задать IP-адрес NTP-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

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

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

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

inet dhcp server add option

Добавить опцию DHCP-сервера в соответствии с [RFC 2132](#).

Синтаксис

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

Параметры и ключевые слова

- `<номер>` — номер опции DHCP-сервера (от 1 до 254).
- `ip` — опция содержит IP-адрес.
- `ascii` — опция содержит текст в кодировке ASCII.
- `hex` — опция содержит разрядное шестнадцатеричное число (с точками разрядов, без учета регистра).
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задается опция DHCP-сервера.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой будет передаваться опция DHCP-сервера. Удаленная подсеть должна быть предварительно задана командой `inet dhcp server add relay-interface`.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задается опция DHCP-сервера (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 администратора.

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 рабочего можно указать физический, VLAN- или агрегированный сетевой 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 узла сети ViPNet, для которого задается IP-адрес шлюза по умолчанию (в параметрах секции [id] указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 администратора.

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 рабочего можно указать физический, VLAN- или агрегированный сетевой 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 администратора.

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 администратора.

Особенности использования

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

Пример использования

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

```
hostname# inet dhcp server delete ntp 192.168.15.41 interface eth1
```
- Чтобы удалить IP-адрес NTP-сервера 192.168.15.41 для клиентов удаленной подсети с адресом 192.168.1.0/24:

```
hostname# inet dhcp server delete ntp 192.168.15.41 remote subnet 192.168.1.0 mask  
255.255.255.0
```
- Чтобы удалить IP-адрес NTP-сервера 192.168.15.41 для узла сети ViPNet с именем host123:

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

inet dhcp server delete option

Удалить опцию DHCP-сервера в соответствии с [RFC 2132](#).

Синтаксис

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

Параметры и ключевые слова

- <номер> — номер опции DHCP-сервера (от 1 до 254).
- <интерфейс> — название сетевого интерфейса в системе, для которого удаляется опция DHCP-сервера.
- <подсеть> — IP-адрес удаленной подсети, клиентам которой передается опция DHCP-сервера.
- <маска> — маска удаленной подсети.
- <имя узла> — имя узла сети ViPNet, для которого задана опция DHCP-сервера (в параметрах секции [id] указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 администратора.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. [inet dhcp server stop](#)).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов, заданных командой [inet dhcp server add interface](#).

Пример использования

Чтобы удалить интерфейс `eth1`, на котором DHCP-сервер обрабатывает запросы от агента DHCP-relay, работающего в удаленной подсети с адресом 192.168.10.0/24:

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

inet dhcp server delete router

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

Синтаксис

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

Параметры и ключевые слова

- `<адрес>` — IP-адрес шлюза по умолчанию.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого задан IP-адрес шлюза по умолчанию.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передается IP-адрес шлюза по умолчанию.
- `<маска>` — маска удаленной подсети.
- `<имя узла>` — имя узла сети ViPNet, для которого задан IP-адрес шлюза по умолчанию.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

Чтобы удалить адрес шлюза по умолчанию 192.168.10.1, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

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

inet dhcp server delete subnet-mask

Удалить маску подсети, передаваемую DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Перед выполнением команды завершите работу DHCP-сервера (см. [inet dhcp server stop](#)).
- По команде будет автоматически удален широковещательный IP-адрес, передаваемый DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP-relay).

Пример использования

Чтобы удалить маску подсети, передаваемую DHCP-сервером клиентам сети 192.168.10.0/24:

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

inet dhcp server delete tftp

Удалить настройки TFTP-сервера, передаваемые DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

Чтобы удалить IP-адрес TFTP-сервера 192.168.10.65, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

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

inet dhcp server delete voip

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

Синтаксис

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

Параметры и ключевые слова

- `<адрес сервера>` — IP-адрес TFTP-сервера Cisco VoIP.
- `<интерфейс>` — название сетевого интерфейса в системе, для которого заданы параметры TFTP-сервера Cisco VoIP.
- `<подсеть>` — IP-адрес удаленной подсети, клиентам которой передаются параметры TFTP-сервера Cisco VoIP.
- `<маска>` — маска удаленной подсети.

- `<имя узла>` — имя узла сети ViPNet, для которого заданы параметры TFTP-сервера Cisco VoIP (в параметрах секции `[id]` указанного узла файла `iplir.conf`).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

Чтобы удалить IP-адрес TFTP-сервера Cisco VoIP 192.168.10.65, передаваемый DHCP-сервером клиентам сети 192.168.10.0/24:

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

inet dhcp server delete wins

Удалить адрес [WINS-сервера](#) из списка адресов, передаваемых DHCP-сервером своим клиентам (либо клиентам удаленной подсети при использовании стороннего DHCP relay).

Синтаксис

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

Параметры и ключевые слова

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

Режимы командного интерпретатора

Режим администратора.

Особенности использования

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

Пример использования

Удалить IP-адрес WINS-сервера 192.168.10.65, передаваемый DHCP-сервером клиентам удаленной подсети 192.168.10.0/24:

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

inet dhcp server mode

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

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 администратора.

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 KB, и завершить работу DHCP-сервера.

Синтаксис

```
inet dhcp server reset
```

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 администратора.

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 KB.

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 администратора.

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 KB.

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 администратора.

Особенности использования

При вводе адреса работают автодополнение и подсказка, данные для подсказки берутся из текущего списка клиентов DNS-сервера.

Пример использования

```
hostname# inet dns clients delete 192.168.0.7
```

```
Client '192.168.0.7' removed from the list of allowed clients
```

```
Reloading domain name service...: bind9.
```

inet dns clients list

Просмотреть список DNS-клиентов, которым разрешена передача запросов DNS-серверу.

Синтаксис

```
inet dns clients list
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> inet dns clients list
Allow DNS requests from the following client(s):
any
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 осуществляется перенаправление запросов.

Синтаксис

```
inet dns forwarders add <адрес> [for-zone <имя зоны>]
```

Параметры и ключевые слова

- <адрес> — IP-адрес DNS-сервера.
- <имя зоны> — имя зоны (окончание доменного имени сетевых узлов, запросы от которых перенаправляются на DNS-сервер).

Режимы командного интерпретатора

Режим администратора.

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 пересылки добавить сервер с адресом 10.0.2.3:

```
hostname# inet dns forwarders add 10.0.2.3
```

- Чтобы в список DNS-серверов пересылки 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 (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 администратора.

Особенности использования

- При вводе адреса работают автодополнение и подсказка, данные для подсказки берутся из текущего списка DNS-серверов 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 пересылки удалить сервер с адресом 10.0.2.3:

```
hostname# inet dns forwarders delete 10.0.2.3
```
- Чтобы из списка DNS-серверов пересылки 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 пересылки (forwarder).

Синтаксис

```
inet dns forwarders list
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Если адреса DNS-серверов пересылки 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 USER`.

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 KB.

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 администратора.

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 start

Запустить DNS-сервер.

Синтаксис

```
inet dns start
```

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 администратора.

Особенности использования

- При вводе имени интерфейса работают автодополнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен относиться к классу `access`.

- 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 горячего резервирования (см. [failover show info](#)). 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 администратора.

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`.
- Нельзя добавить IP-адрес, если на указанном интерфейсе 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.

Пример использования

```
hostname# inet ifconfig eth1 address add 192.168.10.2 netmask 255.255.255.0
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 администратора.

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`.
- Нельзя удалить дополнительный IP-адрес, если на указанном интерфейсе установлен режим DHCP.
- Если дополнительный IP-адрес с указанными параметрами существует, то удаляется соответствующий виртуальный интерфейс.

Пример использования

Чтобы с интерфейса `eth1` удалить дополнительный IP-адрес `192.168.10.2` с маской подсети `255.255.255.0`:

```
hostname# inet ifconfig eth1 address delete 192.168.10.2 netmask 255.255.255.0
```

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 администратора.

Особенности использования

- Задаваемый подчиненный физический интерфейс должен относиться к классу `slave`.
- 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 KB (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 администратора.

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 администратора.

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 администратора.

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 администратора.

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` (см. [inet bonding add mode slaves](#)). 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 администратора.

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` (см. [inet bonding add mode slaves](#)). 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 администратора.

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

Установить класс заданного 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

По умолчанию все физические интерфейсы ViPNet Coordinator KB относятся к классу `access`.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Класс `trunk` можно установить только для физических интерфейсов. Виртуальные интерфейсы всегда относятся к классу `access`.
- Для 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.
- Установка класса `trunk` или `slave` при работе в удаленной SSH приведет к потере связи с удаленным сетевым узлом.

Пример использования

Чтобы установить класс `trunk` на интерфейсе `eth1` для возможности создавать на его базе виртуальные интерфейсы, выполните:

```
hostname# inet ifconfig eth1 class trunk
```

inet ifconfig dhcp

Установить режим DHCP на заданном 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.
- `on` — включение автоматического приема указанной настройки.
- `off` — выключение автоматического приема указанной настройки.

Значения по умолчанию

По умолчанию для всех настроек, передаваемых с помощью DHCP, автоматический прием включен (on).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Указанный интерфейс должен быть включен.
- Параметр <настройка> при вводе команды может не задаваться. В этом случае на интерфейсе будет просто включен режим DHCP.
- Указанный интерфейс может относиться к классу `access`.
- 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 конкретном сетевом интерфейсе ViPNet Coordinator KB.

Синтаксис

```
inet ifconfig <имя интерфейса> dhcp route-metric {<1-255> | none}
```

Параметры и ключевые слова

- <1-255> — значение метрики.
- none — удаляет метрику на сетевом интерфейсе.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Если на сетевом интерфейсе не установлен режим DHCP, то заданная метрика будет сохранена. Но метрика начнет учитываться только после того, как режим DHCP будет установлен.
- Указанный интерфейс может относиться к классу `access`.
- 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 администратора.

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 KB.

Пример использования

Чтобы выключить виртуальный интерфейс `eth1.2`:

```
hostname# inet ifconfig eth1.2 down
```

inet ifconfig mtu

Изменить значение MTU для заданного сетевого интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> mtu {<значение MTU> | auto}
```

Параметры и ключевые слова

- `<интерфейс>` — имя сетевого интерфейса.
- `<значение MTU>` — размер MTU в байтах. Допустимые значения: 1280–9000.
- `auto` — задает значение MTU по умолчанию (1500 байт).

Значения по умолчанию

По умолчанию используется значение MTU 1500 байт.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда не может быть использована для сетевых интерфейсов классов `vlan` и `slave`.
- Значение MTU, заданное для интерфейса класса `trunk`, автоматически применяется ко всем виртуальным интерфейсам класса `vlan`, созданным на этом физическом интерфейсе.
- Значение MTU, заданное для интерфейса класса `bond`, будет использоваться на всех подчиненных физических интерфейсах класса `slave`.
- При создании агрегированного интерфейса с помощью командного интерпретатора для всех подчиненных физических интерфейсов автоматически задается значение MTU 1500 байт.
- Если вы исключаете подчиненный физический интерфейс из агрегированного, для исключенного интерфейса устанавливается значение MTU 1500 байт.

Пример использования

Чтобы для интерфейса `eth0` задать размер MTU, равный 3000 байт:

```
hostname# inet ifconfig eth0 mtu 3000
```

inet ifconfig reset

Сбросить настройки заданного 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 администратора.

Особенности использования

- При выполнении команды с параметром `all` происходит сброс настроек всех физических интерфейсов. Все виртуальные интерфейсы при этом удаляются.
- Выполнение команды при работе в удаленной SSH-сессии с параметром `all` приведет к потере связи с удаленным сетевым узлом.
- Команда используется для подготовки указанного интерфейса к установке новых параметров.
- По команде будут выполнены следующие 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 VLAN по команде не сбрасываются следующие настройки:
 - Имя соответствующего физического интерфейса.
 - Номер виртуального интерфейса VLAN.

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. Можно указать одно из следующих значений: 10, 100, 1000.
- `half` — полудуплекс.
- `full` — полный дуплекс.
- `autoneg` — режим автосогласования скорости интерфейса (autonegotiation):
 - `on` — режим автосогласования включен;
 - `off` — режим автосогласования выключен.

Значения по умолчанию

По умолчанию на интерфейсе устанавливаются автоматические параметры (определяются, исходя из характеристик интерфейса).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Режим полудуплекса не поддерживается для аппаратных платформ KB100 Q1 и KB100 Q2.

- Нельзя установить параметры скорости виртуального интерфейса, так как он наследует эти параметры от соответствующего физического интерфейса.
- Команда неприменима к интерфейсам класса slave.
- 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 KB и коммутационного оборудования, подключенного к данному интерфейсу.
- Нельзя изменить параметры скорости, режим дуплекса и автосогласования для оптических интерфейсов (для исполнений, оборудованных соответствующими разъемами).

Пример использования

Чтобы 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 на заданном интерфейсе режим автоматического определения параметров скорости.

Синтаксис

```
inet ifconfig <интерфейс> speed auto
```

Параметры и ключевые слова

<интерфейс> — имя интерфейса.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Нельзя установить параметры скорости виртуального интерфейса, так как он наследует эти параметры от соответствующего физического интерфейса.
- Команда неприменима к интерфейсам класса slave.

Пример использования

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

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

inet ifconfig up

Включить сетевой интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> up
```

Параметры и ключевые слова

<интерфейс> — имя интерфейса.

Режимы командного интерпретатора

Режим администратора.

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 администратора.

Особенности использования

- Физический интерфейс должен относиться к классу `trunk`.
- 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 KB (включая физические, агрегированные, виртуальные, VLAN и localhost) не может превышать 128.
- Номер виртуальной сети `<номер>` должен находиться в диапазоне от 1 до 4094. Значения 0 и 4095 зарезервированы.

Пример использования

Чтобы на базе интерфейса `eth1` создать интерфейс для виртуальной сети с номером 2:

```
hostname# inet ifconfig eth1 vlan add 2
```

inet ifconfig vlan delete

Удалить виртуальный интерфейс.

Синтаксис

```
inet ifconfig <интерфейс> vlan delete <номер>
```

Параметры и ключевые слова

- `<интерфейс>` — имя физического интерфейса.
- `<номер>` — номер виртуальной сети.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- При вводе номера работают автодополнение и подсказка, данные для подсказки берутся из списка существующих виртуальных интерфейсов.

- Невозможно удалить виртуальный интерфейс, заданный как рабочий в параметрах функции L2OverIP, если эта функция включена.

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 администратора.

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 администратора.

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 пользователя.
- Режим администратора.

Особенности использования

- NTP-серверы, полученные по DHCP, отмечены как `from DHCP`.
- NTP-серверы, заданные пользователем, отмечены как `from USER`.
- Команда выводит только IP-адреса NTP-серверов, заданных пользователем, даже если при добавлении использовались их доменные имена.

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 KB.

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 администратора.

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 удастся 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 администратора.

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 администратора.

Пример использования

```
hostname# inet ntp start
```

```
Starting NTP server...
```

inet ntp stop

Завершить работу NTP-сервера.

Синтаксис

```
inet ntp stop
```

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# inet ntp stop
Stopping NTP server: ntpd.
```

inet ospf mode

Включить или выключить использование протокола [OSPF](#).

