



ViPNet Coordinator KB 4

Справочник команд и конфигурационных
файлов

1991–2019 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.465614.001РЭЗ

Версия продукта 4.2.0

Этот документ входит в комплект поставки ViPNet Coordinator KB, 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 ОАО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

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

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, дом 1/23, строение 1

Тел: (495) 737-61-96 (горячая линия), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: <https://infotecs.ru>

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение.....	10
О документе.....	11
Для кого предназначен документ	12
Соглашения документа	13
Обратная связь.....	15
О программно-аппаратном комплексе ViPNet Coordinator KB	16
Основные сведения по работе с командным интерпретатором.....	17
Глава 1. Справочник команд	18
Команды группы admin.....	19
admin config delete.....	19
admin config list.....	20
admin config load	21
admin config save	22
admin export keys binary-encrypted usb	22
admin export logs	24
admin export dnsd log	25
admin export packetdb usb	26
admin export-and-clear logs usb.....	26
admin remove keys.....	27
admin show dnsd log.....	28
admin show dsdrnet.....	29
admin show logs.....	30
admin update-dsdr	31
admin upgrade software usb.....	32
Команды группы alg	34
alg module process off.....	34
alg module process on	34
alg show	35
alg start.....	37
alg stop	37
Команды группы failover.....	39
failover config edit	39
failover config mode	40
failover show config.....	41

failover show info	41
failover start	43
failover stop	44
failover view	44
Команды группы firewall	46
firewall add	46
firewall add name	49
firewall change append	50
firewall delete	52
firewall move rule	53
firewall object delete	54
firewall object show	55
firewall rules show	56
firewall show	57
Команды группы inet	60
inet clear mac-address-table	60
inet dhcp client route-default-metric	60
inet dhcp client route-distance	61
inet dhcp relay add listen-interface	62
inet dhcp relay delete listen-interface	63
inet dhcp relay external-interface	64
inet dhcp relay mode	64
inet dhcp relay reset	65
inet dhcp relay start	66
inet dhcp relay stop	67
inet dhcp server add wins	67
inet dhcp server delete wins	68
inet dhcp server interface	69
inet dhcp server lease	70
inet dhcp server mode	70
inet dhcp server range	71
inet dhcp server router	72
inet dhcp server start	73
inet dhcp server stop	74
inet dns clients add	74
inet dns clients delete	75
inet dns clients list	76
inet dns forwarders add	77
inet dns forwarders delete	77

inet dns forwarders list.....	78
inet dns mode.....	79
inet dns start.....	80
inet dns stop.....	80
inet ifconfig address.....	81
inet ifconfig address add.....	82
inet ifconfig address delete.....	83
inet ifconfig class.....	84
inet ifconfig dhcp.....	85
inet ifconfig dhcp route-metric.....	86
inet ifconfig down.....	87
inet ifconfig reset.....	88
inet ifconfig speed.....	89
inet ifconfig speed auto.....	90
inet ifconfig up.....	91
inet ifconfig vlan add.....	92
inet ifconfig vlan delete.....	93
inet ntp add.....	93
inet ntp delete.....	94
inet ntp list.....	95
inet ntp mode.....	96
inet ntp orphan.....	96
inet ntp start.....	97
inet ntp stop.....	98
inet ospf mode.....	98
inet ospf network add.....	99
inet ospf network delete.....	100
inet ospf redistribute add.....	101
inet ospf redistribute delete.....	102
inet ping.....	103
inet route add.....	104
inet route clear.....	105
inet route delete.....	106
inet show dhcp client.....	107
inet show dhcp relay.....	108
inet show dhcp server.....	109
inet show dns.....	110
inet show interface.....	111
inet show mac-address-table.....	112

inet show ntp.....	113
inet show ospf configuration.....	115
inet show ospf database.....	116
inet show ospf neighbour.....	117
inet show routing.....	118
inet show snmp.....	119
inet show snmp community.....	120
inet show vlan.....	121
inet snmp community ro.....	122
inet snmp community trap.....	123
inet snmp debug-level.....	123
inet snmp mode.....	124
inet snmp start.....	125
inet snmp stop.....	126
inet snmp trapsink.....	127
inet vlan comment add.....	127
inet vlan comment delete.....	128
Команды группы iplir.....	130
iplir config.....	130
iplir info.....	131
iplir option get.....	132
iplir option set antispoofing.....	133
iplir option set block-other-protocols.....	134
iplir option set cleanup-interval.....	135
iplir option set connection-ttl-ip.....	135
iplir option set connection-ttl-tcp.....	136
iplir option set connection-ttl-udp.....	137
iplir option set dynamic-ports.....	137
iplir option set dynamic-timeouts.....	138
iplir option set max-connections.....	139
iplir ping.....	140
iplir set l2overip interface.....	141
iplir set l2overip local-port.....	142
iplir set l2overip mac-ttl.....	142
iplir set l2overip mode.....	143
iplir set l2overip remote-port.....	144
iplir set l2overip remote-port delete.....	145
iplir set l2overip unsolicited-frames.....	145
iplir set thread-count.....	146

iplir show adapters.....	147
iplir show config.....	148
iplir show firewall status.....	149
iplir show key-info.....	150
iplir show keys-upgrade-log	152
iplir show l2overip	153
iplir show thread-count.....	154
iplir start	154
iplir stop.....	155
iplir view	156
Команды группы machine	158
machine halt	158
machine reboot	158
machine self-test.....	159
machine set date.....	161
machine set hostname	161
machine set loghost	162
machine set timezone.....	163
machine show date	164
machine show dnssd log	165
machine show dnssd log usb.....	165
machine show hostname.....	166
machine show loghost.....	167
machine show logs.....	168
machine show memory	169
machine show session-timeout	170
machine show timezone	170
machine show uptime.....	171
Команды группы mftp.....	173
mftp config.....	173
mftp info.....	174
mftp show config.....	175
mftp start	176
mftp stop.....	177
mftp view	178
Команды группы ups	180
ups set driver	180
ups set mode.....	180
ups set monitoring	181

ups show config	182
ups show status	183
ups start	184
ups stop	185
Команды группы vpn	186
vpn start	186
vpn stop	187
Прочие команды	188
debug off	188
debug on	188
enable	189
exit	190
version features list	191
version	192
who	192
Глава 2. Справочник по конфигурационным файлам	194
Файл failover.ini	195
Секция [channel]	195
Секция [debug]	197
Секция [misc]	197
Секция [network]	198
Секция [sendconfig]	199
Файл iplir.conf	202
Секция [id]	202
Секция [adapter]	207
Секция [dynamic]	208
Секция [misc]	209
Секция [debug]	211
Секция [servers]	212
Секция [virtualip]	212
Секция [visibility]	213
Секция [packet-settings]	213
Секция [protection]	214
Файл iplir.conf- <интерфейс>	215
Файл mftp.conf	217
Секция [channel]	217
Специфические параметры для канала MFTP	218
Специфические параметры для канала SMTP	218

Секция [transport]	219
Секция [mailtrans]	220
Секция [journal]	220
Секция [misc]	221
Секция [debug]	223
Секция [reserv]	224
Секция [upgrade]	224
Приложение А. Глоссарий	226



Введение

О документе	11
Для кого предназначен документ	12
Соглашения документа	13
Обратная связь	15
О программно-аппаратном комплексе ViPNet Coordinator KB	16
Основные сведения по работе с командным интерпретатором	17

О документе

Документ содержит описание команд, доступных для выполнения в [командном интерпретаторе программно-аппаратного комплекса ViPNet Coordinator KB](#) (см. глоссарий, стр. 231). 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 управляющего демона (см. [Файл iplir.conf](#) на стр. 202).
- `iplir.conf-<интерфейс или группа интерфейсов>` — конфигурационные файлы сетевых интерфейсов ViPNet Coordinator KB.
- `failover.ini` — конфигурационный файл системы защиты от сбоев (см. [Файл failover.ini](#) на стр. 195).
- `mftp.conf` — конфигурационный файл транспортного модуля MFTP (см. [Файл mftp.conf](#) на стр. 217).

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 управления командного интерпретатора, который позволяет изменять настройки ViPNet Coordinator KB.
- Режим наблюдения командного интерпретатора, 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 наблюдения (доступен ограниченный набор команд управления, обозначается символом «>» в приглашении интерпретатора). Для управления ViPNet Coordinator KB требуется перейти из режима наблюдения в режим управления.

Для кого предназначен документ

Документ предназначен для пользователей, отвечающих за настройку и эксплуатацию ViPNet Coordinator KB. Далее именуется администратором ViPNet Coordinator KB.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
Код	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены в режиме управления командного интерпретатора, содержат приглашение с символом «#». Например:

```
hostname# команда
```

- Команды, которые могут быть выполнены в режиме наблюдения командного интерпретатора, 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

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТекС»:

- Информация о продуктах ViPNet <https://infotecs.ru/product/>.
- Информация о решениях ViPNet <https://infotecs.ru/resheniya/>.
- Часто задаваемые вопросы <https://infotecs.ru/support/faq/>.
- Форум пользователей продуктов ViPNet <https://infotecs.ru/forum/>.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТекС»:

- Единый многоканальный телефон:
+7 (495) 737-6192,
8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба технической поддержки: hotline@infotecs.ru.
Форма для обращения в службу технической поддержки через сайт <https://infotecs.ru/support/request/>.
Консультации по телефону для клиентов с расширенной схемой технической поддержки:
+7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТекС» регулируется политикой ответственного разглашения <https://infotecs.ru/disclosure.php>.

О программно-аппаратном комплексе ViPNet Coordinator KB

Программно-аппаратный комплекс ViPNet Coordinator KB представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet, которое функционирует под управлением адаптированной ОС GNU/Linux. Описание выполняемых функций ViPNet Coordinator KB и аппаратных платформ см. в документе «ViPNet Coordinator KB. Общее описание».

Основные сведения по работе с командным интерпретатором

Все операции по настройке ViPNet Coordinator KB вы можете выполнить с помощью командного интерпретатора. Работа в командном интерпретаторе возможна при локальном подключении к ViPNet Coordinator KB.

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

Чтобы вернуться в режим наблюдения, выполните команду `exit`.

Чтобы выйти из командного интерпретатора, выполните команду `exit`. В случае выхода из командного интерпретатора на консоли снова появится приглашение для аутентификации пользователя.