Синтаксис

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

Параметры и ключевые слова

- `on` — включение протокола OSPF;
- `off` — выключение протокола OSPF.

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# inet ospf mode on
Starting OSPF ...
hostname#
```

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 администратора.

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
-----	-----	-----
10.0.5.0	255.255.255.0	1

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 администратора.

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 администратора.

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 администратора.

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 ping

Проверить соединение с сетевым узлом.

Синтаксис

```
inet ping {<IP-адрес> | <доменное имя>}
```

Параметры и ключевые слова

- <IP-адрес> — IP-адрес узла (в виде октетов или шестнадцатеричного числа), с которым необходимо проверить соединение.
- <доменное имя> — доменное имя узла, с которым необходимо проверить соединение.

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- IP-адрес в виде шестнадцатеричного числа перед выполнением опроса преобразовывается в корректный IPv4 адрес.
- Чтобы завершить проверку соединения нажмите **Ctrl+C**.

Пример использования

Чтобы проверить соединение с адресом 10.0.2.1:

```
hostname> inet ping 10.0.2.1
Pinging 10.0.2.1, press Ctrl+C to cancel.
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
^C
--- 10.0.2.1 ping statistics ---
4 packets transmitted, 4 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. Может содержать символы латинского алфавита, цифры и дефис. Максимальная длина — 253 символа.
- default — использовать политику маршрутизации по умолчанию.

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 администратора.

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; 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.

Режимы командного интерпретатора

Режим администратора.

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. 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 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 администратора.

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. Может содержать символы латинского алфавита, цифры и дефис. Максимальная длина — 63 символа;
- <приоритет> — приоритет правила в списке, возможные значения от 1025 до 2048. Чем меньше значение, тем выше приоритет правила;
- `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 администратора.

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 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 администратора.

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 в том случае, если наряду с этим маршрутом будет присутствовать другой маршрут в ту же самую 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` (см. [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 общей таблице маршрутизации.

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 show dgd configuration

Просмотреть параметры службы DGD.

Синтаксис

```
inet show dgd configuration
```

Режимы командного интерпретатора

- Режим пользователя.

- Режим администратора.

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 пользователя.
- Режим администратора.

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 пользователя.
- Режим администратора.

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 пользователя.
- Режим администратора.

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 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 пользователя.
- Режим администратора.

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 dhcp server

Просмотреть настройки DHCP-сервера и его текущее состояние.

Синтаксис

```
inet show dhcp server
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

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 пользователя.
- Режим администратора.

Особенности использования

Если среди клиентов DHCP-сервера присутствуют клиенты, подключенные к разным интерфейсам VLAN, у которых 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	2023-12-12 01:37:06
d8:a2:5e:94:40:81	192.168.0.178	foo-2	2023-12-12 01:04:56
e8:9a:8f:6e:0f:60	192.168.0.127	angela	2023-12-11 23:55:32
ec:55:f9:c5:f2:55	192.168.0.179	angela	2023-12-11 23:54:56
f0:4f:7c:3f:9e:dc	192.168.0.183	kindle-1234567	2023-12-11 23:54:31
f4:ec:38:e2:f9:67	192.168.0.185	-NA-	2023-12-11 23:55:40
f8:d1:11:b7:5a:62	192.168.0.184	-NA-	2023-12-11 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 2023/01/30 08:02:54;
ends 5 2023/02/04 08:02:54;
hardware ethernet
00:50:04:53:D5:57;
uid 01:00:50:04:53:D5:57;
client-hostname "PC0097";
}
...
```

inet show dns

Просмотреть информацию о состоянии DNS-сервера.

Синтаксис

```
inet show dns
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

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

inet show interface

Вывести параметры заданного интерфейса и его текущее состояние.

Синтаксис

```
inet show interface [<имя интерфейса> | <имя интерфейса>:<номер>]
```

Параметры и ключевые слова

- <имя интерфейса> — имя физического или виртуального интерфейса.
- <имя интерфейса>:<номер> — имя виртуального интерфейса, если основной интерфейс имеет дополнительный IP-адрес (alias).

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- При вводе имени интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- Если параметр не указан, то выводится информация обо всех интерфейсах, включая существующие дополнительные IP-адреса интерфейсов.
- Если в качестве параметра вы указали имя виртуального интерфейса, созданного при добавлении на основной интерфейс дополнительного IP-адреса, то будет выдана краткая информация по основному интерфейсу.

Пример использования

Чтобы просмотреть информацию об интерфейсе eth0:

```
hostname> inet show interface eth0

eth0      Link encap:Ethernet  HWaddr 00:15:17:e4:6c:5a
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

```

RX bytes:0 (0.0 B)   TX bytes:0 (0.0 B)

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

Speed: 1000Mb/s
Duplex: Full
Auto-negotiation: off
Link detected: yes

```

По команде выводится следующая информация:

- IP-адрес.
- Маска подсети.
- Настройки получения информации от DHCP-сервера и заданная метрика для маршрутов DHCP-сервера, если на интерфейсе включен соответствующий режим.
- Класс интерфейса (access, trunk или slave). В зависимости от класса интерфейса также выводится следующая информация:
 - Для класса trunk — список существующих дочерних виртуальных интерфейсов.
 - Для класса access — информация о родительском интерфейсе данного виртуального интерфейса.
- Состояние интерфейса (включен или выключен).

inet show mac-address-table

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

Синтаксис

```
inet show mac-address-table
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```

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

```

inet show ntp

Вывести настройки NTP-сервера и его текущее состояние.

Синтаксис

```
inet show ntp
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

Если NTP-сервер запущен, дополнительно выводятся параметры NTP-серверов, используемых для синхронизации. Эта информация выводится в виде таблицы.

Пример использования

```
hostname> inet show ntp
NTP server is autostart off
NTP server is RUNNING
  remote      refid      st t when poll reach  delay  offset jitter
=====
  10.0.2.1      10.0.2.4   5 u  36   64    1  3.893  0.708  0.000
  10.0.2.1      10.0.6.100 4 u  35   64    1  0.702 25.706  0.000
  194.149.67.129 .INIT.    16 u   -   64    0  0.000 0.000  0.000
hostname>
```

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.

В зависимости от столбца, в нем содержится следующая информация:

- **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 KB и NTP-серверами.
- jitter — абсолютное значение в миллисекундах с указанием среднеквадратичного отклонения смещения относительно ViPNet Coordinator KB.
- refid — код ошибки или идентификатор NTP-сервера.

inet show ospf configuration

Вывести настройки протокола OSPF.

Синтаксис

```
inet show ospf configuration
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> inet show ospf configuration
```

```
OSPF protocol is enabled
```

```
OSPF networks defined:
```

Destination	Netmask	OSPF Area
-----	-----	-----
10.0.2.0	255.255.255.0	1

```
10.0.5.0      255.255.255.0    0
```

```
Redistribution of DHCP routes is enabled.
```

```
hostname>
```

По команде выводится следующая информация:

- включено или выключено использование протокола OSPF;
- список сетей, в которых ViPNet Coordinator KB осуществляет маршрутизацию по протоколу OSPF (IP-адреса, маски и области);
- включено или выключено перераспределения маршрутов (статических или от DHCP-сервера).

inet show ospf database

Просмотреть информацию о состоянии каналов связей между всеми OSPF-маршрутизаторами в базе данных (link state database).

Синтаксис

```
inet show ospf database
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> inet show ospf 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 show ospf neighbour

Просмотреть сведения о соседних OSPF-маршрутизаторах, работающих в вашей сети по протоколу OSPF.

Синтаксис

```
inet show ospf neighbour
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> inet show ospf neighbour
```

Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmtl	Rqstl	DBsm1
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 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 пользователя.
- Режим администратора.

Особенности использования

- Чтобы завершить просмотр нажмите **Q**.
- Команда недоступна на пассивном узле при работе в кластере горячего резервирования.

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

Вывести содержимое общей таблицы маршрутизации или списки маршрутов от конкретного источника (Static, DHCP/PPP, OSPF).

Синтаксис

```
inet show routing {static | dhcp | ospf}
```

Параметры и ключевые слова

- `static` — для просмотра статических маршрутов;
- `dhcp` — для просмотра динамических маршрутов, получаемых от DHCP/PPP-сервера;
- `ospf` — для просмотра динамических маршрутов передаваемых по протоколу OSPF.

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Если параметр не указан, то выводится список со всеми маршрутами.
- 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.

Пример использования

```
hostname> inet show routing
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel, D - DHCP/PPP,
       > - selected route, * - FIB route

D      0.0.0.0/0 [35/23] via 10.1.30.5, eth1
S>      0.0.0.0/0 [10/0] (weight 1) via 10.0.1.4 inactive
          (weight 1) via 10.0.2.1 inactive
*          (weight 1) via 10.0.5.2, eth0
S>*    10.0.1.0/24 [10/0] via 10.0.5.2, eth0
S>*    10.0.2.0/24 [10/0] via 10.0.5.2, eth0
O      10.0.5.0/24 [110/10] is directly connected, eth0, 5d22h18m
```

```
C>* 10.0.5.0/24 is directly connected, eth0
S 10.1.1.1/32 [10/0] (weight 1) via 10.2.2.2 inactive
                               (weight 1) via 10.3.3.2 inactive
D>* 10.100.2.0/24 [30/23] (weight 1) via 10.1.30.202, eth1
*                               (weight 1) via 10.1.30.202, eth1
hostname>
```

Пояснения по атрибутам, которые выводятся перед списком маршрутов, приведены в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора», в разделе «Просмотр таблицы маршрутизации».

inet show snmp

Вывести информацию о текущем состоянии SNMP-агента, IP-адресе удаленного узла, на который отправляются оповещения SNMP Traps, а также о заданном уровне протоколирования.

Синтаксис

```
inet show snmp
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> inet show snmp
Net-SNMP agent is RUNNING.
ViPNet SNMP plugin is RUNNING.
VPN SNMP service autostart is ON.
debug-level = debug
trapsink = 192.168.0.1
```

inet show snmp community

Просмотреть пароли:

- пароль для авторизации на удаленной станции сетевого менеджмента, заданный с помощью команды `inet snmp community trap`.
- пароль доступа к SNMP-параметрам ViPNet Coordinator KB, заданный с помощью команды `inet snmp community ro`.

Синтаксис

```
inet show snmp community
```

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# inet show snmp community
community ro = public
community trap = public
```

inet show vlan

Просмотреть список виртуальных интерфейсов.

Синтаксис

```
inet show vlan
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

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
```

inet snmp community ro

Задать пароль доступа к SNMP-параметрам вашего ViPNet Coordinator KB.

Синтаксис

```
inet snmp community ro
```

Значения по умолчанию

Задан пароль `public`.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- После выполнения команды введите пароль и нажмите **Enter**.
- Длина пароля должна быть от 6 до 18 символов.
- В паролях вы можете использовать символы латинского алфавита, цифры, а также следующие специальные символы: `. * / - : _ ? = @ & ( ) , .`

Пример использования

Чтобы задать пароль `Aa1234567`:

```
hostname# inet snmp community ro
```

```
SNMP community ro: Aa1234567
```

inet snmp community trap

Задать пароль, используемый при авторизации на удаленной станции сетевого менеджмента, принимающей оповещения SNMP Traps.

Синтаксис

```
inet snmp community trap
```

Значения по умолчанию

Задан пароль `public`.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- После выполнения команды введите пароль и нажмите **Enter**.
- Длина пароля должна быть от 6 до 18 символов.
- В паролях вы можете использовать символы латинского алфавита, цифры, а также следующие специальные символы: . * / - : _ ? = @ & () , .

Пример использования

Чтобы задать пароль Aa1234567:

```
hostname# inet snmp community trap
SNMP community trap: Aa1234567
```

inet snmp debug-level

Задать уровень важности событий SNMP-агента, которые будут записываться в системный журнал.

Синтаксис

```
inet snmp debug-level <уровень важности>
```

Параметры и ключевые слова

<уровень важности> — может принимать одно из следующих значений:

- `off` — запись событий в журнал выключена;
- `info` — в журнал записывается только информация, касающаяся инициализации SNMP-агента;
- `debug` — в журнал записывается служебная информация, используемая при отладке;
- `error` — в журнал записываются ошибки, после которых SNMP-агент может продолжать работу;
- `critical` — в журнал записываются критические ошибки, после которых SNMP-агент не может продолжить работу.

Значения по умолчанию

По умолчанию используется уровень `info`.

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# inet snmp debug-level off
```

inet snmp mode

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

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Запуск SNMP-агента при загрузке ViPNet Coordinator KB включен (`on`).

Режимы командного интерпретатора

Режим администратора.

Пример использования

Чтобы включить запуск SNMP-агента при загрузке ViPNet Coordinator KB:

```
hostname# inet snmp mode on
```

```
VPN SNMP agent enabled and will be started during next boot.
```

```
You have to start VPN SNMP agent manually or reboot to start it.
```

```
hostname#
```

inet snmp start

Запустить встроенный SNMP-агент.

Синтаксис

```
inet snmp start
```

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# inet snmp start  
Starting VPN SNMP agent: vpn-snmpd.
```

inet snmp stop

Завершить работу встроенного SNMP-агента.

Синтаксис

```
inet snmp stop
```

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# inet snmp stop  
Stopping VPN SNMP services: ViPNet SNMP plugin.  
Stopping VPN SNMP services: Net-SNMP agent.  
hostname#
```

inet snmp trapsink

Задать сетевой узел, на который будут направляться оповещения по протоколу SNMP.

Синтаксис

```
inet snmp trapsink {<адрес> | null}
```

Параметры и ключевые слова

- <адрес> — IP-адрес или доменное имя удаленного сетевого узла.

- `null` — выключить оповещения.

Значения по умолчанию

Сетевой узел не задан.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Сетевой узел, на который будут отправляться оповещения по протоколу SNMP, должен быть доступен для ViPNet Coordinator KB.

Пример использования

Для направления оповещений по протоколу SNMP на узел с адресом 192.168.10.10:

```
hostname# inet snmp trapsink 192.168.10.10
```

inet ssh

Подключиться по SSH к заданному ViPNet Coordinator KB.

Синтаксис

```
inet ssh {host <адрес> | id <идентификатор>} [user <пользователь>]
```

Параметры и ключевые слова

- `<адрес>` — доменное имя или IP-адрес удаленного ViPNet Coordinator KB.
- `<идентификатор>` — идентификатор сетевого узла ViPNet в шестнадцатеричном формате. Используется для доступа к защищенному узлу.
- `<пользователь>` — имя пользователя удаленного ViPNet Coordinator KB.

Значения по умолчанию

- `<пользователь>` — `user`.

Режимы командного интерпретатора

- Режим администратора.

Особенности использования

- При вводе идентификатора работают автозаполнение и подсказка, данные для подсказки берутся из списка связей ViPNet Coordinator KB.
- 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 KB 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 ViPNet Coordinator KB с идентификатором 0x270e000a:

```
hostname# inet ssh id 0x270e000a
```

inet vlan comment add

Добавить комментарий к виртуальной сети.

Синтаксис

```
inet vlan <номер> comment add <комментарий>
```

Параметры и ключевые слова

- <номер> — номер виртуальной сети.
- <комментарий> — комментарий. Комментарий, содержащий пробелы, должен быть указан в двойных кавычках.

Режимы командного интерпретатора

Режим администратора.

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 администратора.

Пример использования

Чтобы удалить комментарий к виртуальной сети с номером 10:

```
hostname# inet vlan 10 comment delete
```

Команды группы iplir

Настройка параметров работы в защищенной [сети ViPNet](#), а также параметров [L2OverIP](#).

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 администратора.

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 удаляемого сетевого интерфейса.

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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

Открыть для редактирования один из конфигурационных файлов: основной конфигурационный файл или конфигурационный файл заданного интерфейса.

Синтаксис

```
iplir config <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя [статического интерфейса](#), для которого требуется редактировать конфигурационный файл.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Если в команде не указан параметр, то будет запущен текстовый редактор с основным конфигурационным файлом `iplir.conf`.
- Перед редактированием файла `iplir.conf` или файла `iplir.conf-<интерфейс или группа интерфейсов>` требуется завершить работу службы `iplircfg` (см. [iplir stop](#)).

Пример использования

Чтобы отредактировать конфигурационный файл интерфейса `eth0`:

```
hostname# iplir config eth0
```

iplir info

Вывести информацию о своем узле и количестве туннельных соединений, а также статистику фильтрации IP-пакетов по заданному интерфейсу или группе интерфейсов.

Синтаксис

```
iplir info <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя [статического интерфейса](#), для которого требуется просмотреть статистику фильтрации IP-пакетов.

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Если в команде не указан параметр, то 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 в команде указан интерфейс, то выводится только статистика фильтрации IP-пакетов по этому интерфейсу.
- Если в команде указана группа интерфейсов, то выводится статистика фильтрации IP-пакетов по всем активным интерфейсам, входящим в эту группу.
- Для выполнения команды требуется, чтобы была запущена служба `iplircfg`.

Пример использования

Для просмотра статистики 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

hostname>

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 KB.
- <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 get

Просмотреть состояние или значение одного из параметров [межсетевого экрана](#).

Синтаксис

```
iplir option get <параметр>
```

Параметры и ключевые слова

<параметр> — параметр межсетевого экрана:

- antispoofing — состояние функции [антиспуфинга](#);
- block-fragmented-packets — состояние функции блокирования фрагментированных IP-пакетов, передаваемых по всем сетевым интерфейсам;

- `block-other-protocols` — состояние функции блокирования IP-пакетов, передаваемых по всем протоколам, кроме IP, ARP и RARP;
- `cleanup-interval` — время, по истечении которого производится удаление соединений с истекшим временем жизни;
- `connection-ttl-ip` — время жизни соединений по протоколу IP;
- `connection-ttl-tcp` — время жизни соединений по протоколу TCP;
- `connection-ttl-udp` — время жизни соединений по протоколу UDP;
- `dynamic-ports` — диапазон портов, используемых для динамической трансляции IP-адресов;
- `dynamic-timeouts` — состояние функции динамических тайм-аутов соединений;
- `max-connections` — максимальное количество параллельно установленных соединений.

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

Для просмотра состояния функции блокирования всех IP-пакетов:

```
hostname> iplir option get block-other-protocols
Option: Block-other-protocols State: On
```

iplir option set antispoofing

Включить или выключить [антиспуфинг](#).

Синтаксис

```
iplir option set antispoofing {on | off}
```

Параметры и ключевые слова

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

Значения по умолчанию

Антиспуфинг выключен (`off`).

Режимы командного интерпретатора

Режим администратора.

Пример использования

Включить антиспуфинг:

```
hostname# iplir option set antispoofing on
```

iplir option set block-fragmented-packets

Включить или выключить блокирование входящих фрагментированных IP-пакетов, которые принимаются по всем сетевым интерфейсам.

Синтаксис

```
iplir option set block-fragmented-packets {on | off}
```

Параметры и ключевые слова

- `on` — включить блокирование;
- `off` — отключить блокирование.

Значения по умолчанию

По умолчанию блокирование выключено (`off`).

Режимы командного интерпретатора

Режим администратора.

Пример использования

Включить блокирование:

```
hostname# iplir option set block-fragmented-packets on
```

iplir option set block-other-protocols

Включения или выключить блокировку IP-пакетов, которые передаются по протоколам, отличным от IP, ARP или RARP. Заблокированные IP-пакеты регистрируются в журнале событий под номером 147.

Синтаксис

```
iplir option set block-other-protocols {on | off}
```

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию блокировка выключена (`off`).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Для команды не поддерживается автодополнение при вводе.

Пример использования

```
hostname# iplir option set block-other-protocols on
```

iplir option set cleanup-interval

Настроить временной период, по истечении которого будут удаляться устаревшие соединения (с истекшим тайм-аутом).

Синтаксис

```
iplir option set cleanup-interval <интервал>
```

Параметры и ключевые слова

<интервал> — время в десятых долях секунды. Возможные значения: 0–65535.

Значения по умолчанию

2 секунды (20).

Режимы командного интерпретатора

Режим администратора.

Пример использования

Чтобы устаревшие соединения удалялись по истечении 10 десятых долей секунды (1 секунды):

```
hostname# iplir option set cleanup-interval 10
```

iplir option set connection-ttl-ip

Настройка времени жизни соединения по протоколу IP при отсутствии активности в нем.

Синтаксис

```
iplir option set connection-ttl-ip <значение>
```

Параметры и ключевые слова

<значение> — время жизни в секундах.

Значения по умолчанию

300 секунд.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Для команды не поддерживается автодополнение при вводе

Пример использования

Чтобы задать время жизни соединений по протоколу IP равным 150 секунд:

```
hostname# iplir option set connection-ttl-ip 150
```

iplir option set connection-ttl-tcp

Настройка времени жизни соединения по протоколу TCP при отсутствии активности в нем.

Синтаксис

```
iplir option set connection-ttl-tcp <значение>
```

Параметры и ключевые слова

<значение> — время в секундах.

Значения по умолчанию

1800 секунд.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Для команды не поддерживается автодополнение при вводе

Пример использования

Чтобы задать время жизни соединений по протоколу TCP равным 1500 секунд:

```
hostname# iplir option set connection-ttl-tcp 1500
```

iplir option set connection-ttl-udp

Задать время жизни соединений по протоколу UDP при отсутствии активности в нем.

Синтаксис

```
iplir option set connection-ttl-udp <интервал>
```

Параметры и ключевые слова

<интервал> — время жизни в секундах. Возможные значения: 0–65535.

Значения по умолчанию

300 секунд (300).

Режимы командного интерпретатора

Режим администратора.

Пример

Чтобы задать время жизни соединений по протоколу UDP равным 150 секунд:

```
hostname# iplir option set connection-ttl-udp 150
```

iplir option set dynamic-ports

Задать диапазон портов, используемых для динамической трансляции IP-адресов.

Синтаксис

```
iplir option set dynamic-ports <порт1>--<порт2>
```

Параметры и ключевые слова

- <порт1> — начало диапазона;
- <порт2> — конец диапазона.

Значения по умолчанию

1025–65535.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Для команды не поддерживается автодополнение при вводе

Пример использования

Чтобы задать диапазон портов 32800–64000:

```
hostname# iplir option set dynamic-ports 32800-64000
```

iplir option set dynamic-timeouts

Включить или выключить режим динамических тайм-аутов соединений.

Режим динамических тайм-аутов используется для противодействия флуд-атакам. Когда количество соединений достигает определенного процента от максимума, тайм-ауты всех соединений уменьшаются на определенную величину. Эта величина тем больше, чем ближе число соединений к максимуму. При этом тайм-ауты не уменьшаются ниже определенного минимума. Когда количество соединений уменьшается до определенного процента от максимального, значения тайм-аутов восстанавливаются до исходной величины.

Синтаксис

```
iplir option set dynamic-timeouts {on | off}
```

Параметры и ключевые слова

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

Значения по умолчанию

Режим динамических тайм-аутов выключен (`off`).

Режимы командного интерпретатора

Режим администратора.

Пример

```
hostname# iplir option set dynamic-timeouts on
```

iplir option set max-connections

Задать максимальное количество параллельно установленных соединений.

Синтаксис

```
iplir option set max-connections <количество>
```

Параметры и ключевые слова

<количество> — количество соединений. Допустимый диапазон: 1-1000000.

Значения по умолчанию

Значение по умолчанию, а также максимально возможное значение параметра зависят от используемой аппаратной платформы ViPNet Coordinator KB.

Таблица 1. Значения параметра `max-connections` для разных аппаратных платформ ViPNet Coordinator KB

Аппаратная платформа ViPNet Coordinator KB	Значение по умолчанию	Максимальное значение
KB100 N1	150000	150000
KB100 Q1/Q2	500000	500000
KB1000 Q6	800000	1000000
KB1000 Q8	2000000	4000000
KB2000 Q4	2500000	3000000

Аппаратная платформа ViPNet Coordinator KB	Значение по умолчанию	Максимальное значение
KB2000 Q5	4000000	8000000
KB5000 Q1	6000000	6500000
KB5000 Q2	8000000	16000000

Режимы командного интерпретатора

Режим администратора.

Пример использования

Чтобы установить максимальное количество одновременных соединений равным 200000:

```
hostname# iplir option set max-connections 200000
```

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 пользователя.
- Режим администратора.

Особенности использования

- При вводе идентификатора работают автодополнение и подсказка, данные для подсказки берутся из списка связей ViPNet Coordinator KB с другими узлами.
- Служба `iplircfg` должна быть запущена ([iplir start](#)).

Пример использования

Чтобы проверить связь ViPNet Coordinator KB с узлом, который имеет идентификатор `0x15ea000d`:

```
hostname> iplir ping 0x15ea000d  
Check connection with 0x15ea000d...  
Connection successful
```

iplir set l2overip interface

Задать рабочий интерфейс [L2OverIP](#).

Синтаксис

```
iplir set l2overip interface <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя интерфейса, к которому подключен локальный сегмент сети.

Режимы командного интерпретатора

Режим администратора.

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 KB.

Режимы командного интерпретатора

Режим администратора.

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 администратора.

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 функцию L2OverIP.

Синтаксис

```
iplir set l2overip mode {switch | none}
```

Параметры и ключевые слова

- `switch` — включить функцию L2OverIP.
- `none` — выключить функцию L2OverIP.

Значения по умолчанию

По умолчанию функция L2OverIP выключена (`none`).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Невозможно включить функцию L2OverIP в следующих случаях:

- ViPNet Coordinator KB входит в состав кластера горячего резервирования и в момент выполнения команды находится в пассивном режиме.
- Заданы не все параметры, необходимые для работы функции.

Пример использования

Чтобы включить функцию L2OverIP:

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

iplir set l2overip remote-port

Добавить параметры удаленного сегмента сети в настройках L2OverIP.

Синтаксис

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

Параметры и ключевые слова

- `<порт>` — номер порта удаленного сегмента.

- <IP-адрес> — актуальный IP-адрес видимости ViPNet Coordinator KB, к которому подключен удаленный сегмент сети (реальный или виртуальный адрес удаленного ViPNet Coordinator KB).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Указанный номер удаленного порта должен быть отличен от номера локального порта.
- Можно добавить не более 31 удаленного порта, так как число объединяемых сегментов сети не может быть больше 32.
- Можно указать номер порта, который уже был добавлен. В этом случае будет обновлен IP-адрес удаленного сегмента.

Пример использования

Чтобы добавить удаленный сегмент сети с номером порта 2 и адресом 172.16.2.2:

```
hostname# iplir set l2overip remote-port 2 172.16.2.2
```

iplir set l2overip remote-port delete

Удалить порт с заданным номером из настроек L2OverIP.

Синтаксис

```
iplir set l2overip remote-port <порт> delete
```

Параметры и ключевые слова

<порт> — номер порта, который требуется удалить.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Перед удалением порта выключите L2OverIP (iplir set l2overip mode).
- При выполнении команды запрашивается подтверждение.

Пример использования

Чтобы удалить порт с номером 2:

```
hostname# iplir set l2overip remote-port 2 delete
```

```
Do you want to delete remote port number 2 from L2OverIP configuration? [Yes/No]: y
```

iplir set l2overip unsolicited-frames

Задать режим обработки одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя.

Синтаксис

```
iplir set l2overip unsolicited-frames {drop | broadcast | smart-broadcast}
```

Параметры и ключевые слова

- `drop` — блокировать.
- `broadcast` — обрабатывать как многоадресные с рассылкой на несколько портов:
 - кадры, принятые от локального порта, пересылать на все удаленные порты и на порт с номером 0;
 - кадры, принятые от удаленного порта, пересылать на локальный порт и на порт с номером 0;
 - кадры, принятые от порта с номером 0, пересылать на все удаленные порты и на локальный порт.
- `smart-broadcast` — аналогично режиму `broadcast`, но без обработки кадров от порта с номером 0. В этом режиме кадры, принятые от порта с номером 0, блокируются.
Рекомендуемый режим при использовании технологий агрегирования каналов.

Значения по умолчанию

Установлен режим `drop`.

Режимы командного интерпретатора

Режим администратора.

Пример использования

Чтобы задать режим обработки `smart-broadcast`:

```
hostname# iplir set l2overip unsolicited-frames smart-broadcast
```

iplir set thread-count

Задать количество потоков в драйвере `drviplir`.

Синтаксис

```
iplir set thread-count <количество>
```

Параметры и ключевые слова

<количество> — количество потоков в драйвере `drviplir`.

Значения по умолчанию

Число потоков в драйвере определяется лицензией.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Возможный диапазон значений — от 1 до количества логических процессоров в системе. Если значение параметра выходит за границы допустимого диапазона, то число потоков устанавливается равным ближайшей границе (1 или числу процессоров).
- При выполнении команды подтвердите изменение количества потоков. В результате выводится информация о фактически установленном количестве потоков.

Пример использования

```
hostname# iplir set thread-count 3
```

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 пользователя.
- Режим администратора.

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

Просмотр информации о прохождении IP-трафика через все активные сетевые интерфейсы ViPNet Coordinator KB.

Синтаксис

```
iplir show adapters
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Для выполнения команды драйвер `iplir` должен быть запущен (см. [iplir start](#)).
- Параметр `allowtraffic` показывает, разрешено или заблокировано прохождения IP-трафика через интерфейс.