1

Справочник команд

Команды группы admin	19
Команды группы alg	34
Команды группы failover	39
Команды группы firewall	46
Команды группы inet	60
Команды группы iplir	130
Команды группы machine	158
Команды группы mftp	173
Команды группы ups	180
Команды группы vrn	186
Прочие команды	188

Команды группы admin

Команды группы `admin` предназначены для выполнения задач по настройке ViPNet Coordinator KB.

admin config delete

Команда используется для удаления копии конфигурации VPN с заданным именем.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При вводе имени работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка сохраненных копий конфигурации VPN.
- В имени можно указать символ «*» для обозначения любого количества символов. Это позволяет производить удаление 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

Для удаления всех сохраненных копий конфигурации VPN, у которых имя начинается с `Config_`, выполните команду:

```
hostname# admin config delete Config_*
```

admin config list

Команда предназначена для просмотра текущего списка сохраненных копий конфигурации VPN.

Синтаксис

```
admin config list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# admin config list
"Config_1", version 4.1.0, full, saved on 31.07.2014 at 20:06, never loaded
hostname#
```

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 конфигурации VPN 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`.

admin config load

Команда используется для загрузки (восстановления) настроек ViPNet Coordinator KB из копии конфигурации VPN с заданным именем.

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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При вводе имени работают автозаполнение 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 требуется ввести имя, под которым будет сохранена копия текущей конфигурации.
- Если текущая версия ПО ViPNet Coordinator KB ниже версии, указанной в команде, то требуется дополнительно подтвердить загрузку настроек из копии конфигурации VPN.

Пример использования

Для загрузки настроек из копии конфигурации VPN с именем `Rollback_config`, относящейся к версии 3.2.0, выполните команду:

```
hostname# admin config load Rollback_config 3.2.0
```

admin config save

Команда используется для сохранения копии текущей конфигурации VPN с заданным именем.

Синтаксис

```
admin config save <имя>
```

Параметры и ключевые слова

<имя> — имя копии конфигурации VPN.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Перед выполнением команды необходимо остановить [демоны failoverd, iplir, mftpd](#) (см. [vpn stop](#) на стр. 187).
- В имени можно использовать только символы латинского алфавита, цифры, знаки «дефис» и «подчеркивание».
- Если в списке сохраненных копий конфигурации VPN есть копия конфигурации VPN с указанным именем, то запрашивается подтверждение на перезапись этой копии конфигурации VPN.

Пример использования

Для сохранения копии текущей конфигурации VPN под именем `Rollback_config` выполните команду:

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

```
There are running daemons: failover iplir mftpd. Stop them and try again.
```

admin export keys binary-encrypted usb

Команда используется для экспорта [справочников, ключей](#) (см. глоссарий, стр. 233) и настроек ViPNet Coordinator KB на USB-носитель. При этом ключевая информация с установленного ключевого блокнота ДСДР не экспортируется на USB-носитель.

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Имя файла экспорта формируется по следующему шаблону:
`<название ViPNet Coordinator KB>-<идентификатор узла>-<дата 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 демонов `iplircfg` (см. [iplir stop](#) на стр. 155) и `mftpd` (см. [mftp stop](#) на стр. 177).
- Необходимо дождаться сообщения с разрешением извлечь устройство прежде, чем извлечь USB-носитель из разъема.

Пример использования

Ниже приведен пример выполнения команды:

```
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.vbe
Put kb-15ea000b-2017-05-09.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.vbe to be copied onto the USB drive.
```

```
File kb-15ea000b-2017-05-09.vbe was successfully copied onto the USB drive.  
You may remove the USB drive.  
hostname#
```

admin export logs

Команда используется для экспорта файлов журналов, хранящихся на жестком диске ViPNet Coordinator KB, на USB-носитель.

Синтаксис

```
admin export logs usb
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Имя файла экспорта — `logs.tar.gz`.
- Для того, чтобы на USB-носитель можно было выгрузить журнал событий СКЗИ предварительно его необходимо сохранить на жестком диске ViPNet Coordinator KB (см. [admin export dnsd log](#) на стр. 25).
- По запросу командного интерпретатора задайте пароль, на котором будет рассчитана имитовставка.

Пример использования

Ниже приведен пример выполнения команды:

```
hostname# admin export logs usb  
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 dnssd log

Команда используется для сохранения журнала событий СКЗИ на жесткий диск ViPNet Coordinator KB для возможности последующего просмотра и выгрузки на USB-носитель.

Синтаксис

```
admin export dnssd log
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы экспортировать журнала событий датчика несанкционированного доступа, выполните команду:

```
hostname# admin export dnssd log
```

admin export packetdb usb

Команда используется для экспорта журнала регистрации IP-пакетов на USB-носитель.

Синтаксис

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

Параметры и ключевые слова

<имя> — имя файла экспорта.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

При вводе имени файла работает автозаполнение и подсказка, данные для подсказки берутся из списка существующих файлов экспорта.

Пример использования

Чтобы экспортировать журнал регистрации IP-пакетов в файл с именем `ippacket`, выполните команду:

```
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.
hostname#
```

admin export-and-clear logs usb

Команда используется для экспорта файлов журнала устранения неполадок, хранящихся на ViPNet Coordinator KB, на USB-носитель с последующим удалением их с ViPNet Coordinator KB.

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

```
You are about to export and remove logs from ViPNet Coordinator KB. Do you want to continue? [y/n] y
```

```
Logs archivation is in progress. Press ^+C to abort.
```

```
Please insert the USB flash drive and press y to continue. [y/n] y
```

```
Copying logs archive file to /dev/sda1. Press ^+C to abort.
```

```
Logs archive file integrity check successful.
```

```
Logs exported and removed from ViPNet Coordinator KB successfully.
```

```
hostname#
```

admin remove keys

Команда используется для удаления справочников, ключей и ключевого блокнота ДСДР ViPNet Coordinator KB.

Синтаксис

```
admin remove keys
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Если на ViPNet Coordinator KB запущены серверы DNS, NTP и DHCP, то их работа будет автоматически завершена.
- Будет завершены все запущенные сервисы ViPNet и выгружены все драйверы ViPNet.
- Все сетевые интерфейсы ViPNet Coordinator KB будут автоматически отключены.

Пример использования

```
hostname# admin remove keys
This command removes all ViPNet keys and cannot be reverted,
it will be necessary to deploy new keys after executing this command.
Do you really wish to execute this command?[Yes,No]
Yes
DHCP server is already off. Command ignored.
DNS server is already off. Command ignored.
NTP server is already off. Command ignored.
Stopping all VPN services
...
server login:
```

admin show dnsd log

Команда используется для отображения журнала СКЗИ.

Синтаксис

```
admin show dnsd log
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# admin show dnsd log
02-12-2017 10:28:37: Diagnose check on the periodical key, status: ok...
02-12-2017 10:27:44: Key event [checksums with PKKC checking]
02-12-2017 10:27:37: Diagnose check on the periodical key, status: ok...
02-12-2017 10:10:37: Key event [PKKC generation]
02-12-2017 10:10:31: Key event [random numbers generation]
02-12-2017 10:08:04: Key event [predefined generation]
02-12-2017 10:08:03: Diagnose check on the technological key, status: ok...
02-12-2017 10:06:04: Key event [checksums with TKKC generation]
02-12-2017 10:05:57: Diagnose check on the technological key, status: ok...
02-12-2017 10:05:50: Key event [TKKC generation]
02-12-2017 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

Команда используется для отображения сведений о номере и серии [ключевых блокнотов ДСДР](#) (см. глоссарий, стр. 230), 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 управления.

Особенности использования

Сведения отображаются следующем формате:

```
AAAAVVVVVV  CCCCCC
```

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

Для возвращения к командной строке введите с клавиатуры символ `q`.

Пример использования

```
hostname# admin show dsdrnet
```

```
0001888888  2890000C
```

```
0004888888  2890000D
```

```
0002888888  28900024
```

admin show logs

Команда используется для отображения событий безопасности системного журнала безопасности за определенную дату.

Синтаксис

```
admin show logs <dd.mm.yyyy>
```

Параметры и ключевые слова

<dd.mm.yyyy> — дата.

Значения по умолчанию

<dd.mm.yyyy> — текущая дата.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы просмотреть события системного журнала безопасности за 20 декабря 2018 года, выполните команду:

```
hostname# admin show logs 20.12.2018
```

admin update-dsdr

Команда используется для установки и обновления ключевого блокнота ДСДР.

Синтаксис

```
admin update-dsdr
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Перед первичной установкой ключевого блокнота ДСДР на ViPNet Coordinator KB должен быть установлен [дистрибутив ключей](#) (см. глоссарий, стр. 229). 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](#) (см. глоссарий, стр. 228) 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

Команда используется для обновления ПО VipNet Coordinator KB с USB-носителя.

Синтаксис

```
admin upgrade software usb
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Перед выполнением команды рекомендуется проверить подлинность и целостность файла обновления. Для этого вычислите контрольную сумму файла по алгоритму MD5, а затем сравните ее с контрольной суммой, приведенной в файле с расширением *.md5, который поставляется с файлом обновления.

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

Команды группы `alg` предназначены для управления обработкой прикладных протоколов.

`alg module process off`

Команда используется для выключения обработки 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`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Для выключения обработки прикладного протокола `DNS` выполните команду:

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

`alg module process on`

Команда используется для включения обработки прикладного протокола `DNS`, `FTP`, `H.323`, `SCCP` или `SIP` либо изменения параметров 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, sccp или dns.
- <порты> — номера портов для обработки.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- В качестве портов можно указать один порт, диапазон портов либо список портов и диапазонов портов, перечисленных через запятую.
- Нулевое значение порта означает выключение обработки прикладного протокола указанным сетевым протоколом.

Пример использования

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

```
hostname# alg module ftp process tcp 20-21,26 on
Waiting for alg daemon..
hostname#
```

alg show

Команда предназначена для просмотра текущих параметров обработки прикладных протоколов.

Синтаксис

```
alg show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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           |ON    |
+=====+=====+=====+=====+
|SIP           |UDP     |5060           |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).

alg start

Команда используется для запуска работы демона `algd`, отвечающего за обработку прикладных протоколов.



Примечание. Для обеспечения бесперебойной работы прикладных сервисов в процессе штатного функционирования ПО ViPNet Coordinator KB не рекомендуется завершать работу демона `algd`.

Синтаксис

```
alg start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> alg start
```

```
hostname>
```

alg stop

Команда используется для завершения работы демона `algd`, отвечающего за обработку прикладных протоколов.



Примечание. Для обеспечения бесперебойной работы прикладных сервисов в процессе штатного функционирования ПО ViPNet Coordinator KB не рекомендуется завершать работу демона `algd`.

Синтаксис

```
alg stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

При завершении работы демона `algd` с помощью данной команды продолжается обработка протокола `DNS`. Выключить обработку протокола `DNS` можно только с помощью команды `alg module process off` (на стр. 34).

Пример использования

```
hostname> alg stop
Shutting down Alg daemon
hostname>
```

Команды группы failover

Команды группы `failover` предназначены для настройки и управления системой защиты от сбоев ViPNet Coordinator KB.

`failover config edit`

Команда используется для редактирования файла конфигурации системы защиты от сбоев.

Синтаксис

```
failover config edit
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

По команде будет запущен текстовый редактор с файлом конфигурации `failover.ini`.