Пример использования

```
hostname> iplir show adapters

Active interface    Allowtraffic
eth0                on
eth1                on
eth2                off
eth3                on
```

iplir show config

Просмотр конфигурационного файла: основного или сетевого интерфейса.

Синтаксис

```
iplir show config <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя [статического интерфейса](#), конфигурационный файл которого требуется просмотреть.

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Если в команде не указан параметр, то выводится основной конфигурационный файл `iplir.conf`.
- Если в команде указан интерфейс, то выводится конфигурационный файл этого интерфейса и `iplir.conf-<интерфейс>`.
- Для завершения просмотра конфигурационного файла используется клавиша **Q**.

Пример использования

```
hostname> iplir show config
[id]
id= 0x15ea000b
name= Coordinator 2
ip= 10.0.14.101
...
```

iplir show firewall status

Вывести статистику работы межсетевого экрана.

Синтаксис

```
iplir show firewall status
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> iplir show firewall status
Max connections      800000
Dynamicport minimum   4096
Dynamicport maximum   65535
TCP SYN timeout      10
Connection ttl TCP    1800
Connection ttl UDP    300
ICMP timeout         10
Dynamic timeouts      0
Connection ttl IP     300
Total connections count 3960
Public connections count 283
VPN connections count  3677
hostname>
```

По команде выводится следующая информация:

- `Max connections` — максимальное количество одновременных соединений.
- `Dynamicport minimum` — нижняя граница диапазона портов, используемых для динамической трансляции адресов.
- `Dynamicport maximum` — верхняя граница диапазона портов, используемых для динамической трансляции адресов.

Границы диапазона портов для динамической трансляции адресов задаются с помощью команды `iplir option set dynamic-ports`.

- `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.
- `Dynamic timeouts` — состояние динамической корректировки тайм-аутов соединений: 1 — корректировка включена, 0 — корректировка выключена (см. [iplir option set dynamic-timeouts](#)).
- `Connection ttl IP` — время жизни соединения для протоколов, отличных от TCP, UDP, ICMP.
- `Total connections count` — текущее количество открытых и защищенных соединений по всем протоколам.
- `Public connections count` — текущее количество открытых (незашифрованных) соединений по всем протоколам.

- `VPN connections count` — текущее количество защищенных (зашифрованных) соединений по всем протоколам.

iplir show key-info

Просмотреть информацию о ключах, установленных на ViPNet Coordinator KB:

- [персональный ключ пользователя](#);
- [резервный набор персональных ключей \(РНПК\)](#);
- [ключи узла](#).

Синтаксис

```
iplir show key-info
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

Получение информации о ключах может требоваться в следующих случаях:

- Администратору ViPNet Coordinator KB — чтобы убедиться в наличии или отсутствии файла РНПК на узле.
- Сотрудникам технического сопровождения ИнфоТеКС — для выяснения причин возникновения проблем с ключевой системой ViPNet Coordinator KB (например, после обновления справочников и ключей).

Пример использования

```
hostname> iplir show key-info
```

```
Current personal key info: //Информация о персональном ключе
```

```
User ID: 0x16310029
```

```
Current personal key variant: 0
```

```
Master personal key date: 2023-01-23 13:44:57 MSK
```

```
Master personal key number: 1
```

```
Current personal key update date: 2023-01-25 15:40:24 MSK
```

```
Spare personals key set info: //Информация о РНПК
```

```
User ID: 0x16310029
```

```
Personals key variants: from 0 to 19
```

Master personal key date: 2023-06-23 13:44:57 MSK

Master personal key number: 1

Lck key info:

//Информация о ключах узла

User ID: 0x16310029

Master defense key date: 2023-06-23 13:44:57 MSK

Current defense key info:

AP ID: 0x1631002a

Current defense key variant: 0

Master defense key date: 2023-06-23 13:44:57 MSK

Master defense key number: 1

Current defense key update date: 2023-05-25 15:40:24 MSK

Cck key info:

Ap ID: 0x1631002a

Master cck key date: 2023-06-23 13:44:57 MSK

iplir show keys-upgrade-log

Просмотреть журнал, в котором содержится информация о принятых обновлениях [справочников](#) и [ключей](#).

Синтаксис

```
iplir show keys-upgrade-log
```

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# iplir show keys-upgrade-log
19/01/2023 16:37:34.896 Starting upgrade process ...
19/01/2023 16:37:34.896 try find /opt/vipnet/ccc/ap*.dtm
...
```

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 пользователя.
- Режим администратора.

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 thread-count

Вывести количество потоков в драйвере `drviplir`.

Синтаксис

```
iplir show thread-count
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> iplir show thread-count
```

```
3
```

iplir start

Запустить управляющую службу `iplircfg`.

Синтаксис

```
iplir start
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> iplir start
```

```
Loading IpLir
```

iplir stop

Команда используется для завершения работы управляющей службы `iplircfg`.

Синтаксис

```
iplir stop
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

Выполнение команды при работе в удаленной SSH-сессии приведет к потере связи с удаленным сетевым узлом.

Пример использования

```
hostname> iplir stop
Shutting down IpLir
hostname>
```

iplir view

Открыть журнал регистрации IP-пакетов.

Синтаксис

```
iplir view
```

Режимы командного интерпретатора

- Режим администратора.

Особенности использования

- После ввода команды будет запущена программа просмотра с эмуляцией графического интерфейса, на экране появится окно для задания параметров поиска в журнале IP-пакетов. После ввода параметров и поиска нужных записей появится окно с результатом поиска.
- Для выполнения команды требуется, чтобы была запущена служба `iplircfg`.
- При работе ViPNet Coordinator KB в режиме [кластера горячего резервирования](#) на пассивном сервере кластера нельзя просмотреть журнал IP-пакетов.

Пример использования

```
hostname# iplir view
```

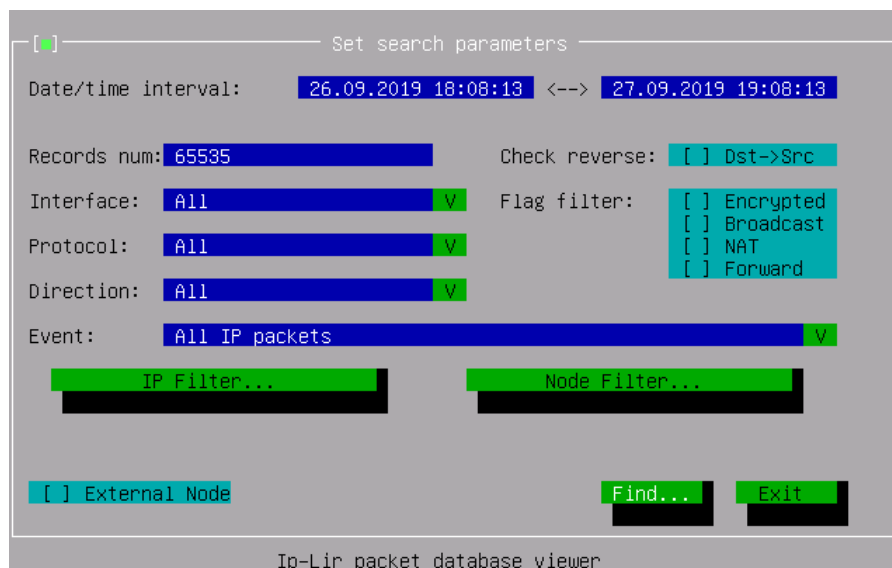


Рисунок 1. Задание параметров поиска записей в журнале регистрации IP-пакетов

Команды группы machine

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

machine halt

Выключить ViPNet Coordinator KB.

Синтаксис

```
machine halt
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine halt
Shutting down failover daemon
Shutting down MFTP daemon
Shutting down IpLir
hostname> The session has been forced to close.
```

machine reboot

Перезагрузить ViPNet Coordinator KB.

Синтаксис

```
machine reboot
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine reboot
```

```
Shutting down failover daemon
Shutting down MFTP daemon
Shutting down IpLir
The session has been forced to close.
...
```

machine self-test

Запустить регламентный контроль ViPNet Coordinator KB.

Синтаксис

```
machine self-test
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Команда недоступна при работе в удаленной SSH-сессии.
- До начала тестирования работа всех служб будет завершена.
- В процессе регламентного контроля производится проверка целостности модулей и конфигурационных файлов, проверка файловых систем на первом и втором разделах загрузочного носителя, проверка контрольных сумм ядра и образа ПО и так далее.
- При обнаружении ошибок искаженные файлы будут восстановлены из резервных копий.
- Если резервная копия искаженного файла не найдена, ViPNet Coordinator KB загрузится, однако службы, отвечающие за работу в сети ViPNet, не будут запущены. Если у вас есть файл экспорта справочников, ключей и настроек с расширением *.vbe, попробуйте восстановить систему, импортировав этот файл. Если восстановить работу ViPNet Coordinator KB не удалось, обратитесь в ИнфоТеКС.
- При успешной проверке целостности будет выведено на экран значение контрольной суммы ПО ViPNet Coordinator KB и запрос подтверждения совпадения контрольной суммы, выведенной на экран, с последней зафиксированной контрольной суммой.



Примечание. Для исполнения ViPNet Coordinator KB1000 Q7 на экран выводятся имена проверенных файлов и шестнадцатеричные значения их контрольных сумм.

- При подтверждении совпадения контрольной суммы, выдаваемой на экран, с последней зафиксированной контрольной суммой генерируется новая контрольная сумма, которая рассчитывается с использованием нового ключа и выводится на экран.



Примечание. Для исполнения ViPNet Coordinator KB1000 Q7 подтверждения не требуется.

- Если контрольная сумма, выдаваемая на экран, не совпадает с последней зафиксированной контрольной суммой, то в ответ на сообщение `Is it correct? [Yes; No]` введите `No` и нажмите **Enter**. После этого ViPNet Coordinator KB автоматически запустит процедуру сброса настроек к заводскому состоянию. Для последующей работы с ViPNet Coordinator KB выполните процедуру ввода в эксплуатацию. Подробное описание процедуры ввода в эксплуатацию приведено в документе «ViPNet Coordinator KB Настройка с помощью командного интерпретатора».
- По завершении процедуры регламентного контроля необходимо перезагрузить ViPNet Coordinator KB. Для этого в ответ на сообщение `Press enter to reboot` необходимо нажать **Enter**.

Пример использования

Чтобы запустить регламентный контроль ViPNet Coordinator KB:

```
hostname# machine self-test

...
If you run selftest, then all daemons will be stopped.
Continue?[Yes/No]: Yes
>> Stop Daemons...
stopped /usr/sbin/crond (pid 6021)
Stopping Advanced Configuration and Power Interface daemon: acpid.
Shutting down IpLir
...

Checksum: 0x2e0a553c

Is it correct? [Yes, No] Yes

>> Run Daemons...

Starting VPN SNMP services: Net-SNMP agent.

Starting VPN SNMP services: ViPNet SNMP plugin.

>> Self test execute successful.

New checksum: 0x4c2af3f2

Press ENTER to reboot...
```

machine set dailyreboot mode

Включить или выключить ежедневную перезагрузку ViPNet Coordinator KB.

Синтаксис

```
machine set dailyreboot mode {on | off}
```

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию ежедневная перезагрузка выключена (`off`).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Во время перезагрузки будет потеряна связь между данным координатором ViPNet Coordinator KB и стоящими за ним узлами, а также связь с туннелируемыми координатором ресурсами.

Пример использования

Чтобы включить ежедневную перезагрузку:

```
hostname# machine set dailyreboot mode on
```

```
Daily reboot is enabled
```

machine set dailyreboot time

Задать время ежедневной перезагрузки ViPNet Coordinator KB.

Синтаксис

```
machine set dailyreboot time <время>
```

Параметры и ключевые слова

<время> — время перезагрузки в формате `hh:mm`, где `hh` — часы (24-часовой формат), `mm` — минуты.

Значения по умолчанию

Время перезагрузки по умолчанию — `00:00`.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- В режиме кластера необходимо устанавливать время перезагрузки на каждом узле, настройки не синхронизируются.
- Рекомендуется устанавливать разное время перезагрузки на узлах кластера с интервалом в 30 минут.

Пример использования

Чтобы настроить ежедневную перезагрузку в 6 часов утра:

```
hostname# machine set dailyreboot time 06:00
```

machine set date

Установить дату и время ViPNet Coordinator KB.

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 администратора.

Особенности использования

Перед установкой даты и времени требуется остановить службы `iplircfg` (см. [iplir stop](#)), `failoverd` (см. [failover stop](#)) и `mftpd` (см. [mftp stop](#)), а после установки восстановить их работу с помощью соответствующих команд.

Если требуется установить время отличающиеся от текущего значения ViPNet Coordinator KB большее чем на 4 часа, то вы можете использовать данную команду для изменения времени в нужную сторону требуемое количество раз, с интервалом изменения времени не более чем 4 часа.

При работе ViPNet Coordinator KB в составе кластера резервирования на пассивной ноде возможность изменения времени блокируется. При вводе команды будет выведено сообщение `Device is in passive mode. Date couldn't be set.`

Пример использования

Чтобы установить дату 22 июля 2023 года и время, равное 12 часам:

```
hostname# machine set date 2023-07-22 12:00:00
```

machine set hostname

Установить имя узла ViPNet Coordinator KB.

Синтаксис

```
machine set hostname <имя>
```

Параметры и ключевые слова

<имя> — имя узла ViPNet Coordinator KB.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- По умолчанию имя узла формируется по шаблону <название>-<идентификатор>, где <название> — наименование аппаратной платформы ViPNet Coordinator KB без последних двух символов, <идентификатор> — идентификатор сетевого узла. Например: KB1000-270E033A.
- Имя узла используется в качестве приглашения командного интерпретатора, а также указывается в начале сообщений, записываемых в протоколы работы при их хранении на жестком диске.
- При вводе имени узла разрешены символы букв, цифры (0-9), дефис «-» и точка «.». Имя не должно начинаться или заканчиваться точкой или символом дефис.

Пример использования

Чтобы установить имя узла KB1000:

```
hostname# machine set hostname KB1000
```

machine set loghost

Задать место хранения системного журнала. С помощью этой команды также можно выключить запись событий в журнал.

Синтаксис

```
machine set loghost {<IP-адрес> | local | null}
```

Параметры и ключевые слова

<IP-адрес> — IP-адрес удаленного сетевого узла, на который должен отправляться системный журнал (удаленное протоколирование).

local — системный журнал хранится на самом ViPNet Coordinator KB (локальное протоколирование).

null — выключение протоколирования.

Значения по умолчанию

По умолчанию во всех исполнениях ViPNet Coordinator KB включено локальное протоколирование (**local**).

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Если системный журнал сохраняется на удаленном узле, то этот узел должен быть доступен для ViPNet Coordinator KB. Если этот узел является открытым, то на ViPNet Coordinator KB должен быть создан фильтр открытой сети, разрешающий исходящий трафик по протоколу UDP на 514-й порт этого открытого узла.
- Не рекомендуется использовать удаленное протоколирование на ViPNet Coordinator KB в режиме кластера горячего резервирования, так как на удаленный сетевой узел не будут передаваться журналы с пассивного сервера, то есть часть информации о работе ViPNet Coordinator KB будет потеряна. Если все же необходимо настроить удаленное протоколирование на кластере, то параметры протоколирования должны быть заданы не только на активном, но и на пассивном сервере кластера, так как данные настройки не передаются с активного сервера на пассивный в ходе резервирования.

Пример использования

Чтобы задать сохранение системного журнала на узле с адресом 192.168.10.10:

```
hostname# machine set loghost 192.168.10.10
```

machine set session-timeout

Задать допустимое время неактивности сессии при удаленном подключении к ViPNet Coordinator KB по протоколу SSH.

Синтаксис

```
machine set session-timeout <время>
```

Параметры и ключевые слова

<время> — время неактивности в минутах, кратное 10 (10, 20, 30 и так далее). Допустимые значения: 0–65530. При значении равном 0 параметр отключен (сессия не будет завершена при неактивности).

Значения по умолчанию

Время неактивности удаленной сессии 30 минут.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

SSH-сессия будет завершена через время неактивности, заданное в параметре <время>, плюс до 5 минут погрешности.

Пример использования

Чтобы установить допустимое время неактивности удаленной сессии 1 час:

```
hostname# machine set session-timeout 60
```

machine set timezone

Установить 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 администратора.

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.
- При работе в режиме кластера горячего резервирования выполнение команды на пассивном узле кластера невозможно. Временная зона на пассивном узле синхронизируется 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
...
hostname# machine set timezone Antarc
```

Чтобы установить часовой пояс Москвы:

```
hostname# machine set timezone Europe/Moscow

Stopping crond... stopped /usr/sbin/crond (pid 6442)

Starting crond...
```

machine show dailyreboot

Просмотреть настройки ежедневной перезагрузки ViPNet Coordinator KB.

Синтаксис

```
machine show dailyreboot
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine show dailyreboot
Daily reboot is on
Daily reboot at 6:00
```

machine show date

Просмотреть дату и время, установленные на ViPNet Coordinator KB.

Синтаксис

```
machine show date
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine show date
Thu Jan 27 19:11:56 MSK +7 2023
```

machine show dnssd log

Вывести содержимое журналов СКЗИ, сохраненных на жестком диске ViPNet Coordinator KB.

Синтаксис

```
machine show dnssd log
```

Режимы командного интерпретатора

Режим администратора.

Пример использования

```
hostname# machine show dnssd log
```

machine show dnssd log usb

Вывести для просмотра журналы СКЗИ, сохраненные на USB-носителе.

Синтаксис

```
machine show dnssd log usb
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

Для просмотра журналов СКЗИ, сохраненных на USB-носителе подключите USB-носитель к ViPNet Coordinator KB.

Чтобы ViPNet Coordinator KB отобразил файлы журнала *.dnssd, они должны быть сохранены в корне файловой системы USB-носителя.

Пример использования

```
hostname# machine show dnssd log usb
```

machine show hostname

Вывести имя узла ViPNet Coordinator KB.

Синтаксис

```
machine show hostname
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine show hostname
```

machine show loghost

Просмотреть настройки хранения системного журнала.

Синтаксис

```
machine show loghost
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

По команде выводится одно из следующих значений:

- `null` — ведение журнала выключено.
- `local` — системный журнал хранится локально на ViPNet Coordinator KB.
- IP-адрес удаленного сетевого узла, заданный с помощью команды `machine set loghost`.

Пример использования

```
hostname> machine show loghost  
The log host set to `local`
```

machine show logs

Просмотреть системный журнал.

Синтаксис

```
machine show logs [reversed] [{since <время> | filtered {<служба> | string <строка>}}]
```

Параметры и ключевые слова

- `reversed` — вывод списка записей в обратном хронологическом порядке.
- `<время>` — вывод записей, начиная с указанного момента времени.
- `<служба>` — вывод записей только для указанной службы в составе ПО ViPNet Coordinator KB.
- `<строка>` — поиск записей журнала по части строки.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Чтобы завершить просмотр нажмите **Q**.
- Параметр `<время>` задается в формате `YYYY-MM-DD hh:mm:ss`

- В параметре `<служба>` можно указать одну из служб в составе ПО ViPNet Coordinator KB. Полный список служб см. в документе «Настройка с помощью командного интерпретатора», разделе «Список служб в составе ViPNet Coordinator KB».

- Для параметра `<строка>` можно использовать символы A-Z, a-z, 0-9, а также следующие символы:

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

Также можно использовать пробел, в этом случае возьмите часть строки в двойные кавычки ("").

- В одной команде `machine show logs` можно одновременно указать только один из параметров `since` или `filtered`. При указании параметра `filtered` можно указать только один из его вариантов `<служба>` или `string <строка>`.

Пример использования

- Чтобы найти все записи системного журнала за все время для всех служб:

```
hostname# machine show logs
```

- Чтобы найти все записи системного журнала, начиная с 14:50 22 февраля 2023 года, и отобразить их в обратном порядке:

```
hostname# machine show logs reversed since 2023-02-22 14:50:00
```

- Чтобы найти все записи системного журнала для службы `vmunix`:

```
hostname# machine show logs filtered vmunix
```

- Чтобы найти записи системного журнала за все время его ведения, для всех служб где есть строка `command 3001`:

```
hostname# machine show logs filtered string "command 3001"
```

machine show memory

Вывести информацию об использовании оперативной памяти, файла подкачки и файловой системы.

Синтаксис

```
machine show memory
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine show memory
```

	total	used	free	shared	buff/cache	available
Mem:	1965	140	972	291	852	1112
Swap:	0	0	0			
...						

machine show session-timeout

Просмотреть допустимое время неактивности сессии.

Синтаксис

```
machine show session-timeout
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine show session-timeout
shell session timeout: 30 minute(s)
```

machine show timezone

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

Синтаксис

```
machine show timezone
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine show timezone
Europe/Samara
```

machine show uptime

Вывести время работы ViPNet Coordinator KB после загрузки, а также среднее число процессов в очереди за ближайшее время.

Синтаксис

```
machine show uptime
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> machine show uptime
18:04:29 up 44 min, 0 user, load average: 2.19, 2.18, 2.06
hostname>
```

По команде отображается следующая информация:

- текущее время;
- время работы ViPNet Coordinator KB после загрузки;
- текущее число пользователей, подключенных удаленно;
- среднее число процессов в очереди за последние 1, 5 и 15 минут. Выводимые значения следует интерпретировать в зависимости от количества процессорных ядер исполнения ViPNet Coordinator KB. Для исполнений с многоядерными процессорами (в том числе с двумя процессорами) критическими являются значения, превышающие общее количество ядер. Например, для исполнений с 4-мя процессорными ядрами значения не должны превышать 4.00 — такие значения говорят о том, что ViPNet Coordinator KB перегружен.



Внимание! Для исполнений с одноядерными процессорами не стоит ориентироваться на эти значения, так как количество запущенных процессов на ViPNet Coordinator KB многократно больше 1. Вместо этого используйте значение `total cpu` в выводе команды [failover show info](#).

machine swap mode

Включить или выключить использование файла подкачки.

Синтаксис

```
machine swap mode {on | off}
```

Параметры и ключевые слова

- `on` — использовать файл подкачки;
- `off` — не использовать файл подкачки.

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Невозможно включить использование файла подкачки, если не был задан его размер (`machine swap set`).
- После выключения использования файл подкачки удаляется.

Пример использования

```
hostname# machine swap mode on
```

```
SWAP is enabled and will be enabled after reboot.
```

machine swap set

Настройка размера файла подкачки.

Синтаксис

```
machine swap set <size>
```

Параметры и ключевые слова

`<size>` — размер файла подкачки в мегабайтах.

Режимы командного интерпретатора

Режим администратора

Особенности использования

- Использование файла подкачки в исполнениях с одним дисковым накопителем невозможно. В результате выполнения команды в указанных исполнениях появится соответствующее сообщение.
- При задании размера файла подкачки на диске должно остаться не менее 256 Мбайт свободного пространства. Если будет задан размер файла подкачки, превышающий размер доступного пространства на диске, появится соответствующее сообщение.

- Просмотреть сведения об использовании оперативной памяти и файле подкачки можно с помощью команды `machine show memory`.

Пример использования

```
hostname# machine swap set 2048

Creating swap. Please, wait... Setting up swapspace version 1, size 2097148 KiB
no label, UUID=of389079-f9f5-4abb-ac2e-a26848eca54c

done.

Activating swap...

done.

hostname#
```

Команды группы mftp

Настройка параметров транспортного сервера MFTP и каналов обмена ViPNet Coordinator KB с другими узлами сети ViPNet.

mftp config

Редактировать конфигурационный файл службы mftpd.

Синтаксис

```
mftp config
```

Режимы командного интерпретатора

Режим администратора.

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.

Синтаксис

```
mftp info
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- Число выводимых записей о конвертах ограничено временем ожидания ответа (30 секунд), но не превышает 400000 записей.
- Для просмотра очереди исходящих конвертов используйте навигационные клавиши.
- Для завершения просмотра используйте клавишу **Q**.

Пример использования

```
hostname> mftp info
Name   Size   Type   Date       Time       Sender Id   Sender Name
@M1~   1390   Mail   15-10-2014  10:40:05   0x1639001b Client-11
0x1639001a Client-10
@M2~   3639   Mail   15-10-2014  10:42:50   0x1639001b Client-11
0x1639001c Client-12
...
hostname>
```

Очередь исходящих конвертов отображается в следующем формате:

```
Name   Size   Type   Date   Time   Sender ID   Sender Name
Receiver ID   Receiver Name
```

где:

- Name — имя конверта.
- Size — размер конверта в килобайтах.
- Type — тип конверта:
 - Mail — **прикладной конверт**;
 - Control request — **управляющий запрос**;
 - Control request answer — **ответ на управляющий запрос**;
 - Task receipt — **прикладная квитанция**;

- o `Transport receipt` — [транспортная квитанция](#).
- `Date, Time` — дата и время создания конверта (первого его появления в очереди).
- `Sender ID` — идентификатор узла-отправителя конверта.
- `Sender Name` — имя узла-отправителя конверта.
- `Receiver ID` — идентификатор узла-получателя конверта.
- `Receiver Name` — имя узла-получателя конверта.

В случае отсутствия конвертов в очереди выводится сообщение `queue is empty`.

mftp show config

Просмотреть конфигурационный файл транспортного сервера MFTP.

Синтаксис

```
mftp show config
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

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 пользователя.
- Режим администратора.

Пример использования

```
hostname> mftp start  
Loading MFTP daemon
```

mftp stop

Завершить работу службы `mftpd` (транспортный сервер MFTP).

Синтаксис

```
mftp stop
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> mftp stop  
Shutting down MFTP daemon
```

mftp view

Вывести журнал конвертов транспортного сервера MFTP.

Синтаксис

```
mftp view
```

Режимы командного интерпретатора

Режим администратора.

Особенности использования

- Если вы выполняете команду на одном из узлов кластера горячего резервирования, отображается только информация о конвертах транспортного сервера, обработанных за периоды, когда этот узел был активным.
- Если имеется несколько файлов журнала транспортных конвертов, то они выводятся по порядку, начиная с последней даты. Чтобы после просмотра одного файла журнала открыть следующий, нажмите клавишу `q` и на запрос командного интерпретатора `Do you want to view the next mftp log file?` ответьте `Yes`.

Пример использования

```
hostname# mftp view
=== MFTP envelopes journal dump at Tue Feb 11 16:45:48 2023
-----
| Envelope filename | Personal envelope name | Sender | Receiver | Date-Time
|   Event           |      Size               | Description | Task      |
-----
| ~OJ) (# (A.RJ9    | ~OJ) (# (A.RJ9          | Admin    | xfva      | 11.02.2023
16:45:48
|   Received        |      19090              |           | File exchange |
-----
-----
```

Журнал отображается в следующем формате:

- `Envelope filename`, `Personal envelope name` — имя конверта.
- `Sender` — имя узла-отправителя конверта.
- `Receiver` — имя узла-получателя конверта.
- `Date-Time` — дата и время события.
- `Event` — событие. Событие может иметь следующие значения:
 - `Received` — конверт получен;
 - `Sent` — конверт отправлен;
 - `Deleted` — конверт удален;
- `Size` — размер конверта в килобайтах.
- `Description` — описание конверта.
- `Task` — прикладная задача, в которой создан конверт.

Команды группы ups

Настройка взаимодействия ViPNet Coordinator KB с [источником бесперебойного питания \(UPS\)](#).

ups set driver

Выбрать драйвер UPS.

Синтаксис

```
ups set driver <драйвер>
```

Параметры и ключевые слова

<драйвер> — название драйвера. В текущей версии ViPNet Coordinator KB можно указать только значение `usbhid-ups`.

Режимы командного интерпретатора

Режим администратора.

Пример использования

Чтобы выбрать драйвер UPS:

```
hostname# ups set driver usbhid-ups
```

ups set mode

Настроить режим взаимодействия ViPNet Coordinator KB 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 администратора.

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 администратора.

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 KB с ИБП.

Синтаксис

```
ups show config
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

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 KB 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 пользователя.
- Режим администратора.

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 KB с ИБП.

Синтаксис

```
ups start
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> ups start
```

ups stop

Завершить работу служб пакета NUT, обеспечивающих взаимодействие ViPNet Coordinator KB с ИБП.

Синтаксис

```
ups stop
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> ups stop
```

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> <важность>]
```

Параметры и ключевые слова

- <источник> — процесс, для которого требуется выключить вывод сообщений.
- <важность> — уровень важности выключаемых сообщений.

Режимы командного интерпретатора

Режим администратора.