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
...
hostname#
```

failover config mode

Команда используется для установки режима работы системы защиты от сбоев.

Синтаксис

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

Параметры и ключевые слова

- `single` — одиночный режим.
- `cluster` — режим [кластера](#) (см. глоссарий, стр. 230).

Значения по умолчанию

По умолчанию установлен одиночный режим (`single`).

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Команда доступна только в исполнениях ViPNet Coordinator KB, поддерживающих работу в кластере горячего резервирования.
- При установке режима кластера автоматически будет завершена работа драйверов и демонов, которые не поддерживаются в этом режиме.
- При установке одиночного режима автоматически будет завершена работа всех демонов.

Пример использования

Для установки режима кластера выполните команду:

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

failover show config

Команда предназначена для просмотра файла конфигурации системы защиты от сбоев.

Синтаксис

```
failover show config
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

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

Пример использования

```
hostname> failover show config
[network]
checktime = 10
timeout = 2
activeretries = 3
channelretries = 3
synctime = 5
fastdown = yes
...
hostname>
```

failover show info

Команда предназначена для просмотра информации о текущем состоянии системы защиты от сбоев.

Синтаксис

```
failover show info
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> failover show info
Running failover info
Versions: ViPNet 4.1.0(150), daemon 1.5 (1)
Workstation configured for ID 15EA000B (Coordinator 2)
The workstation works in a single mode of protection against failures
Workstation time (utc: 1406806848) Thu Jul 31 15:40:48 2014
failover mode * single
failover uptime * 0d 0:14
total cpu * 3%
total memory * 2055488 kB
free memory * 1915324 kB
failover state * works
failover cpu * 1%
iplir state * works
iplir cpu * 4%
mftp state * works
mftp cpu * 1%
alg state * works
alg cpu * 0%
webgui state * works
webgui cpu * 0%
hostname>
```

По команде отображается следующая информация:

- версия ПО ViPNet Coordinator KB и версия демона `failoverd`;
- информация о сетевом узле;
- локальное время на узле;
- режим работы системы защиты от сбоев (одиночный или режим кластера);

- информация об использовании процессора и оперативной памяти;
- информация о текущем состоянии управляющего демона, демонов `mftpd`, `failoverd`, `algd` и веб-интерфейса.

failover start

Команда используется для запуска демона `failoverd`, отвечающего за функционирование системы защиты от сбоев.

Синтаксис

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

Параметры и ключевые слова

- `active` — запуск демона `failoverd` в активном режиме.
- `passive` — запуск демона `failoverd` в пассивном режиме.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

- Параметр можно указать только при работе системы защиты от сбоев в режиме кластера.
- Если в режиме кластера параметр не указан, демон `failoverd` будет запущен в том режиме, в котором он находился до завершения работы.
- Перед запуском демона `failoverd` в активном режиме необходимо убедиться, что на другом ViPNet Coordinator KB кластера демон `failoverd` запущен в пассивном режиме. Запуск демона `failoverd` в активном режиме на обоих элементах кластера приведет к конфликту IP-адресов и другим нежелательным последствиям.

Пример использования

Чтобы запустить демон `failoverd` в пассивном режиме, выполните команду:

```
hostname> failover start passive
```

failover stop

Команда используется для завершения работы демона `failoverd`, отвечающего за функционирование системы защиты от сбоев.

Синтаксис

```
failover stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

failover view

Команда предназначена для просмотра журнала 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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

- Команда доступна только в исполнениях ViPNet Coordinator KB, поддерживающих работу в кластере горячего резервирования.
- Для завершения просмотра журнала используется клавиша **Q**.

Пример использования

```
hostname> failover view 20.10.2014.08.00.00 21.10.2014.19.00.00
View journal of failover switching
Versions: ViPNet 4.1.0 (475), daemon 1.3 (14)
Workstation configured for ID 1031F (Cluster for SGA2)
Workstation works in a mode of hot reservation
Workstation time (utc: 1174916969) Mon Mar 29 17:49:29 2010

09 Mar 2014 12:51:42    <P_START> Start failover daemon in passive mode
22 Mar 2014 12:27:27    <A_START> Start failover daemon in active mode
22 Mar 2014 14:10:35    <A_START> Start failover daemon in active mode
22 Mar 2014 15:30:46    <BOOT> Boot the system
23 Mar 2014 11:09:07    <SWITCH> Switch server from passive mode to active mode

hostname>
```

Команды группы firewall

Команды группы `firewall` предназначены для работы с [сетевыми фильтрами](#) (см. глоссарий, стр. 233), [правилами трансляции адресов](#) (см. глоссарий, стр. 234) и группами объектов.

firewall add

Команда используется для создания сетевого фильтра или правила 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](#) (см. глоссарий, стр. 234);
 - `vpn` — фильтр защищенной сети;
 - `nat` — правило трансляции адресов.
- `<номер>` — порядковый номер фильтра (правила трансляции) в таблице, определяющий его приоритет.
- `<имя>` — имя фильтра (правила трансляции).
- `<адрес отправителя>` — адрес отправителя IP-пакетов.
- `<адрес получателя>` — адрес 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).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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** (см. глоссарий, стр. 226) 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 следующее:
 - для локальных фильтров открытой сети — системную группу `broadcast` или `multicast`;
 - для фильтров защищенной сети — системную группу `broadcast`.
- Протокол можно указать, используя следующее:
 - имена протоколов, написанные строчными буквами и разделенные пробелами. При этом можно также задать дополнительные параметры для протоколов:

- TCP и UDP: `sport` (порт или диапазон портов источника пакета) и/или `dport` (порт или диапазон портов назначения пакета). При использовании обоих этих параметров сначала необходимо указать параметр `sport`, затем — параметр `dport`,
- ICMP: только параметр `type` (тип пакета) либо параметр `type` вместе с параметром `code` (код пакета). Если параметр `code` не задан, то под условие будут подпадать все ICMP-пакеты указанного типа;
- номера протоколов. При этом перед номером каждого протокола необходимо указать ключевое слово `proto`;
- пользовательские группы протоколов в виде: `service @<имя группы>`.
- 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) и интервал времени.
 - `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 команду:

```
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](#) (см. глоссарий, стр. 230) с идентификатором 0x1234abab туннелируемому узлу с адресом 192.168.0.1 ежедневно в интервал с 8 утра до 8 вечера, выполните команду:

```
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 с помощью команды:

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

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

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



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

firewall add name

Команда используется для создания группы 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](#) (см. глоссарий, стр. 233);
 - service-object — протоколы;

- o `schedule-object` — расписания.
- `<имя>` — имя группы объектов.
- `<состав>` — объекты, входящие в группу.
- `<исключения>` — объекты, не входящие в группу.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Имя группы должно быть уникальным в рамках групп объектов одного типа.
- Перед именем группы необходимо указывать символ `@`.
- Сетевые интерфейсы разделяются пробелом, и перед именем каждого сетевого интерфейса необходимо указать слово `interface`;
- Синтаксис протокола и расписания — тот же, что при создании сетевого фильтра или правила трансляции адресов с помощью команды `firewall add` (на стр. 46).

Примеры использования

Чтобы создать группу IP-адресов, включающую сегмент сети за исключением нескольких IP-адресов, выполните команду:

```
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, включающую выходные дни с 9 до 23 часов, выполните команду:

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

Чтобы создать группу интерфейсов, включающую сетевые интерфейсы `eth0` и `eth1`, выполните команду:

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

firewall change append

Команда используется для добавления адреса отправителя, адреса получателя, протокола или расписания 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](#) (см. глоссарий, стр. 234);
 - 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).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Синтаксис адреса отправителя, адреса получателя, протокола и расписания — тот же, что при создании сетевого фильтра (правила трансляции) с помощью команды `firewall add` (на стр. 46).
- Можно указать несколько параметров.

Пример использования

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

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

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

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

firewall delete

Команда используется для удаления сетевого фильтра или правила 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](#) (см. глоссарий, стр. 234);
 - `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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Синтаксис адреса отправителя, адреса получателя, протокола и расписания — тот же, что при создании фильтра (правила трансляции) с помощью команды `firewall add` (на стр. 46).
- Можно указать несколько параметров.
- Поиск фильтров (правил трансляции) для удаления осуществляется по строгому совпадению с заданными параметрами.
- Нумерация фильтров (правил трансляции), следующих за удаленным фильтром (правилом трансляции), изменяется автоматически (их номера уменьшаются на 1).

Пример использования

Для удаления локального фильтра открытой сети с номером 7 выполните команду:

```

hostname# firewall local delete 7
=====+=====+=====+=====+
|Num |Name                               |Option   |Schedule |
+---+-----+-----+-----+
|Act |Source   |Destination |Protocol          |
+---+-----+-----+-----+
|7   |Allow syslog outgoing |User     |              |
+---+-----+-----+-----+
|pass|@local   |@any     |udp: to 514      |
+---+-----+-----+-----+
Do you want to perform the action on the above rule? [y/n]: y
hostname#

```

firewall move rule

Команда используется для изменения порядкового номера (приоритета) 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](#) (см. глоссарий, стр. 234);
 - vpn — фильтр защищенной сети;
 - nat — правило трансляции адресов.
- <текущий номер> — текущий порядковый номер фильтра (правила трансляции).
- <новый номер> — новый порядковый номер фильтра (правила трансляции).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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), выполните команду:

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

```
hostname#
```

firewall object delete

Команда используется для удаления группы объектов с заданным именем.

Синтаксис

```
firewall object delete @<имя>
```

Параметры и ключевые слова

<имя> — имя группы объектов.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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 необходимо сначала удалить эти фильтры, правила и группы, а затем выполнить команду для удаления группы еще раз.

Пример использования

Чтобы удалить группу объектов с именем `IP_group`, выполните команду:

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

firewall object show

Команда предназначена для просмотра всех групп объектов.