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> <важность>]
```

Параметры и ключевые слова

- <источник> — процесс, для которого должны выводиться сообщения. Например:

- o `kern` — ядро;
 - o `user` — пользовательские программы;
 - o `mail` — почтовая система;
 - o `daemon` — службы.
- `<важность>` — уровень важности выводимых сообщений. Например:
 - o `err` — ошибка;
 - o `info` — информационное сообщение;
 - o `debug` — отладочное сообщение.

Значения по умолчанию

- `<источник>` — `daemon`.
- `<важность>` — `debug`.

Режимы командного интерпретатора

Режим администратора.

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 администратора.

Синтаксис

```
enable
```

Режимы командного интерпретатора

Режим пользователя.

Особенности использования

- После выполнения команды требуется указать пароль администратора.
- При вводе пароля на экране ничего не отображается, введенные символы отредактировать нельзя.

Пример использования

```
hostname> enable  
Type the administrator password:
```

exit

Выйти из текущего режима командного интерпретатора.

Синтаксис

```
exit
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

- В режиме администратора происходит переход в режим пользователя.
- В режиме пользователя происходит завершение работы командного интерпретатора. При этом отображается приглашение ввести PIN-код для запуска командного интерпретатора.

Пример использования

```
hostname# exit
```

version features list

Просмотреть список функциональных модулей, входящих в состав текущей версии ViPNet Coordinator KB.

Синтаксис

```
version features list
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> version features list
bonding
dhcp-client
dhcp-relay
dhcp-server
...
```

version

Вывести текущую версию ViPNet Coordinator KB и его компонентов.

Синтаксис

```
version [full]
```

Параметры и ключевые слова

full — вывести текущие версии всех компонентов, а также другие параметры (набор функций для текущего исполнения, архитектура процессора).

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> version full
Product: ViPNet Coordinator KB
Platform: KB1000 Q6
Serial number: 12345678
License: KB1000
Software version: 4.3.3-106
DNSD version 2.0.0,build number: 28
DNSD serial number: 12345678
WebGUI software version: 2.1.0.4204
VPN software version: 4.5.2-1
Iplir driver software version: 4.1.3
Watchdog driver software version: 1.0.5
Feature set: dnsd
```

```
Architecture: x86_64
hostname>
```

По команде выводится название продукта, версия аппаратной платформы ViPNet Coordinator KB и версия ПО ViPNet Coordinator KB. При указании ключевого слова `full` выводятся дополнительные параметры.

webui status

Просмотреть информацию о состоянии службы `webui`, отвечающей за работу веб-интерфейса ViPNet Coordinator KB.

Синтаксис

```
webui status
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Пример использования

```
hostname> webui status
WebUI server is enabled and is running.
```

webui restart

Перезапустить веб-сервер ViPNet Coordinator KB.

Синтаксис

```
webui restart
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

Невозможно перезапустить веб-сервер, если он не был запущен.

Пример использования

```
hostname> webui restart
Shutting down ViPNet Web GUI service
Loading ViPNet Web GUI service
```

who

Просмотреть информацию о запущенных сессиях командного интерпретатора (локальной и удаленных).

Синтаксис

```
who
```

Режимы командного интерпретатора

- Режим пользователя.
- Режим администратора.

Особенности использования

Информация о запущенных сессиях командного интерпретатора обновляется каждые 7 секунд.

Пример использования

```
hostname> who
LINE  HOST          IDLE      MODE  COMMENTS
tty1  local console  00:00:06  user  current
```

Информация отображается в следующем формате:

```
LINE HOST IDLE MODE COMMENTS
```

где:

- `LINE` — имя консоли.
- `HOST` — адрес подключения (для своего узла — `local console`).
- `IDLE` — время неактивности (отсутствие нажатия каких-либо клавиш).
- `MODE` — командный режим: `user` (Режим пользователя) или `admin` (Режим администратора).
- `COMMENTS` — комментарий, содержащий информацию о консоли (обычно информация о местонахождении).

2

Справочник конфигурационных файлов

Файл failover.ini	238
Файл iplir.conf	245
Файл iplir.conf-<интерфейс>	259
Файл mftp.conf	262

Файл failover.ini

Настройка параметров работы системы защиты от сбоев осуществляется путем редактирования конфигурационного файла `failover.ini`.

Чтобы отредактировать файл `failover.ini`:

- 1 Завершите работу службы `failoverd`:

```
hostname# failover stop
```

- 2 Откройте файл для редактирования

```
hostname# failover config edit
```

- 3 Внесите изменения.

- 4 Запустите службу `failoverd`:

```
hostname# failover start
```

Секция [channel]

Каждый сетевой интерфейс активного сервера, работоспособность которого должна контролироваться системой защиты от сбоев при работе в режиме [кластера горячего резервирования](#), должен быть описан секцией `[channel]`.



Примечание. Параметры секций `[channel]` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования.

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 сервера кластера. Если маска не указана, то будет использовано значение маски, установленное в системе. 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. Указывать маску необходимо при организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов.

Независимо от того, в какой нотации была указана маска, после сохранения файла `failover.ini` и запуска службы `failoverd` маска будет перезаписана в нотации CIDR.

- `checkonlyidle` — указание на необходимость проверки только неактивных интерфейсов. 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 горячего резервирования.

- `passiveip` — IP-адрес и маска, которые будет иметь интерфейс пассивного узла кластера. Если маска не указана, то будет использовано значение маски, установленное в системе. Маска может быть указана в таком же формате как в параметре `activeip`.
- `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
```



Примечание. В качестве параметра `testip` не рекомендуется использовать адрес 127.0.0.1, потому что в этом случае контроль работоспособности интерфейса активного узла кластера фактически не будет проводиться: интерфейс активного узла кластера будет считаться работоспособным, так как ответы на эхо-запросы по адресу 127.0.0.1 будут приходить всегда. Использование других адресов из подсети 127.0.0.0/8 запрещено.

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.

Секция `[debug]`

Секция `[debug]` определяет параметры ведения журнала устранения неполадок службы `failoverd` и содержит следующие параметры:

- `debuglevel` — уровень детализации информации, выводимой в журнал. Возможные значения: от 0 до 4 (по умолчанию 3). Чем выше уровень детализации, тем более подробная информация выводится в журнал.
- Не рекомендуется задавать уровень детализации выше 3 для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов АО «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 горячего резервирования и в одиночном режиме:

- `maxjournal` — максимальное количество дней, за которое необходимо хранить записи в журнале переключений кластера горячего резервирования. По умолчанию это ограничение отсутствует.
- `reboot` — задает действия системы в случае обнаружения полной неработоспособности какой-либо службы или драйвера ViPNet Coordinator KB. 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.
- `syncdatetime` — включает или выключает синхронизацию времени и часового пояса между узлами кластера. Становится доступно только после включения ViPNet Coordinator KB в кластер.
 - `yes` (по умолчанию) — синхронизация времени между узлами кластера включена: активный узел кластера передает пассивному узлу данные времени и часового пояса;
 - `no` — синхронизация времени между узлами кластера выключена.

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 горячего резервирования.

Секция `[network]`

Секция `[network]` описывает различные параметры работы системы защиты от сбоев, относящиеся к отправке пакетов в сеть в режиме кластера горячего резервирования.



Примечание. Все параметры секции `[network]` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования. Все параметры этой секции рекомендуется настроить одинаково на обоих серверах кластера.

Секция `[network]` содержит следующие параметры:

- `activeretries` — количество неуспешных попыток опроса пассивным сервером активного сервера, после которых делается вывод об отсутствии активного сервера 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 сервере — для проверки работоспособности интерфейса;
 - на пассивном сервере — для поиска IP-адресов активного сервера.
 Указывается в секундах, по умолчанию — 10.
- `fastdown` — указывает на принудительное выключение сетевых интерфейсов перед перезагрузкой сервера. Возможные значения: `yes` (по умолчанию) или `no`. Значение, выбранное по умолчанию, позволяет быстрее установить отсутствие активного сервера в сети и дать возможность второму серверу перейти в активный режим, однако при этом завершение работы сетевых сервисов происходит уже при выключенных интерфейсах и может быть некорректным.
- `synctime` — период отправки пакетов синхронизации по резервному каналу. Указывается в секундах, значение по умолчанию — 5.
- `timeout` — время ожидания ответа на запрос (эхо-запрос или запрос IP-адресов активного сервера), по истечении которого делается вывод о неуспешности этого запроса. Указывается в секундах, по умолчанию — 2.

Секция `[sendconfig]`

В секции `[sendconfig]` задаются параметры, контролирующие отправку конфигурационных файлов с активного узла на пассивный с целью резервирования.



Примечание. Все параметры секции `[sendconfig]` интерпретируются только при работе системы защиты от сбоев в режиме кластера горячего резервирования.

Секция `[sendconfig]` содержит следующие параметры:

- `activeip` — адрес резервного канала другого узла кластера (который работает в режиме, противоположном режиму данного узла).
- `config` — включение или выключение резервирования группы конфигурационных файлов. Возможные значения: `yes` (по умолчанию) или `no`. В группу входят следующие конфигурационные файлы:
 - файл `iplir.conf`;
 - файлы `iplir.conf`-<интерфейс или группа интерфейсов>, кроме файла для интерфейса резервного канала;
 - файл `mftp.conf` (см. [Файл mftp.conf](#));
 - файлы, содержащие сетевые фильтры и правила трансляции (заданные пользователем и полученные из ViPNet Policy Manager);

- 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 пассивный узел кластера 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` — системное имя интерфейса, который используется для организации резервного канала.
- `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 пересылки этого файла 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 файлов журналов, необходимо установить параметр `config` или `journals` в значение `no` и указать 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 следующие файлы:
 - файлы журналов IP-пакетов сетевых интерфейсов, кроме интерфейса резервного канала;
 - файлы журнала конвертов транспортного модуля MFTP;
 - другие служебные файлы журналов.



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 резервирования 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` или `journals` установлены в значение `yes`. Установка параметра `config` или `journals` в значение `no` означает выключение резервирования соответствующей группы. Не рекомендуется устанавливать параметр `config` в значение `no`, так как это может привести к некорректной работе ПО ViPNet.

- `port` — номер порта, на котором данный активный узел кластера ожидает соединения от пассивного узла для передачи ему файлов для резервирования. По умолчанию — 10090.
- `sendtime` — период резервирования файлов, то есть период между попытками пересылки файлов. Указывается в секундах, по умолчанию — 60.

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 `[adapter]`, то все проходящие через него [IP-пакеты](#) блокируются.

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]`. Если обнаруживается, что интерфейс выключен в системе, 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:
 - `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:

- Если ViPNet Coordinator KB работает в режиме «Без использования межсетевого экрана» или «С динамической трансляцией адресов», то все интерфейсы должны иметь тип `internal`.

- Если ViPNet Coordinator KB работает в режиме «Координатор» или «Со статической трансляцией адресов» (с фиксированным [внешним адресом](#)), то интерфейсу, посредством которого ViPNet Coordinator KB будет связываться с узлом, выполняющим функции [межсетевого экрана](#), следует назначить тип `external`, остальным интерфейсам ViPNet Coordinator KB — 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 устранения неполадок управляющей службы. Она содержит следующие параметры:

- `debuglevel` — уровень детализации информации, выводимой в журнал. Возможные значения: от 0 до 4 (по умолчанию 3). Чем выше уровень детализации, тем более подробная информация выводится в журнал.
- Не рекомендуется задавать уровень детализации выше 3 для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов АО «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 KB. С помощью сервера соединений ViPNet Coordinator KB 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`.

Нередактируемые параметры секции `[dynamic]`

- `firewallip` — внешний [IP-адрес доступа](#) к ViPNet Coordinator KB, работающему в режиме «С динамической трансляцией адресов», со стороны других сетевых узлов.
- `port` — порт назначения, на который следует посылать пакеты для ViPNet Coordinator KB, работающего в режиме «С динамической трансляцией адресов».

Секция `[id]`

Секция `[id]` используется для описания адресных настроек [защищенных узлов](#), связанных с ViPNet Coordinator KB. Каждому узлу, с которым у ViPNet Coordinator KB есть связь, соответствует своя секция `[id]`. Первая секция соответствует собственным настройкам ViPNet Coordinator KB (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 KB.

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 KB.
 - `manual` — задан администратором вручную (редактированием файла `iplir.conf`).
 - `addrdoc` — взят из справочников, полученных из ViPNet Administrator.
 - `agreed-packet-settings` — определяет версию формата зашифрованного IP-пакета и тип шифрования. Может принимать следующие значения:
 - `-1` — версия формата определяется настройками узла ViPNet по умолчанию (версия 4.2 для узлов ViPNet Coordinator KB, версия 4.1 для остальных узлов);
 - `0` — для передачи данных используется формат пакета версии 6.0;
 - `1` — для передачи данных используется формат пакета версии 4.2.
 - `blockforward` — включение или выключение блокирования транзитных пакетов, передаваемых через ViPNet Coordinator KB узлу ViPNet, связанному с ViPNet Coordinator KB. Используется только в секциях `[id]`, описывающих настройки узлов ViPNet, связанных с ViPNet Coordinator KB. Возможные значения:
 - `off` — все транзитные пакеты в направлении узла пропускаются;
 - `on` — все транзитные пакеты в направлении узла блокируются с кодом 70.
- По умолчанию этот параметр отсутствует, что эквивалентно значению `off`.
- `fixfirewall` — режим фиксации настроек работы собственного узла через внешний межсетевой экран:

- o `off` (по умолчанию) — внешний IP-адрес и порт доступа к ViPNet Coordinator KB определяются автоматически по информации от узлов внешней сети;
 - o `on` — внешний IP-адрес и порт доступа к ViPNet Coordinator KB заданы администратором в параметрах `firewallip` и `port` данной секции.
- `ip` — [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`. При этом 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` — 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:
 - o в собственной секции `[id]`:
 - `0xfffffffffe` — при работе в режиме «С динамической трансляцией адресов» (если в секции `[dynamic]` параметр `dynamic_proxy` установлен в `on` (см. [Секция \[dynamic\]](#)));
 - `0x00000000` — при работе в режиме «Со статической трансляцией адресов» (если в собственной секции `[id]` параметр `usefirewall` установлен в `on`);
 - идентификатор собственного координатора — при работе в режиме «Без использования межсетевого экрана» (если в собственной секции `[id]` параметр `usefirewall` установлен в `off`). Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`.
 - o в любой секции `[id]`, кроме собственной:
 - `0xfffffffffe` — при работе в режимах «Со статической трансляцией адресов» или «С динамической трансляцией адресов», если ViPNet Coordinator KB является [сервером соединений](#) для узла;
 - `0` — при работе в режиме «Без использования межсетевого экрана»;
 - идентификатор координатора — при работе в режимах «Координатор» или «С динамической трансляцией адресов». Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`.
- `tunnel` — адреса незащищенных компьютеров, [туннелируемых ViPNet Coordinator KB](#) (указаны в собственной секции) или [другими координаторами](#), в виде: `<ip1>-<ip2> to <ip3>-<ip4>`, где:
 - o `<ip1>-<ip2>` — начальный и конечный реальные адреса диапазона туннелируемых узлов;

- `<ip3>-<ip4>` — диапазон виртуальных адресов, которые соответствуют реальным адресам из диапазона `<ip1>-<ip2>`, и которые будут использоваться вместо реальных адресов туннелируемых узлов, если на узле, который к ним обращается, настроена видимость по виртуальным адресам. Например, 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]`, который может принимать одно из двух значений:

- `auto` — параметры `<ip1>` и `<ip2>` задаются администратором сети ViPNet в ViPNet Центр управления сетью или вручную на ViPNet Coordinator KB.

Например, чтобы в автоматическом режиме указать, что координатор туннелирует адреса с 192.168.0.1 по 192.168.0.100, достаточно сделать следующую запись:

```
tunnel= 192.168.0.1-192.168.0.100
```

- `manual` — параметры `<ip1>-<ip2>` и `<ip3>` задаются вручную. Начальный адрес диапазона виртуальной видимости туннелируемых узлов `ip3` также необходимо указать вручную на каждом узле ViPNet, который будет работать с этими узлами.

Например, чтобы вручную указать, что координатор туннелирует адреса с 192.168.0.1 по 192.168.0.100, а соответствующий им виртуальный диапазон адресов — 192.120.0.1-192.120.0.100, следует сделать следующую запись:

```
tunnel= 192.168.0.1-192.168.0.100 to 192.120.0.1
```

В одной секции `[id]` может быть задано не более чем 1000 параметров `tunnel`.

Внимание! В зависимости от значения параметра `tunnel_virt_assignment` секции `[misc]`, настройки параметра `tunnel` действуют следующим образом:



- Для автоматического режима назначения виртуальных адресов — можно задавать только первый и второй IP-адрес.
 - Для ручного режима назначения виртуальных адресов — можно задать значения всех четырех IP-адресов.
-

- `exclude_from_tunnels` — используется в любой секции `[id]`, кроме собственной. Исключает адреса из списка туннелируемых координатором адресов, указанных в параметре `tunnel`. Задается в виде: `ip1-ip2`, где `ip1` и `ip2` — начальный и конечный реальные адреса диапазона, который не надо туннелировать.

Например, чтобы исключить адрес 192.168.201.7 из туннелируемого диапазона 192.168.201.5-192.168.201.10 (то есть не шифровать трафик при соединении с узлом, имеющим адрес 192.168.201.7), необходимо сделать следующую запись:

```
exclude_from_tunnels= 192.168.201.7-192.168.201.7
```

В одной секции `[id]` можно задать несколько таких параметров.



Внимание! Параметр `exclude_from_tunnels` имеет приоритет над настройками туннелирования, получаемыми из ЦУСа, и не изменяется при получении новых настроек туннелирования.

- `tunnelvisibility` — тип видимости для всех узлов, туннелируемых координатором. Используется в любых секциях `[id]` кроме собственной. Возможные значения:
 - `real` — всегда обращаться к туннелируемым узлам по их реальным адресам;
 - `virtual` — всегда обращаться к туннелируемым узлам по их виртуальным адресам.Если в какой-либо секции `[id]` есть назначенные виртуальные адреса, то параметру присваивается значение `virtual`. Значение данного параметра по умолчанию определяется параметром `tunneldefault` секции `[visibility]`.
- `tunnel_local_networks` — режим туннелирования IP-адресов, входящих в локальную подсеть ViPNet Coordinator KB. Возможные значения:
 - `on` (по умолчанию) — обращаться к туннелируемым узлам только через координатор, который туннелирует данные узлы;
 - `off` — обращаться к узлам, находящимся в локальной подсети, минуя координатор, который туннелирует эти узлы. Рекомендуется использовать в случае, если затруднен доступ к туннелируемым узлам в локальной подсети.
- `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 KB с узлами, которые туннелирует данный координатор, трафик шифроваться не будет.
- `usefirewall` — может принимать значение `on` или `off` и используется в секциях `[id]` в следующих целях:
 - Во всех секциях `[id]`, кроме собственной, — указывает на использование настроек работы через межсетевой экран с данным узлом. Если этот параметр имеет значение `off`, то параметры `firewallip`, `port` и `proxyid` в этой секции игнорируются, и работа с данным узлом будет возможна только по одному из его реальных IP-адресов.
 - В собственной секции `[id]` — указывает на использование внешнего межсетевого экрана. В случае если межсетевой экран использоваться не будет, он установлен в значение `off`, в остальных случаях — в значение `on` (см. описание параметра `proxyid` данной секции).
- `visibility` — тип видимости узла. Используется в любой секции `[id]` кроме собственной. Возможные значения:
 - `auto` — автоматически определять тип видимости узла, в зависимости от текущего [адреса видимости узла](#).
 - `real` — всегда обращаться к данному узлу по его реальному адресу.
 - `virtual` — всегда обращаться к данному узлу по его виртуальному адресу.

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]`, то есть параметрами видимости всей сети, к которой этот узел принадлежит, либо параметрами видимости узлов по умолчанию.



Примечание. Использовать параметр `visibility` нужно осторожно, так как у сетевых узлов, которые видны по виртуальным адресам, могут совпадать реальные адреса (если эти узлы находятся в частных сетях).

Нередактируемые параметры

- `accessip` — текущий **IP-адрес доступа к узлу** со стороны ViPNet Coordinator KB. Может принимать значение одного из реальных или виртуальных IP-адресов, в зависимости от физической топологии сети, режимов подключения к внешней сети ViPNet Coordinator KB 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 Administrator. 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 Administrator 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 различные дополнительные параметры:

- `client_pollinterval` — период опроса координатора ViPNet Coordinator KB **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 KB). 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.

- `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).
- `timediff` — максимально допустимая разница между временем отправки и временем 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. Вы можете задать значение `timediff` от 1 до максимального значения, зависящего от аппаратной платформы. Значение по умолчанию — 6.

Таблица 2. Значения `timediff` для разных аппаратных платформ ViPNet Coordinator KB

Аппаратная платформа	Значение по умолчанию, сек	Максимальное значение, сек
KB100 N1	6	236
KB100 Q1/Q2	6	85
KB1000 Q6, Q8	6	52
KB2000 Q4	6	16
KB2000 Q5	6	8
KB5000 Q1	6	10
KB5000 Q2	6	6

- `timesync` — включение или выключение автоматической установки времени на клиенте в соответствии со временем на координаторе, который служит сервером IP-адресов для этого клиента. На координаторе этот параметр по умолчанию установлен в значение `off`, изменять его не следует.
- `tunnel_virt_assignment` — параметр, определяющий режим назначения виртуальных адресов для узлов, туннелируемых координатором. Возможные значения:
 - `auto` (по умолчанию) — виртуальные адреса туннелируемых узлов задаются автоматически.
 - `manual` — виртуальные адреса туннелируемых узлов задаются вручную в параметрах `tunnel` и `exclude_from_tunnels` [секции \[id\]](#).
- `warnoldautosave` — параметр, включающий или выключающий предупреждения о наличии конфигураций, содержащих настройки ПО ViPNet Coordinator KB, 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 не редактируемый параметр `server`, в котором через запятую указаны идентификатор координатора и его имя.

Секция [virtualip]

Секция `[virtualip]` описывает настройки [виртуальных IP-адресов](#) и содержит следующие параметры:

- `maxvirtualip` — максимальный адрес для формирования базовых виртуальных адресов защищенных узлов (по умолчанию — `11.0.255.255`). Используется для ограничения диапазона назначаемых базовых виртуальных адресов. По умолчанию параметр `maxvirtualip` соответствует максимально возможному адресу, то есть адресу, у которого два старших октета совпадают с этими же октетами стартового адреса `startvirtualip`, а два младших октета равны 255. Данное значение можно уменьшить, при этом необходимо следить за тем, чтобы оно было больше значения параметра `endvirtualip`.
- `startvirtualip` — стартовый адрес для формирования базовых виртуальных адресов защищенных узлов (по умолчанию — `11.0.0.1`). При изменении данного параметра назначение всех базовых виртуальных адресов узлов производится заново, как при начальном формировании конфигурационных файлов. 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).

Нередактируемые параметры секции [virtualip]

- `endvirtualip` — служебный параметр, в котором хранится следующий за последним назначенным [базовый виртуальный адрес](#). Используется в качестве точки отсчета при поиске и назначении базовых виртуальных адресов для новых защищенных узлов. При назначении базовых виртуальных адресов сначала проверяется, есть ли свободный виртуальный адрес в диапазоне от `startvirtualip` до `endvirtualip`, оказавшийся таковым в результате удаления одного из узлов и, если такой есть, то назначается этот свободный виртуальный адрес. Если — нет, то производится поиск первого свободного адреса в диапазоне от `endvirtualip` до `maxvirtualip`.

Секция [visibility]

Секция `[visibility]` содержит настройки видимости защищенных сетевых узлов, с которыми связан ViPNet Coordinator KB. В отличие от параметра `visibility`, с помощью которого [в секциях \[id\]](#) задается видимость отдельных узлов, в этой секции можно задать видимость сразу для всех узлов сетей или подсетей ViPNet. Настройки, заданные в секции `[visibility]`, учитываются при определении видимости узлов со стороны собственного узла.

Секция может содержать следующие параметры:

- `default` — видимость узлов по умолчанию. Возможные значения:
 - `auto` (по умолчанию) — автоматическое определение видимости узлов;
 - `real` — доступ к узлам по их [реальным IP-адресам](#);
 - `virtual` — доступ к узлам по их [виртуальным IP-адресам](#).
- `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.

Секция [packet-settings]

Секция `[packet-settings]` содержит параметры, которые используются протоколом IPliq и алгоритмом шифрования. Может существовать несколько таких секций с разным набором параметров.

Секция `[packet-settings]` содержит следующие параметры:

- `name` — имя конфигурации, представляет собой произвольно заданную строку.
- `format` — версия используемого протокола IPlir. Может принимать следующие значения:
 - `il4x` — использование версии 4.1 и 4.2 протокола IPlir. При указании этого значения параметр `cs` игнорируется. Данные версии протокола используются для совместимости с другими узлами сети ViPNet, не поддерживающими протокол IPlir версии 6.0.
 - `il60` — использование версии 6.0 протокола IPlir.
- `cs` — алгоритм шифрования. В ViPNet Coordinator KB поддерживается значение параметра 2, что соответствует алгоритму шифрования по ГОСТ 28147-89 в режиме CTR с алгоритмом выработки произвольного ключа для протокола IPlir 6.0 и замены блока подстановки алгоритма шифрования ГОСТ 28147-89.

Секция `[protection]`

Секция `[protection]` содержит параметры защищенной связи, определяющие порядок выбора алгоритма шифрования между ViPNet Coordinator KB и другими узлами сети ViPNet. Секция содержит следующие параметры:

- `list` — список разрешенных конфигураций защищенного взаимодействия. Представляет собой перечисление через запятую имен конфигураций, заданных в секциях `[packet-settings]` (см. [Секция `\[packet-settings\]`](#)). На первом месте в списке стоит более приоритетная конфигурация.
- `default` — значение, определяющее параметры защищенного соединения по умолчанию. Значение представляет собой имя конфигурации, заданное в одной из секций `[packet-settings]` (см. [Секция `\[packet-settings\]`](#)). Данный параметр не является обязательным, при его отсутствии используется значение из списка, заданного в параметре `list`, с наименьшим приоритетом.



Примечание. Если указана конфигурация, которая определяет параметры защищенного соединения с узлами по протоколу IPlir версии 6.0, то связь будет только с узлами в сети ViPNet, которые поддерживают эту версию протокола. Если указана конфигурация, которая определяет параметры соединения с узлами по протоколу более ранней версии, то соединение с такими узлами будет установлено по тому протоколу, который они поддерживают.

- `min_dynamic` — имя конфигурации, ограничивающей множество конфигураций, доступных для динамического согласования параметров защищенного взаимодействия. Данный параметр не является обязательным, при его отсутствии динамическое согласование запрещено.
- `min_allowed` — имя конфигурации, ограничивающее минимальную по приоритету конфигурацию из списка, заданного в параметре `list`, используемую для динамического согласования параметров защищенного взаимодействия. Данный параметр не является

обязательным, при его отсутствии используется конфигурация, определенная в значении параметра `default`.

- `always_min_allowed` — параметр, определяющий возможность использования конфигурации, заданной в параметре `min_allowed`, для динамического согласования параметров защищенного взаимодействия с узлом сети ViPNet, если для взаимодействия с этим узлом определена более приоритетная конфигурация из списка, заданного в параметре `list`. Параметр представляет собой имя конфигурации из списка, заданного в параметре `list`.

Файл `iplir.conf`-<интерфейс>

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`, управляющая служба при запуске автоматически создает такой файл с параметрами по умолчанию.

Для редактирования этих файлов используется команда:

```
iplir config <интерфейс>
```

Перед редактированием файла `iplir.conf`-<имя интерфейса> необходимо завершить работу управляющей службы командой `iplir stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его командой `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` вручную рекомендуется сначала запустить управляющую службу командой `iplir start`, затем завершить его работу командой `iplir stop`, после чего отредактировать нужный файл `iplir.conf`-<интерфейс> и снова запустить управляющую службу.

Каждый файл `iplir.conf`-<интерфейс> содержит только одну секцию `[db]`, описанную ниже.

Для каждого интерфейса ведется свой журнал, который хранится в файле `iplir.db`-<интерфейс>, расположенном в подкаталоге `iplirdb` каталога, содержащего файлы `iplir.conf`-<имя интерфейса>.

Записи о пакетах накапливаются в журнале регистрации служебного трафика 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.

Таблица 3. Размер по умолчанию и максимальный размер журнала IP-пакетов

Исполнение	Размер журнала IP-пакетов по умолчанию (Мбайт)	Максимальный размер журнала IP-пакетов (Мбайт)
KB100	50	50
KB1000	50	для физических интерфейсов — 200 для виртуальных интерфейсов — 1800
KB2000	50	для физических интерфейсов — 200

Исполнение	Размер журнала IP-пакетов по умолчанию (Мбайт)	Максимальный размер журнала IP-пакетов (Мбайт)
KB5000	50	для виртуальных интерфейсов — 1800
		для физических интерфейсов — 200
		для виртуальных интерфейсов — 1800

Секция [db] содержит следующие параметры:

- `maxsize` — максимальный размер журнала в мегабайтах (по умолчанию — 50 Мбайт).
Каждый раз при запуске управляющей службы в значение параметра `maxsize` после размера журнала автоматически дописывается слово `MBytes`, если оно отсутствует. Поэтому при изменении значения этого параметра его можно не писать. Значение параметра 0 выключает ведение журнала. При этом если до выключения журнала в нем были записи, то просмотреть их будет невозможно.
- `timedif` — интервал времени, в течение которого одинаковые события объединяются в журнале в одну запись. Задается в секундах, значение по умолчанию — 60. Если этот параметр установлен в 0, то объединение событий не используется. В этом случае при интенсивном трафике в журнале могут регистрироваться не все пакеты.
- `registerall` — включение или выключение регистрации записей обо всех пакетах, проходящих через интерфейс. Возможные значения: `off` (по умолчанию) или `on`. То есть по умолчанию регистрируются только записи о заблокированных пакетах и изменении адресов сетевых узлов.
- `registerbroadcast` — включение или выключение регистрации записей о широковещательных пакетах. Возможные значения: `off` (по умолчанию) или `on`.
- `omittcpclientport` — включение или выключение скрытия информации о порте клиента ViPNet при соединении по протоколу TCP. Возможные значения: `off` (по умолчанию) или `on`.