Синтаксис

```
firewall object show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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 программы ViPNet Policy Manager — Policy, для пользовательских групп — User.
- Inclusion — объекты, входящие в группу.
- Exclusion — объекты, не входящие в группу.

firewall rules show

Команда предназначена для просмотра всех сетевых фильтров и правил трансляции адресов, заданных на узле.

Синтаксис

```
firewall rules show
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> firewall rules show
```

```
Local Rules:
```

```
=====+=====+=====+
|Num |Name                |Option    |Schedule  |
+----+-----+-----+-----+
|Act |Source  |Destination |Protocol  |
```

```

+====+=====+=====+=====+=====+
|1   |Allow DHCP Service   |User   |   |   |
+----+-----+-----+-----+-----+
|pass|@any   |@any   |udp: from 67 to 68 |   |
+====+=====+=====+=====+=====+
|... |   |   |   |   |
+====+=====+=====+=====+=====+
empty rule for Forward Rules:
empty rule for Nat Rules:

hostname>

```

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

Команда предназначена для просмотра 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;

- o `forward` — транзитный фильтр открытой сети;
 - o `tunnel` — фильтр [туннелируемых узлов](#) (см. глоссарий, стр. 234);
 - o `vpn` — фильтр защищенной сети;
 - o `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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

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](#) на стр. 46).
- 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](#) на стр. 55), сетевых фильтров или правил трансляции адресов (см. [firewall rules show](#) на стр. 56).

Пример использования

Для просмотра локальных фильтров для протокола UDP выполните команду:

```
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

Команды группы `inet` предназначены для настройки и управления сервисами, использующими сетевые интерфейсы, предназначенные для подключения к VipNet Coordinator KB средств удаленного управления.

`inet clear mac-address-table`

Команда используется для очистки ARP-таблицы (таблицы преобразования IP-адресов в MAC-адреса).

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# inet clear mac-address-table
This command clears MAC address table.
Do you really wish to execute this command? [Yes,No]: Yes
hostname#
```

`inet dhcp client route-default-metric`

Команда используется для изменения значения [метрики по умолчанию](#) (см. глоссарий, стр. 232) 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 управления.

Особенности использования

Нет.

Пример использования

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

inet dhcp client route-distance

Команда используется для задания [административной дистанции](#) (см. глоссарий, стр. 228) маршрутам, поступающим от DHCP-сервера (с использованием DHCP-протокола).

Синтаксис

```
inet dhcp client route-distance <1-255> [default-route <1-255>]
```

Параметры и ключевые слова

<1-255> — значение общей административной дистанции для всех маршрутов DHCP-сервера.

default-route <1-255> — значение административной дистанции для [маршрутов по умолчанию](#) (см. глоссарий, стр. 231).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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
hostname#
```

inet dhcp relay add listen-interface

Команда используется для добавления интерфейса в список интерфейсов, принимающих запросы от DHCP-клиентов для их последующей ретрансляции на внешний DHCP-сервер.

Синтаксис

```
inet dhcp relay add listen-interface <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Перед выполнением команды необходимо завершить работу службы DHCP-relay (см. [inet dhcp relay stop](#) на стр. 67).

- 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.

Пример использования

Чтобы добавить интерфейс `eth0` в список интерфейсов, принимающих запросы от DHCP-клиентов, выполните команду:

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

inet dhcp relay delete listen-interface

Команда используется для удаления интерфейса из списка интерфейсов, принимающих запросы от DHCP-клиентов.

Синтаксис

```
inet dhcp relay delete listen-interface <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Перед выполнением команды необходимо завершить работу службы DHCP-relay (см. [inet dhcp relay stop](#) на стр. 67).
- При вводе интерфейса работают автозаполнение и подсказка. Данные для подсказки берутся из текущего списка интерфейсов, принимающих DHCP-запросы.

Пример использования

Чтобы удалить интерфейс `eth0` из списка интерфейсов, принимающих запросы от DHCP-клиентов, выполните команду:

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

inet dhcp relay external-interface

Команда используется для установки параметров связи службы DHCP-relay с внешним DHCP-сервером.

Синтаксис

```
inet dhcp relay external-interface <интерфейс> server {<адрес> | <DNS-имя>}
```

Параметры и ключевые слова

- <интерфейс> — имя интерфейса, со стороны которого находится внешний DHCP-сервер.
- <адрес> — IP-адрес внешнего DHCP-сервера.
- <DNS-имя> — DNS-имя внешнего DHCP-сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Перед выполнением команды необходимо завершить работу службы DHCP-relay (см. [inet dhcp relay stop](#) на стр. 67).
- 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 использовать интерфейс `eth1` для связи с внешним DHCP-сервером, имеющим адрес `172.16.1.1`, выполните команду:

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

inet dhcp relay mode

Команда используется для включения или выключения автоматического запуска службы DHCP-relay при загрузке ViPNet Coordinator KB.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

По умолчанию автоматический запуск службы DHCP-relay выключен (`off`).

Режимы командного интерпретатора

Режим управления.

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, выполните команду:

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

inet dhcp relay reset

Команда завершает работу службы DHCP-relay, сбрасывает все ее настройки и выключает автоматический запуск службы при загрузке ViPNet Coordinator KB.

Синтаксис

```
inet dhcp relay reset
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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
```

```
The factory default settings of DHCP-relay will be restored. Continue? [Yes,No]: Yes
```

```
DHCP relay settings successfully restored to factory defaults.
```

```
hostname#
```

inet dhcp relay start

Команда используется для запуска службы DHCP-relay.

Синтаксис

```
inet dhcp relay start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Невозможно запустить службу DHCP-relay в следующих случаях:

- Запущен DHCP-сервер.

- Не заданы какие-либо настройки службы DHCP-relay.

Пример использования

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

inet dhcp relay stop

Команда используется для завершения работы службы DHCP-relay.

Синтаксис

```
inet dhcp relay stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

inet dhcp server add wins

Команда используется для добавления адреса [WINS-сервера](#) (см. глоссарий, стр. 228) в список адресов, передаваемых DHCP-сервером своим клиентам.

Синтаксис

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

Параметры и ключевые слова

<IP-адрес> — IP-адрес WINS-сервера.

Значения по умолчанию

По умолчанию список адресов WINS-серверов содержит адрес 172.16.1.1.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Перед выполнением команды необходимо завершить работу DHCP-сервера (см. [inet dhcp server stop](#) на стр. 74).

Пример использования

Чтобы в список передаваемых адресов WINS-серверов добавить адрес 192.168.10.1, выполните команду:

```
hostname# inet dhcp server add wins 192.168.10.1
```

inet dhcp server delete wins

Команда используется для удаления адреса WINS-сервера из списка адресов, передаваемых DHCP-сервером своим клиентам.

Синтаксис

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

Параметры и ключевые слова

<IP-адрес> — IP-адрес WINS-сервера.

Значения по умолчанию

По умолчанию список адресов WINS-серверов содержит адрес 172.16.1.1.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Перед выполнением команды необходимо завершить работу DHCP-сервера (см. [inet dhcp server stop](#) на стр. 74).

Пример использования

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

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

inet dhcp server interface

Команда используется для задания рабочего интерфейса [DHCP-сервера](#) (см. глоссарий, стр. 226).

Синтаксис

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

Параметры и ключевые слова

<интерфейс> — имя интерфейса.

Значения по умолчанию

По умолчанию в качестве рабочего интерфейса используется `eth0`.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Перед выполнением команды необходимо завершить работу DHCP-сервера (см. [inet dhcp server stop](#) на стр. 74).
- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка интерфейсов в системе.
- В качестве рабочего можно указать Ethernet- или VLAN-интерфейс.
- Рабочий интерфейс DHCP-сервера должен иметь статический адрес.
- Адрес рабочего интерфейса DHCP-сервера не должен принадлежать диапазону выделяемых адресов, заданному командой `inet dhcp range` (см. [inet dhcp server range](#) на стр. 71).

Пример использования

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

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

inet dhcp server lease

Команда используется для задания времени аренды (лизинга) IP-адресов, выделяемых DHCP-сервером своим клиентам.

Синтаксис

```
inet dhcp server lease <время>
```

Параметры и ключевые слова

<время> — время аренды в секундах.

Значения по умолчанию

По умолчанию время аренды 864000 секунд.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Перед выполнением команды необходимо завершить работу DHCP-сервера (см. [inet dhcp server stop](#) на стр. 74).

Пример использования

Чтобы установить время аренды 5 дней, выполните команду:

```
hostname# inet dhcp server lease 432000
```

inet dhcp server mode

Команда используется для включения или выключения автоматического запуска DHCP-сервера при загрузке ViPNet Coordinator KB.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

По умолчанию автоматический запуск DHCP-сервера выключен (`off`).

Режимы командного интерпретатора

Режим управления.

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, выполните команду:

```
hostname# inet dhcp server mode on
DHCP server enabled and will be started on next reboot.
You need to start the NTP server manually or reboot to start it.
hostname#
```

inet dhcp server range

Команда используется для задания диапазона IP-адресов, выделяемых DHCP-сервером своим клиентам.

Синтаксис

```
inet dhcp server range <начало диапазона> <конец диапазона>
```

Параметры и ключевые слова

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

Значения по умолчанию

- <начало диапазона> — 172.16.1.2.
- <конец диапазона> — 172.16.1.254.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Перед выполнением команды необходимо завершить работу DHCP-сервера (см. [inet dhcp server stop](#) на стр. 74).
- Конечный адрес диапазона должен быть не меньше начального.
- В локальной сети, маршрутизируемой в сеть 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 своим клиентам адреса из диапазона 192.168.10.2–192.168.10.254, выполните команду:

```
hostname# inet dhcp server range 192.168.10.2 192.168.10.254
```

inet dhcp server router

Команда используется для задания адреса шлюза по умолчанию, передаваемого DHCP-сервером своим клиентам.

Синтаксис

```
inet dhcp server router <адрес>
```

Параметры и ключевые слова

<адрес> — IP-адрес шлюза по умолчанию.

Значения по умолчанию

<адрес> — 172.16.1.1.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Перед выполнением команды необходимо завершить работу DHCP-сервера (см. [inet dhcp server stop](#) на стр. 74).
- IP-адрес шлюза должен принадлежать сети интерфейса и не должен входить в диапазон IP-адресов, выделяемых клиентам.

Пример использования

Чтобы DHCP-сервер передавал своим клиентам адрес шлюза по умолчанию 192.168.10.1, выполните команду:

```
hostname# inet dhcp server router 192.168.10.1
```

inet dhcp server start

Команда используется для запуска DHCP-сервера.

Синтаксис

```
inet dhcp server start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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
hostname#
```

inet dhcp server stop

Команда используется для завершения работы DHCP-сервера.

Синтаксис

```
inet dhcp server stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# inet dhcp server stop
stopped /usr/sbin/udhcpd (pid 5831)
hostname#
```

inet dns clients add

Команда используется для добавления заданного адреса или подсети в список клиентов [DNS-сервера](#) (см. глоссарий, стр. 226), 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 управления.

Особенности использования

Нет.

Пример использования

Чтобы в список клиентов DNS-сервера добавить узлы из подсети 192.168.10.0/16, выполните команду:

```
hostname# inet dns clients add 192.168.10.0/16
```

inet dns clients delete

Команда используется для удаления заданного адреса или подсети из списка клиентов [DNS-сервера](#) (см. глоссарий, стр. 226), 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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

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

Пример использования

Чтобы из списка клиентов DNS-сервера удалить ключевое слово `any`, по умолчанию присутствующее в списке, выполните команду:

```
hostname# inet dns clients delete any
```

inet dns clients list

Команда предназначена для просмотра текущего списка DNS-клиентов, которым разрешена передача запросов DNS-серверу.

Синтаксис

```
inet dns clients list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

В примере ниже список содержит только ключевое слово `any` (любые узлы), по умолчанию присутствующее в списке:

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

inet dns forwarders add

Команда используется для добавления сервера с заданным адресом в список DNS-серверов (`forwarder`), которые передают запросы DNS-серверу внешней сети.

Синтаксис

```
inet dns forwarders add <адрес>
```

Параметры и ключевые слова

<адрес> — IP-адрес сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы в список DNS-серверов пересылки добавить сервер с адресом 10.0.2.3, выполните команду:

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

inet dns forwarders delete

Команда используется для удаления сервера с заданным адресом из списка DNS-серверов (`forwarder`), которые передают запросы DNS-серверу внешней сети.

Синтаксис

```
inet dns forwarders delete <адрес>
```

Параметры и ключевые слова

<адрес> — IP-адрес удаляемого сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

При вводе адреса работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка DNS-серверов пересылки.

Пример использования

Чтобы из списка DNS-серверов пересылки удалить сервер с адресом 10.0.2.3, выполните команду:

```
hostname# inet dns forwarders delete 10.0.2.3
```

inet dns forwarders list

Команда предназначена для просмотра текущего списка DNS-серверов пересылки (forwarder).

Синтаксис

```
inet dns forwarders list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.

- Режим управления.

Особенности использования

Если адреса DNS-серверов пересылки не заданы (список пустой), то выводится информация о том, что используются корневые DNS-серверы.

Пример использования

```
hostname> inet dns forwarders list
Forward DNS requests to servers:
10.0.2.3
hostname>
```

inet dns mode

Команда используется для включения или выключения автоматического запуска DNS-сервера при загрузке ViPNet Coordinator KB.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

Задается при установке [справочников и ключей](#) (см. глоссарий, стр. 233).

Режимы командного интерпретатора

Режим управления.

Особенности использования

- По команде изменяется только настройка автоматического запуска DNS-сервера, его текущее состояние не изменяется.
- Невозможно включить автоматический запуск, если DNS-сервер не запущен.
- Невозможно выключить автоматический запуск, если DNS-сервер запущен.

Пример использования

Чтобы выключить автоматический запуск DNS-сервера, выполните команду:

```
hostname# inet dns mode off
```

inet dns start

Команда используется для запуска DNS-сервера.

Синтаксис

```
inet dns start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# inet dns start
Starting domain name service...: bind9.
hostname#
```

inet dns stop

Команда используется для завершения работы DNS-сервера.

Синтаксис

```
inet dns stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# inet dns stop
Stopping domain name service...: bind9 waiting for pid 2902 to die
hostname#
```

inet ifconfig address

Команда используется для установки параметров заданного [интерфейса](#) (см. глоссарий, стр. 233).

Синтаксис

```
inet ifconfig <интерфейс> address <IP-адрес> netmask <маска>
```

Параметры и ключевые слова

- <интерфейс> — имя интерфейса.
- <IP-адрес> — IP-адрес.
- <маска> — маска подсети.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При вводе интерфейса работают автозаполнение 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 требуется завершить работу DHCP-сервера (см. [inet dhcp server stop](#) на стр. 74).
- При изменении адреса интерфейса в [таблице маршрутизации](#) (см. глоссарий, стр. 234) автоматически изменяются все маршруты, связанные с этим интерфейсом. Необходимо скорректировать 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.
- Не рекомендуется в качестве маски подсети использовать маски 255.255.255.254 и 255.255.255.255.

Пример использования

Чтобы на интерфейсе `eth1` установить IP-адрес 192.168.10.1 и маску подсети 255.255.255.0, выполните команду:

```
hostname# inet ifconfig eth1 address 192.168.10.1 netmask 255.255.255.0
```

inet ifconfig address add

Команда используется для добавления дополнительного IP-адреса на заданный 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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При вводе интерфейса работают автозаполнение 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

Чтобы на интерфейсе `eth1` установить дополнительный IP-адрес `192.168.10.2` с маской подсети `255.255.255.0`, выполните команду:

```
hostname# inet ifconfig eth1 address add 192.168.10.2 netmask 255.255.255.0
Alias eth1:0 has been created.
hostname#
```

В результате появится новый виртуальный интерфейс с именем `eth1:0`, адресом `192.168.10.2` и маской подсети `255.255.255.0`.

inet ifconfig address delete

Команда используется для удаления дополнительного IP-адреса с заданного 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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При вводе интерфейса работают автозаполнение 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`, выполните команду:

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

inet ifconfig class

Команда используется для установки класса заданного интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> class {access | trunk}
```

Параметры и ключевые слова

- `<интерфейс>` — имя интерфейса.
- `trunk` — класс интерфейсов, предназначенных для передачи трафика из нескольких [VLAN](#) (см. глоссарий, стр. 228).
- `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 управления.

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` требуется удалить все виртуальные интерфейсы, созданные на базе указанного интерфейса.

Пример использования

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

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

inet ifconfig dhcp

Команда используется для установки режима 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 управления.

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, выполните команду:

```
hostname# inet ifconfig eth1 dhcp
```

Чтобы установить на интерфейсе `eth2` режим DHCP и выключить автоматический прием маршрута по умолчанию, выполните команду:

```
hostname# inet ifconfig eth2 dhcp route off
```

inet ifconfig dhcp route-metric

Команда используется для задания специфичной [метрики](#) (см. глоссарий, стр. 232) 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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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](#) на стр. 60).

Пример использования

Чтобы назначить на сетевом интерфейсе `eth0` метрику 50, выполните команду:

```
hostname# inet ifconfig eth0 dhcp route-metric 50
```

Чтобы удалить метрику на сетевом интерфейсе `eth0`, выполните команду:

```
hostname# inet ifconfig eth0 dhcp route-metric none
```

inet ifconfig down

Команда используется для выключения заданного интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> down
```

Параметры и ключевые слова

<интерфейс> — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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, выполните команду:

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

inet ifconfig reset

Команда используется для сброса настроек заданного сетевого интерфейса либо всех интерфейсов.

Синтаксис

```
inet ifconfig {<интерфейс> | all} reset
```

Параметры и ключевые слова

- <интерфейс> — имя интерфейса.
- all — все интерфейсы.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При выполнении команды с параметром all происходит сброс настроек всех физических интерфейсов. Все виртуальные интерфейсы при этом удаляются.
- 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`, выполните команду:

```
hostname# inet ifconfig eth1 reset
This command will reset eth1 interface settings to default
Continue? [Yes,No]: Yes
done.
hostname#
```

inet ifconfig speed

Команда используется для установки параметров скорости заданного интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> speed <скорость> duplex {half | full}
```

Параметры и ключевые слова

- <интерфейс> — имя интерфейса.
- <скорость> — скорость в Мбит/с. Можно указать одно из следующих значений: 10, 100, 1000.
- `half` — полудуплекс (см. глоссарий, стр. 232).
- `full` — полный дуплекс (см. глоссарий, стр. 229).

Значения по умолчанию

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

Режимы командного интерпретатора

Режим управления.

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.
- 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.

Пример использования

Чтобы на интерфейсе `eth1` установить скорость 100 Мбит/с и режим полудуплекса, выполните команду:

```
hostname# inet ifconfig eth1 speed 100 duplex half
```

inet ifconfig speed auto

Команда используется для установки на заданном интерфейсе режима автоматического определения параметров скорости.

Синтаксис

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

Параметры и ключевые слова

<интерфейс> — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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, выполните команду:

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

inet ifconfig up

Команда используется для включения заданного интерфейса.

Синтаксис

```
inet ifconfig <интерфейс> up
```

Параметры и ключевые слова

<интерфейс> — имя интерфейса.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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`, выполните команду:

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

inet ifconfig vlan add

Команда используется для создания интерфейса для [виртуальной сети](#) (см. глоссарий, стр. 228) с заданным номером.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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, выполните команду:

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

inet ifconfig vlan delete

Команда используется для удаления заданного виртуального интерфейса.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При вводе номера работают автозаполнение и подсказка, данные для подсказки берутся из списка существующих виртуальных интерфейсов.
- Невозможно удалить виртуальный интерфейс, заданный как рабочий в параметрах функции L2OverIP, если эта функция включена.

Пример использования

Чтобы удалить виртуальный интерфейс `eth1.2`, выполните команду:

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

inet ntp add

Команда предназначена для добавления сервера с заданным адресом в список [NTP-серверов](#) (см. глоссарий, стр. 227), используемых для синхронизации времени.

Синтаксис

```
inet ntp add {server | peer} {<адрес> | <DNS-имя>}
```

Параметры и ключевые слова

- `server` — используется для добавления адреса NTP-сервера, работающего в одностороннем режиме (рассылка данных времени).
- `peer` — используется для добавления адреса NTP-сервера, работающего в двустороннем режиме (рассылка и получение данных времени).
- `<адрес>` — IP-адрес сервера.
- `<DNS-имя>` — DNS-имя сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы в список NTP-серверов добавить сервер `ntp.psn.ru`, работающий в одностороннем режиме, выполните команду:

```
hostname# inet ntp add server ntp.psn.ru
```

inet ntp delete

Команда предназначена для удаления сервера с заданным адресом из списка NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp delete {<адрес> | <DNS-имя>}
```

Параметры и ключевые слова

- `<адрес>` — IP-адрес удаляемого сервера.
- `<DNS-имя>` — DNS-имя удаляемого сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

При вводе адреса или DNS-имени работают автозаполнение и подсказка, данные для подсказки берутся из текущего списка NTP-серверов.

Пример использования

Чтобы из списка NTP-серверов удалить сервер `ntp.psn.ru`, выполните команду:

```
hostname# inet ntp delete ntp.psn.ru
```

inet ntp list

Команда предназначена для просмотра текущего списка NTP-серверов, используемых для синхронизации времени.

Синтаксис

```
inet ntp list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> inet ntp list
NTP servers list:
10.0.2.1 from USER
10.0.2.4 from USER
```

```
hostname>
```

inet ntp mode

Команда используется для включения или выключения автоматического запуска NTP-сервера при загрузке ViPNet Coordinator KB.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение автоматического запуска.
- `off` — выключение автоматического запуска.

Значения по умолчанию

Задается при установке [справочников и ключей](#) (см. глоссарий, стр. 233).

Режимы командного интерпретатора

Режим управления.

Особенности использования

- По команде изменяется только настройка автоматического запуска NTP-сервера, его текущее состояние не изменяется.