Обычно порт клиента при TCP-соединении выделяется динамически и никакой полезной информации не несет. Если с какого-либо сетевого ресурса производятся попытки подключиться к какому-либо порту на компьютере, а соединение по каким-то причинам не будет установлено, то при следующей попытке установить соединение с того же ресурса будет использоваться другой порт. При использовании сканеров портов или каких-либо сетевых атаках число таких попыток может достигать нескольких сотен в секунду. Поскольку клиент использует каждый раз разные порты, то такие пакеты не считаются одинаковыми и для каждого из них создается своя запись в журнале, что засоряет его и затрудняет последующий анализ. Если параметр `omittcpclientport` установлен в значение `on`, порт клиента при TCP-соединении не регистрируется и не учитывается, а в журнале числовое значение номера порта указывается равным нулю, что позволяет объединить события о попытках подключения к какому-либо порту на компьютере с определенного адреса в одну запись. Это часто бывает удобно.

- `registerevents` — включение или выключение регистрации служебных событий. Список служебных событий см. в документе «ViPNet Coordinator KB. Настройка с помощью командного

интерпретатора», в приложении «Типы событий в журнале регистрации IP-пакетов».
Возможные значения: `off` или `on` (по умолчанию).

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 KB может обмениваться данными с другими узлами. Каждому узлу, с которым у ViPNet Coordinator KB есть связь, соответствует своя секция `[channel]`. Набор параметров в каждой секции зависит от типа выбранного канала. По умолчанию при создании файла конфигурации для всех каналов устанавливается тип `mftp`.



Внимание! Добавление и удаление секций `[channel]` осуществляется автоматически, делать это вручную не следует.

Секции `[channel]` для каналов любого типа содержат следующие параметры:

- `type` — тип канала. Возможные значения: `mftp` (по умолчанию), `smtp`, `viaroute` (подробнее см. в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора», в главе «Настройка транспортного модуля»).
- `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:

- o `yes` — попытка передачи конверта по каналу производится немедленно (по умолчанию для каналов обмена с координаторами).
- o `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.

Нередактируемые параметры секции [channel]

- `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.

Кроме того, для каждого из типов каналов существуют специфические параметры, описанные ниже.

Специфические параметры для канала MFTP

Для канала MFTP в секции [channel] дополнительно задаются следующие параметры:

- `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` — уникальный идентификатор сетевого узла ViPNet, на который необходимо перенаправлять конверты, отправляемые по данному каналу. Используется для настройки каналов обмена с координаторами при межсетевом взаимодействии и позволяет снизить нагрузку на шлюзовую координатор за счет передачи через него конвертов без обработки транспортным модулем. Идентификатор указывается в шестнадцатеричном формате с префиксом `0x`, например: `transit = 0x270e000a`.

Нередактируемые параметры для канала MFTP

- `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 [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`).
- `app_in_path` — абсолютный путь к каталогу, в который помещаются файлы, полученные от других узлов сети ViPNet (по умолчанию — `/opt/vipnet/in/app`).

Секция [mailtrans]

Секция [mailtrans] содержит параметры, отвечающие за взаимодействие транспортного модуля с модулем почтового обмена mailtrans.

Секция [mailtrans] содержит следующие параметры:

- `frommailbox` — адрес электронной почты отправителя SMTP-конвертов в формате:
`frommailbox = <имя пользователя>@<сервер>.<домен>`
- `inputmailbox` — адрес электронной почты, по которому модуль почтового обмена будет забирать конверты по протоколу POP3, в формате:

```
inputmailbox = <имя пользователя>:<пароль>@<IP-адрес POP3-сервера>
```

- `mailtrans_bin` — абсолютный путь к исполняемому файлу модуля почтового обмена (по умолчанию — `/sbin/mailtrans`).
- `mail_call_timeout` — период вызова модуля почтового обмена, то есть период опроса адреса электронной почты для входящих и исходящих конвертов по каналу SMTP. По умолчанию вызов не производится (`mail_call_timeout = -1`). Однако при наличии в очереди исходящих конвертов, предназначенных для отправки по каналу SMTP, вызов будет производиться, если это не запрещено параметром `call_flag` соответствующего канала.
- `mail_in_chunks_path` — абсолютный путь к каталогу, в который модуль почтового обмена помещает принятые фрагменты SMTP-конвертов в случае использования протокола версии 2.0. По умолчанию — `/opt/vipnet/smtpin/chunks`.
- `mail_in_path` — абсолютный путь к каталогу, в который модуль почтового обмена помещает принятые конверты. По умолчанию — `/opt/vipnet/smtpin`.
- `mail_out_path` — абсолютный путь к каталогу, в котором транспортный модуль формирует заголовочные файлы на отправляемые конверты. По умолчанию — `/opt/vipnet/smtpout`.
- `outputmailbox` — IP-адрес SMTP-сервера, на который модуль почтового обмена будет отправлять конверты по протоколу SMTP.
- `maxsmtpsize` — максимальный размер почтового SMTP-конверта при отправке (в килобайтах). Используется в случае, если в параметре `version` данной секции установлена версия протокола 2.0. При отправке MFTP-конверт разбивается на несколько SMTP-конвертов, размер каждого из которых не превышает заданный параметром `maxsmtpsize`. Возможные значения: от 100 до 2048000 (2 Гбайт). Значение 0 означает, что ограничение на размер SMTP-конвертов отсутствует.

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.2023.09.23`.
- `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.
- `t1lctl` — 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 `t1lctl`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `t1lout` — 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 `t1lout`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `t1ltrash` — 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 `t1ltrash`, 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 потребуются повторная настройка обхода шлюзовых координаторов.

Секция `[debug]`

Секция `[debug]` определяет параметры ведения системного журнала транспортного сервера и содержит следующие параметры:

- `debuglevel` — уровень детализации информации, выводимой в журнал. Возможные значения: от 0 до 4 (по умолчанию 3). Чем выше уровень детализации, тем более подробная информация выводится в журнал.

Не рекомендуется задавать уровень детализации выше 3 для постоянного использования, так как эти уровни используются только для диагностики возможных проблем и должны быть включены только по рекомендации специалистов АО «ИнфоТеКС».

- `debuglogfile` — источник информации, выводимой в журнал, в формате: `syslog:<facility.level>`, где:
 - `facility` — процесс, формирующий информацию. Возможные значения: `kern` (ядро), `user` (пользовательские программы), `mail` (почтовая система) или `daemon` (системные службы).
 - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

Секция [reserv]

Секция `[reserv]` содержит параметры настройки транспортного модуля на координаторе, работающем в составе кластера горячего резервирования:

- `cmd_port` — порт, на котором служба `mftpd` пассивного сервера ожидает соединений с активным сервером по резервному каналу для приема управляющих команд (по умолчанию — 6084). Данный параметр должен иметь одинаковое значение в конфигурационных файлах транспортного модуля 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 горячего резервирования:
 - `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 кластере горячего резервирования 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 `t1lctl` секции `[misc]`.
-

Секция [upgrade]

Данная секция полностью игнорируется в процессе функционирования ViPNet Coordinator KB.



Термины и сокращения

DHCP-сервер

Сервер, автоматически администрирующий IP-адреса DHCP-клиентов и выполняющий соответствующую настройку для сети.

DNS-сервер

Хранит информацию о соответствии доменных имен интернет-узлов их IP-адресам и предоставляет эту информацию по запросам.

IP-пакет

Форматированный блок информации, передаваемый в сети по протоколу IP.

IP-трафик

Поток данных, передаваемых в сети по протоколу IP.

IP-форвардинг

IP-форвардинг или маршрутизация транзитных IP-пакетов (не предназначенных для этого компьютера), является опциональной возможностью стека протоколов TCP/IP в операционной системе GNU/Linux. Данная функция обеспечивает пересылку транзитных IP-пакетов через сетевые интерфейсы компьютера.

L2OverIP

Технология, которая позволяет организовать защиту удаленных сегментов сети, использующих одно и то же адресное пространство, на канальном уровне модели OSI. В результате узлы из разных сегментов сети смогут взаимодействовать друг с другом в одном широковещательном

доме. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

NTP-сервер

Сервер, с помощью которого можно синхронизировать время на компьютерах и других сетевых устройствах. Получает значение времени от эталонного источника по протоколу NTP и передает его на устройства.

NUT (Network UPS Tools)

Пакет программ для управления и мониторинга работы источника бесперебойного питания (UPS).

OSPF (Open Shortest Path First)

Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала для нахождения кратчайшего маршрута. Распространяет информацию о доступных маршрутах внутри автономной системы.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

VLAN

Виртуальная локальная компьютерная сеть, представляет собой группу сетевых узлов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к ширококвещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет узлам группироваться вместе, даже если они не находятся в одной физической сети.

WINS-сервер

Сервер, выполняющий сопоставление NetBIOS-имен компьютеров с IP-адресами узлов.

Административная дистанция

Характеристика [маршрута](#). Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

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 и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet и по которым приложения отправляют свой трафик.

Адреса доступа

IP-адреса, по которым узел доступен в сети (например, адреса межсетевого экрана, за которым он находится).

Антиспуфинг

Защита от спуфинг-атак, при которых злоумышленник подделывает адрес источника для обхода межсетевых экранов и организации DoS-атак (от англ. Denial of Service, отказ в обслуживании).

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.

Вес

Параметр, который задается для шлюза в статическом [маршруте](#) в виде целого числа в диапазоне от 1 до 255. Позволяет настроить балансировку IP-трафика между шлюзами в одинаковый адрес назначения. Определяет долю IP-трафика, который должен передаваться по маршруту на указанный шлюз.

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.

Внешние IP-адреса

Адреса внешней сети.

Датчик несанкционированного доступа (ДНСД)

Устройство для контроля доступа к средству криптографической защиты информации.

Используется для экстренного удаления ключевой информации при попытке несанкционированного доступа.

Дистрибутив ключей

Файл с расширением *.dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии для первичного запуска и последующей работы программы ViPNet на сетевом узле. Для работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Дуплекс

Способ связи, при котором сетевой интерфейс может одновременно и передавать, и принимать информацию.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Инкапсуляция пакетов

Принцип передачи данных, при котором данные в формате одного протокола упаковываются в формат другого протокола.

Источник бесперебойного питания (ИБП)

Автоматическое электронное устройство с аккумуляторной батареей, предназначенное для бесперебойного кратковременного снабжения электрической энергией с целью корректного завершения работы и сохранения данных в случае резкого падения или отсутствия входного питающего напряжения системы.

Класс сетевого интерфейса

Признак, определяющий назначение сетевого интерфейса. В ViPNet Coordinator KB сетевым интерфейсам можно назначить следующие классы: `access`, `trunk`, `slave`.

По умолчанию сетевому интерфейсу назначен класс `access`. Если требуется, чтобы сетевой интерфейс или агрегированный сетевой интерфейс обрабатывал трафик из нескольких VLAN, ему необходимо назначить класс `trunk`. Чтобы объединить несколько сетевых интерфейсов в агрегированный сетевой интерфейс, каждому из таких интерфейсов необходимо предварительно назначить класс `slave`.

Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных ViPNet Coordinator KB, 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 KB на активном ViPNet Coordinator KB, пассивный ViPNet Coordinator KB переключается в активный режим для выполнения функций. При этом сбойный ViPNet Coordinator KB 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.

Ключевой блокнот ДСДР

Ключевой блокнот ДСДР содержит ключевую информацию, которая используется для шифрования конфиденциальной информации. ДСДР используется в средствах криптографической защиты данных, не содержащих сведений, составляющих государственную тайну.

Ключи узла ViPNet

Совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

Командный интерпретатор

Командная оболочка, предназначенная для администрирования программного обеспечения ViPNet Coordinator KB 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.

Маршрут

Путь следования IP-трафика при передаче в сети от одного узла другому.

Маршрут по умолчанию

Путь следования IP-пакетов, для которых не был найден подходящий маршрут в таблице маршрутизации.

Маршрутизатор-сосед

OSPF-маршрутизатор, находящиеся в одной области маршрутизации с другими маршрутизаторами этого типа.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних IP-адресов в адреса, доступные из внешней сети (выполняет NAT).

Метрика адреса доступа

Определяет задержку (в миллисекундах) отправки тестовых пакетов при выполнении опроса узла для определения доступности адреса. Предназначена для задания приоритета использования каналов связи.

Метрика маршрута

Параметр, определяющий приоритет маршрута передачи IP-трафика.

Область маршрутизации

Одна или несколько IP-сетей, в которых осуществляется обмен информацией по определенному протоколу, в частности, по протоколу [OSPF](#).

Протокол OSPF рассматривает межсетевую среду как множество областей, соединенных друг с другом через некоторую базовую область (backbone area). Для идентификации областей каждой из них выделяется специальный идентификатор (area ID), представляющий собой целое число в десятичном формате.

Перераспределение маршрутов

Обмен маршрутной информацией между двумя различными маршрутизирующими протоколами.

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

Полудуплекс

Способ связи, при котором сетевой интерфейс в один момент времени может только передавать или только принимать информацию.

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.

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ создает для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер принимает и передаёт IP-пакеты. Физическим интерфейсом может служить сетевой адаптер Ethernet, виртуальным — агрегированный интерфейс, интерфейс для VLAN.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Справочники и ключи

Справочники, [ключи узла](#) и ключи пользователя.

Статический сетевой интерфейс

[Сетевой интерфейс](#), для работы которого требуется задать секцию `[adapter]` в файле `iplir.conf` с описанием параметров этого интерфейса. К таким интерфейсам относятся физические (Ethernet) и виртуальные (VLAN) интерфейсы.

Стоимость маршрута

Количество издержек, которые возникнут при отправке IP-пакета в сеть назначения через тот или иной шлюз. Стоимость маршрута обратно пропорциональна его пропускной способности канала связи.

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора пути для передачи данных в сети.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, используемые в одной сети, в адреса и порты, используемые в другой.

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки транспортного конверта 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.