Пример использования

Чтобы выключить автоматический запуск NTP-сервера, выполните команду:

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

inet ntp orphan

Команда предназначена для включения и выключения перехода 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 параметру `<stratum>` устанавливается значение 5

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы настроить переход локального NTP-сервера в изолированный режим при потере соединения с внешними NTP-серверами 5го уровня, выполните команду:

```
hostname# inet ntp orphan on 5
```

inet ntp start

Команда используется для запуска NTP-сервера.

Синтаксис

```
inet ntp start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# inet ntp start
```

inet ntp stop

Команда используется для завершения работы NTP-сервера.

Синтаксис

```
inet ntp stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

inet ospf mode

Команда предназначена для включения или выключения использования протокола [OSPF](#) (см. глоссарий, стр. 227).

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# inet ospf mode on
Loading capability module if not yet done.
Starting Quagga daemons (prio:10): ospfd.
Stopping Quagga monitor daemons: watchquagga.
Loading capability module if not yet done.
Stopping Quagga monitor daemons: watchquagga.
```

inet ospf network add

Команда используется для добавления сети, в которой должна осуществляться маршрутизация по протоколу [OSPF](#) (см. глоссарий, стр. 227).

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 (см. глоссарий, стр. 232).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Если использование протокола OSPF (см. глоссарий, стр. 227) 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

```
hostname#
```

inet ospf network delete

Команда используется для удаления сети, которая была указана как маршрутизируемая по протоколу OSPF (см. глоссарий, стр. 227).

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 (см. глоссарий, стр. 232).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Если [использование протокола OSPF](#) (см. глоссарий, стр. 227) 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

```
hostname#
```

inet ospf redistribute add

Команда используется для включения [перераспределения](#) (см. глоссарий, стр. 232) статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол [OSPF](#) (см. глоссарий, стр. 227).

Синтаксис

```
hostname# inet ospf redistribute add {static | dhcp}
```

Параметры и ключевые слова

- `static` — включение перераспределения статических маршрутов;
- `dhcp` — включение перераспределения маршрутов DHCP-сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Команда не будет выполнена в следующих случаях:

- Не включено использование протокола OSPF (см. [inet ospf mode](#) на стр. 98).
- Перераспределение указанного типа маршрутов было включено ранее.

Пример использования

```
hostname# inet ospf redistribute add static
Redistribution of static routes has been enabled.
hostname#
```

inet ospf redistribute delete

Команда используется для выключения [перераспределения](#) (см. глоссарий, стр. 232) статических маршрутов или маршрутов DHCP-сервера, которое позволяет выполнять протокол [OSPF](#) (см. глоссарий, стр. 227).

Синтаксис

```
hostname# inet ospf redistribute delete {static | dhcp}
```

Параметры и ключевые слова

- `static` — выключение перераспределения статических маршрутов;
- `dhcp` — выключение перераспределения маршрутов DHCP-сервера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Команда не будет выполнена в следующих случаях:

- Не включено использование протокола OSPF (см. [inet ospf mode](#) на стр. 98).

- Перераспределение указанного типа маршрутов не было включено ранее.

Пример использования

```
hostname# inet ospf redistribute delete static
Redistribution of static routes has been disabled.
hostname#
```

inet ping

Команда используется для проверки соединения с заданным IP-адресом.

Синтаксис

```
inet ping <IP-адрес>
```

Параметры и ключевые слова

<IP-адрес> — IP-адрес, с которым необходимо проверить соединение.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Для завершения проверки соединения используется сочетание клавиш **Ctrl+C**.

Пример использования

Чтобы проверить соединение с адресом 10.0.2.1, выполните команду:

```
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
hostname>
```

inet route add

Команда используется для добавления статического [маршрута](#) (см. глоссарий, стр. 231).

Синтаксис

```
inet route add {<IP-адрес назначения> | default} next-hop <IP-адрес шлюза> [netmask
<маска> [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.
- [distance <1-255>] — [административная дистанция](#) (см. глоссарий, стр. 228).
- [weight <1-255>] — [вес](#) (см. глоссарий, стр. 229).

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 управления.

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](#) на стр. 106).

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, выполните команду:

```
hostname# inet route add 10.10.0.0 next-hop 172.16.5.1 netmask 255.255.0.0 distance 15
```

Чтобы добавить маршрут по умолчанию, для которого IP-пакеты будут передаваться на шлюз 172.16.5.2, выполните команду:

```
hostname# inet route add default next-hop 172.16.5.2
```

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, выполните команды:

```
hostname# inet route add 10.0.5.0 next-hop 10.0.1.1 netmask 255.255.255.0 distance 20 weight 1
```

```
hostname# inet route add 10.0.5.0 next-hop 10.0.4.3 netmask 255.255.255.0 distance 20 weight 1
```

В результате последние два маршрута будут просуммированы — объединены в один маршрут с двумя шлюзами.

inet route clear

Команда используется для удаления всех маршрутов, в том числе маршрута по умолчанию.

Синтаксис

```
inet route clear
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы удалить все маршруты, выполните команду:

```
hostname# inet route clear
```

inet route delete

Команда используется для удаления маршрута.

Синтаксис

```
inet route delete {<IP-адрес назначения> | default} [netmask <маска> [next-hop <IP-адрес шлюза>]]
```

Параметры и ключевые слова

- <IP-адрес назначения> — IP-адрес назначения.
- default — маршрут по умолчанию.
- <маска> — маска подсети.
- <IP-адрес шлюза> — IP-адрес шлюза.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Для маршрута по умолчанию не указывается маска подсети.
- Если в удаляемом маршруте не указаны маска сети и IP-адрес шлюза, то производится 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 символ `y` и

нажмите клавишу **Enter**. Аналогичная ситуация возникнет при удалении маршрута с несколькими шлюзами.

Пример использования

Чтобы удалить маршрут с адресом назначения 10.0.14.0, выполните команду:

```
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.
hostname#
```

inet show dhcp client

Команда предназначена для просмотра настроек DHCP на сетевых интерфейсах (настроек DHCP-клиента).

Синтаксис

```
inet show dhcp client
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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
eth2         no       yes       default   yes      yes
eth3         no       yes       default   yes      yes
hostname>
```

По команде выводится следующая информация:

- административная дистанция, которая задана для маршрутов, поступающих от DHCP-сервера;
- метрика по умолчанию;
- список сетевых интерфейсов со следующими параметрами:
 - статус режима DHCP: включен (*yes*) или выключен (*no*);
 - разрешение на автоматическое получение IP-адресов;
 - специфичные метрики на сетевых интерфейсах, если такие заданы;
 - разрешение на автоматическое получение адресов DNS-серверов;
 - разрешение на автоматическое получение адресов NTP-серверов.

inet show dhcp relay

Команда предназначена для просмотра настроек службы DHCP-relay и ее текущего состояния.

Синтаксис

```
inet show dhcp relay
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> inet show dhcp relay
Mode of dhcp relay is set to off
The server for forwarding dhcp relay requests is set in 172.16.1.1
The interface on which side is dhcp the server is eth1
The list of interfaces on which will listen dhcp requests: eth2
Service dhcp relay is running
hostname>
```

inet show dhcp server

Команда предназначена для просмотра настроек DHCP-сервера и его текущего состояния.

Синтаксис

```
inet show dhcp server
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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
hostname>
```

inet show dns

Команда предназначена для просмотра текущего состояния DNS-сервера.

Синтаксис

```
inet show dns
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

inet show interface

Команда предназначена для просмотра параметров заданного интерфейса и его текущего состояния.

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).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

- При вводе 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, выполните команду:

```
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

Команда предназначена для просмотра ARP-таблицы (таблицы преобразования IP-адресов в MAC-адреса).

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.

- Режим управления.

Особенности использования

Нет.

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
172.16.5.3       ether   4c:02:89:08:ef:24  C           eth3
hostname>
```

inet show ntp

Команда предназначена для просмотра настроек NTP-сервера и его текущего состояния.

Синтаксис

```
inet show ntp
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

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

Команда предназначена для просмотра настроек протокола OSPF.

Синтаксис

```
inet show ospf configuration
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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

Команда предназначена для просмотра информации о состоянии каналов связей между всеми OSPF-маршрутизаторами в базе данных (link state database).

Синтаксис

```
inet show ospf database
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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]

hostname>

inet show ospf neighbour

Команда предназначена для просмотра сведений о соседних OSPF-маршрутизаторах, работающих в вашей сети по протоколу OSPF.

Синтаксис

```
inet show ospf neighbour
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmt1	Rqst1	DBsm1
10.1.30.5	1	Full/DR	33.310s	10.0.5.5	eth0:10.0.5.2	0	0	0

hostname>

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 routing

Команда предназначена для просмотра содержимого общей таблицы маршрутизации или списков 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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

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

Команда используется для просмотра информации 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
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> inet show snmp
VPN SNMP agent mode is ON.
VPN SNMP agent is RUNNING.
debug-level = info
trapsink = 192.168.0.1
hostname>
```

inet show snmp community

Команда используется для просмотра следующих паролей:

- 1 Пароль для авторизации на удаленной станции сетевого менеджмента, заданный с помощью команды `inet snmp community trap` (на стр. 123).
- 2 Текущий пароль доступа к SNMP-параметрам ViPNet Coordinator KB, заданный с помощью команды `inet snmp community ro` (на стр. 122).

Синтаксис

```
inet show snmp community
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

inet show vlan

Команда предназначена для просмотра списка существующих виртуальных интерфейсов.

Синтаксис

```
inet show vlan
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> inet show vlan
VLAN interfaces
Id      | Name      | IP          | Parent | Comment
11     | eth2.11  | 172.16.11.2 | eth2   | VLAN11
12     | eth2.12  | 172.16.12.2 | eth2   | VLAN12
13     | eth2.13  | 172.16.13.2 | eth2   | VLAN13
14     | eth2.14  | 172.16.14.2 | eth2   | VLAN14
hostname>
```

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.

inet snmp community ro

Команда используется для задания пароля доступа к SNMP-параметрам вашего ViPNet Coordinator КВ.

Синтаксис

```
inet snmp community ro <пароль>
```

Параметры и ключевые слова

<пароль> — последовательность, содержащая от 6 до 18 символов.

Значения по умолчанию

По умолчанию задан пароль `public`.

Режимы командного интерпретатора

Режим управления.

Особенности использования

В паролях вы можете использовать символы латинского алфавита, цифры, а также следующие специальные символы: «.», «*», «/», «-», «:», «_», «?», «=», «@», «&», «(», «)», «,».

Пример использования

Чтобы задать пароль `Aa1234567`, выполните команду:

```
hostname# inet snmp community ro Aa1234567
hostname#
```

inet snmp community trap

Команда используется для задания пароля, используемого при авторизации на удаленной станции сетевого менеджмента, принимающей оповещения SNMP Traps.

Синтаксис

```
inet snmp community trap <пароль>
```

Параметры и ключевые слова

<пароль> — последовательность, содержащая от 6 до 18 символов

Значения по умолчанию

По умолчанию задан пароль `public`.

Режимы командного интерпретатора

Режим управления.

Особенности использования

В паролях вы можете использовать символы латинского алфавита, цифры, а также следующие специальные символы: «.», «*», «/», «-», «:», «_», «?», «=», «@», «&», «(», «)», «,».

Пример использования

Чтобы задать пароль `Aa1234567`, выполните команду:

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

inet snmp debug-level

Команда используется для задания событий SNMP-агента, которые будут записываться в журнал событий.

Синтаксис

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

Параметры и ключевые слова

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

- `off` — протоколирование выключено.
- `info` — протоколируется только информация, касающаяся инициализации SNMP-агента.
- `debug` — протоколируется служебная информация, используемая при отладке.
- `error` — протоколируются ошибки, после которых SNMP-агент может продолжать работу.
- `critical` — протоколируются критические ошибки, после которых SNMP-агент не может продолжить работу.

Значения по умолчанию

По умолчанию используется уровень `info`.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы выключить протоколирование событий SNMP-агента, выполните команду:

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

inet snmp mode

Команда предназначена для включения или выключения запуска SNMP-агента при загрузке ViPNet Coordinator KB.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение запуска SNMP-агента при загрузке ViPNet Coordinator KB.
- `off` — выключение запуска SNMP-агента при загрузке ViPNet Coordinator KB.

Значения по умолчанию

По умолчанию запуск SNMP-агента при загрузке ViPNet Coordinator KB включен (`on`).

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

```
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 have it running.
```

```
hostname#
```

inet snmp start

Команда используется для запуска встроенного SNMP-агента.

Синтаксис

```
inet snmp start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

inet snmp stop

Команда используется для завершения работы встроенного SNMP-агента.

Синтаксис

```
inet snmp stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# inet snmp stop
Stopping VPN SNMP agent: vpn-snmpd.
hostname#
```

inet snmp trapsink

Команда используется для задания сетевого узла, на который будут направляться оповещения по протоколу `SNMP`.

Синтаксис

```
inet snmp trapsink {<IP-адрес> | HOST | null}
```

Параметры и ключевые слова

- `<IP-адрес>` — IP-адрес удаленного сетевого узла.
- `HOST` — адрес локального сервера мониторинга.
- `null` — выключить оповещения.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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` выполните команду:

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

inet vlan comment add

Команда используется для добавления комментария к виртуальной сети с заданным номером.

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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы добавить комментарий «This is VLAN number 10» к виртуальной сети с номером 10, выполните команду:

```
hostname# inet vlan 10 comment add "This is VLAN number 10"
```

inet vlan comment delete

Команда используется для удаления комментария к виртуальной сети с заданным номером.

Синтаксис

```
inet vlan <номер> comment delete
```

Параметры и ключевые слова

<номер> — номер виртуальной сети.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы удалить комментарий к виртуальной сети с номером 10, выполните команду:

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

Команды группы `iplir`

Команды группы `iplir` предназначены для настройки параметров работы в защищенной сети [ViPNet](#) (см. глоссарий, стр. 233), а также для настройки параметров функции [L2OverIP](#) (см. глоссарий, стр. 227).

`iplir config`

Команда используется для редактирования одного из файлов конфигурации: основного файла конфигурации или файла конфигурации заданного интерфейса.

Синтаксис

```
iplir config <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя [статического интерфейса](#) (см. глоссарий, стр. 233), для которого требуется редактировать файл конфигурации.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Если в команде не указан параметр, то будет запущен текстовый редактор с основным файлом конфигурации `iplir.conf`.
- Перед редактированием файла `iplir.conf` или файла `iplir.conf-<интерфейс или группа интерфейсов>` требуется завершить работу демона `iplircfg` (см. [iplir stop](#) на стр. 155).

Пример использования

Чтобы отредактировать файл конфигурации интерфейса `eth0`, выполните команду:

```
hostname# iplir config eth0
```

iplir info

Команда предназначена для просмотра информации о своем узле и количестве туннельных соединений, а также для просмотра статистики фильтрации IP-пакетов по заданному интерфейсу или группе интерфейсов.

Синтаксис

```
iplir info <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя [статического интерфейса](#) (см. глоссарий, стр. 233), для которого требуется просмотреть статистику фильтрации IP-пакетов.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

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 был запущен демон `iplircfg`.

Пример использования

Для просмотра статистики по интерфейсу `eth0` выполните команду:

```
hostname> iplir info eth0
Interface:          eth0
```

Category	Received	Sent
Non-encrypted packets passed:	0	0
Non-encrypted packets dropped:	0	0

```

Non-encrypted bytes passed:          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 passed: 0          0
Non-encrypted broadcast packets dropped: 2          0
Non-encrypted broadcast bytes passed:   0          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          271
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

Команда предназначена для просмотра текущего состояния или значения одного из параметров [межсетевого экрана](#) (см. глоссарий, стр. 231).

Синтаксис

```
iplir option get <параметр>
```

Параметры и ключевые слова

<параметр> — имя параметра межсетевого экрана. Можно указать один из следующих параметров:

- `antispoofing` — состояние функции [антиспуфинга](#) (см. глоссарий, стр. 228);

- `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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

Для просмотра состояния функции блокирования IP-пакетов выполните команду:

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

iplir option set antispoofing

Команда используется для включения или выключения [антиспуфинга](#) (см. глоссарий, стр. 228).

Синтаксис

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

Параметры и ключевые слова

- `on` — включение антиспуфинга.

- `off` — выключение антиспуфинга.

Значения по умолчанию

По умолчанию антиспуфинг выключен (`off`).

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Для включения антиспуфинга выполните команду:

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

iplir option set block-other-protocols

Команда используется для включения или выключения блокирования IP-пакетов, которые передаются по протоколам, отличным от IP, ARP или RARP.

Синтаксис

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

Параметры и ключевые слова

- `on` — включение блокирования.
- `off` — выключение блокирования.

Значения по умолчанию

По умолчанию блокирование выключено (`off`).

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Для включения блокирования выполните команду:

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

iplir option set cleanup-interval

Команда используется для задания времени, по истечении которого будут удаляться устаревшие соединения (с истекшим тайм-аутом).

Синтаксис

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

Параметры и ключевые слова

<значение> — время в десятых долях секунды.

Значения по умолчанию

20 (2 секунды).

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

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

iplir option set connection-ttl-ip

Команда используется для задания 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 управления.

Особенности использования

Нет.

Пример использования

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

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

iplir option set connection-ttl-tcp

Команда используется для задания 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 управления.

Особенности использования

Нет.

Пример использования

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

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

iplir option set connection-ttl-udp

Команда используется для задания времени жизни соединения по протоколу UDP при отсутствии активности в нем.

Синтаксис

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

Параметры и ключевые слова

<значение> — время в секундах.

Значения по умолчанию

300 секунд.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

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

iplir option set dynamic-ports

Команда используется для задания диапазона 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 управления.

Особенности использования

Нет.

Пример использования

Чтобы задать диапазон портов 32800–64000, выполните команду:

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

iplir option set dynamic-timeouts

Команда используется для включения или выключения режима 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 — включение режима.

- `off` — выключение режима.

Значения по умолчанию

По умолчанию режим динамических тайм-аутов выключен (`off`).

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы включить режим динамических тайм-аутов соединений, выполните команду:

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

iplir option set max-connections

Команда используется для задания максимального количества параллельно установленных соединений.

Синтаксис

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

Параметры и ключевые слова

<количество> — количество соединений.

Значения по умолчанию

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

Таблица 3. Значения параметра `max-connections` для разных аппаратных платформ ViPNet Coordinator KB

Аппаратная платформа ViPNet Coordinator KB	Объем оперативной памяти	Значение по умолчанию	Максимальное значение
KB100 N1	2 Гбайт	150000	150000
KB1000 Q6	2 Гбайт	800000	1000000

Аппаратная платформа ViPNet Coordinator KB	Объем оперативной памяти	Значение по умолчанию	Максимальное значение
KB2000 Q4	4 Гбайт	2500000	3000000
KB5000 Q1	8 Гбайт	6000000	6500000

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы установить максимальное количество одновременных соединений равным 200000, выполните команду:

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

iplir ping

Команда используется для проверки соединения с заданным сетевым узлом ViPNet.

Синтаксис

```
iplir ping <идентификатор>
```

Параметры и ключевые слова

<идентификатор> — шестнадцатеричный идентификатор сетевого узла ViPNet, соединение с которым необходимо проверить.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

- При вводе идентификатора работают автозаполнение и подсказка, данные для подсказки берутся из списка связей ViPNet Coordinator KB с другими узлами.
- Для выполнения команды требуется, чтобы был запущен демон `iplircfg`.

Пример использования

Для проверки связи ViPNet Coordinator KB с узлом, который имеет идентификатор `0x15ea000d`, выполните команду:

```
hostname> iplir ping 0x15ea000d
```

iplir set l2overip interface

Команда используется для задания рабочего интерфейса в настройках функции [L2OverIP](#) (см. глоссарий, стр. 227).

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При вводе интерфейса работают автозаполнение и подсказка, данные для подсказки берутся из списка существующих Ethernet-интерфейсов.
- В качестве параметра можно указать физический или виртуальный Ethernet-интерфейс.

Пример использования

Чтобы в качестве рабочего интерфейса для функции L2OverIP задать виртуальный интерфейс `eth0.2`, выполните команду:

```
hostname# iplir set l2overip interface eth0.2
```

iplir set l2overip local-port

Команда используется для добавления параметров локального сегмента сети в настройки функции 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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

В качестве IP-адреса можно указать только статический адрес.

Пример использования

Чтобы добавить в настройки функции L2OverIP локальный сегмент сети с номером порта 1 и адресом 172.16.1.1, выполните команду:

```
hostname# iplir set l2overip local-port 1 172.16.1.1
```

iplir set l2overip mac-ttl

Команда используется для задания времени 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

По умолчанию установлено время 300 секунд.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы задать время жизни адреса в таблице MAC-адресов виртуального коммутатора 10 минут, выполните команду:

```
hostname# iplir set l2overip mac-ttl 600
```

iplir set l2overip mode

Команда используется для включения или выключения функции 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 управления.

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

Для включения функции L2OverIP выполните команду:

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

iplir set l2overip remote-port

Команда используется для добавления параметров удаленного сегмента сети в настройки 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).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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 в настройки функции L2OverIP удаленный сегмент сети с номером порта 2 и адресом 172.16.2.2, выполните команду:

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

iplir set l2overip remote-port delete

Команда используется для удаления порта с заданным номером из настроек функции L2OverIP.

Синтаксис

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

Параметры и ключевые слова

<порт> — номер удаляемого порта.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы удалить из настроек функции L2OverIP порт с номером 2, выполните команду:

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

iplir set l2overip unsolicited-frames

Команда используется для задания режима обработки одноадресных Ethernet-кадров с неизвестным MAC-адресом получателя при объединении сегментов сети с помощью функции L2OverIP.

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.

Значения по умолчанию

По умолчанию установлен режим `drop`.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы в настройках функции `L2OverIP` задать режим обработки `broadcast`, выполните команду:

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

iplir set thread-count

Команда используется для установки количества потоков в драйвере `drviplir`.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

По умолчанию число потоков в драйвере равно значению, заданному в лицензии.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Возможный диапазон значений — от 1 до количества логических процессоров в системе. Если значение параметра выходит за границы указанного допустимого диапазона, то число потоков устанавливается равным ближайшей границе (1 или числу процессоров).
- Если параметр не является натуральным числом, то появляется сообщение об ошибке.
- После выполнения команды на консоль выводится информация о фактически установленном числе потоков.

Пример использования

Для установки 3 потоков в драйвере `drviplir` выполните команду:

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

iplir show adapters

Команда предназначена для просмотра всех активных интерфейсов ViPNet Coordinator KB. При просмотре для каждого интерфейса в списке указан параметр `allowtraffic`, который показывает, разрешено или заблокировано прохождение IP-трафика через интерфейс.

Синтаксис

```
iplir show adapters
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

Для просмотра списка активных сетевых интерфейсов выполните команду:

```
hostname> iplir show adapters

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

iplir show config

Команда предназначена для просмотра одного из файлов конфигурации: основного файла конфигурации, файла конфигурации заданного интерфейса.

Синтаксис

```
iplir show config <интерфейс>
```

Параметры и ключевые слова

<интерфейс> — имя [статического интерфейса](#) (см. глоссарий, стр. 233), файл конфигурации которого требуется просмотреть.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

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

Пример использования

Чтобы просмотреть основной файл конфигурации, выполните команду:

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

iplir show firewall status

Команда предназначена для просмотра статистики работы межсетевого экрана.

Синтаксис

```
iplir show firewall status
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> iplir show firewall status
Max connections      800000
Dynamicport minimum  1025
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](#) на стр. 138).
- `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

Команда используется для получения информации о ключах, установленных на ViPNet Coordinator KB. Предоставляется информация о следующих ключах:

- [персональный ключ пользователя](#) (см. глоссарий, стр. 232);
- [резервный набор персональных ключей \(РНПК\)](#) (см. глоссарий, стр. 232);
- [ключи узла](#) (см. глоссарий, стр. 231).

Синтаксис

```
iplir show key-info
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

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: 2017-06-23 13:44:57 MSK
```

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

```
Current personal key update date: 2018-05-25 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: 2017-06-23 13:44:57 MSK
```

```
Lck key info: //Информация о ключах узла
```

```
User ID: 0x16310029
```

```
Master defense key date: 2017-06-23 13:44:57 MSK
```

Current defense key info:

AP ID: 0x1631002a

Current defense key variant: 0

Master defense key date: 2014-06-23 13:44:57 MSK

Master defense key number: 1

Current defense key update date: 2015-05-25 15:40:24 MSK

Cck key info:

Ap ID: AP ID: 0x1631002a

Master cck key date: 2014-06-23 13:44:57 MSK

hostname#

iplir show keys-upgrade-log

Команда предназначена для просмотра журнала, в котором содержится информация о принятых обновлениях [справочников и ключей](#) (см. глоссарий, стр. 233).

Синтаксис

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

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# iplir show keys-upgrade-log
19/05/2018 16:37:34.896 Starting upgrade process ...
19/05/2018 16:37:34.896 try find /opt/vipnet/ccs/ap*.dtm
...
hostname#
```

iplir show l2overip

Команда предназначена для просмотра текущего состояния или настроек функции L2OverIP.

Синтаксис

```
iplir show l2overip <опция>
```

Параметры и ключевые слова

<опция> — параметр команды, который может принимать одно из следующих 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 функции L2OverIP.
- `mac-address-table` — просмотр таблицы MAC-адресов, используемой функцией L2OverIP.
- `mac-hash-stats` — просмотр статистики хэш-таблицы MAC-адресов, используемой функцией L2OverIP. Информация предназначена для тестирования и локализации ошибок.
- `port-table` — просмотр таблицы портов, используемой функцией L2OverIP.
- `status` — просмотр текущего состояния функции L2OverIP: `switch` — включена, `none` — выключена.
- `virtual-switch-stats` — просмотр статистики по обработке Ethernet-кадров функцией L2OverIP: общее количество обработанных и заблокированных кадров, а также количество обработанных и заблокированных одноадресных кадров с неизвестным MAC-адресом получателя.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

Ниже приведен пример выполнения команды с параметром `config`:

```
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
hostname>
```

iplir show thread-count

Команда используется для просмотра количества потоков в драйвере `drviplir`.

Синтаксис

```
iplir show thread-count
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

Для просмотра количества потоков в драйвере `drviplir` выполните команду:

```
hostname> iplir show thread-count
3
hostname>
```

iplir start

Команда используется для запуска управляющего демона `iplircfg`.

Синтаксис

```
iplir start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> iplir start
Loading Kernel Interface driver
Loading Iplir Watchdog driver
Loading IpLir Crypto driver
Loading IpLir driver
Loading IPCLS driver
Loading IpLir
hostname>
```

iplir stop

Команда используется для завершения работы управляющего демона `iplircfg`.

Синтаксис

```
iplir stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

iplir view

Команда предназначена для просмотра журнала регистрации IP-пакетов.

Синтаксис

```
iplir view
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

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 был запущен демон `iplircfg`.
- При работе ViPNet Coordinator KB в режиме [кластера горячего резервирования](#) (см. глоссарий, стр. 230) на пассивном сервере кластера нельзя просмотреть журнал IP-пакетов.

Пример использования

```
hostname> iplir view
```

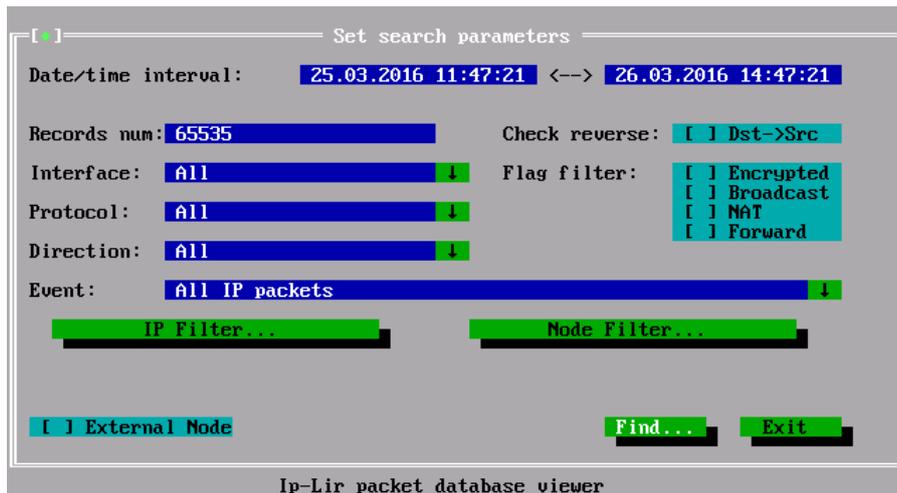


Рисунок 1. Задание параметров поиска записей в журнале регистрации IP-пакетов

Команды группы machine

Команды группы `machine` предназначены для выключения и перезагрузки ПАК, установки имени ПАК и системного времени, работы с журналом устранения неполадок, а также для регламентного тестирования ViPNet Coordinator KB.

machine halt

Команда используется для выключения ПАК.

Синтаксис

```
machine halt
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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

Команда используется для перезагрузки ПАК.

Синтаксис

```
machine reboot
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

machine self-test

Команда используется для запуска регламентного контроля целостности ViPNet Coordinator KB.

Синтаксис

```
machine self-test
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- До начала тестирования работа всех демонов будет автоматически завершена.
- В процессе регламентного тестирования производится проверка целостности модулей и файлов конфигурации, 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 демоны, 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 службу поддержки ОАО «ИнфоТекС».
- При успешной проверке целостности будет посчитано и выведено на экран значение контрольной суммы ПО ViPNet Coordinator KB и запрос подтверждения совпадения контрольной суммы выведенной на экран, с последней зафиксированной контрольной суммой.
 - 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.
 - 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 тестирования необходимо перезагрузить ViPNet Coordinator KB. Для этого в ответ на сообщение `Press enter to reboot` необходимо нажать **Enter**.

Пример использования

Чтобы запустить регламентное тестирование ViPNet Coordinator KB, выполните команду:

```
hostname# machine self-test
```

```
Machine self testing will be performed. Connection will be lost during testing!  
Daemons will be stopped. Continue? [Yes, No] Yes
```

```
First stage of machine self test was successful...
```

```
Checksum: 0x71a55eed
```

```
Is it correct? [Yes, No] Yes
New checksum: 0x71a55eed
Machine self test was successfull...
```

machine set date

Команда используется для переустановки даты и времени 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 — час, mm — минуты, ss — секунды.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Если требуется установить время отличающиеся от текущего значения ViPNet Coordinator KB больше 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.

Пример использования

Чтобы установить дату 22 июля 2014 года и время, равное 12 часам, выполните команду:

```
hostname# machine set date 2014-07-22 12:00:00
```

machine set hostname

Команда используется для установки имени ПАК.

Синтаксис

```
machine set hostname <имя>
```

Параметры и ключевые слова

<имя> — имя компьютера.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- По умолчанию имя ПАК сформировано по шаблону <название>-<идентификатор>, где <название> — наименование аппаратной платформы ViPNet Coordinator KB без последних двух символов, <идентификатор> — идентификатор сетевого узла. Например: KB1000-270E033A.
- Имя ПАК используется в качестве приглашения командного интерпретатора, а также указывается в начале сообщений, записываемых в протоколы работы при их хранении на жестком диске.

Пример использования

Чтобы установить имя ПАК KB1000, выполните команду:

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

machine set loghost

Команда используется для задания места хранения журнала устранения неполадок. С помощью этой команды также можно выключить запись событий в журнал.

Синтаксис

```
machine set loghost <IP-адрес>
```

Параметры и ключевые слова

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

Значения по умолчанию

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

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Если протоколы работы будут направляться на удаленный сетевой узел, 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

Для отправки журнала устранения неполадок на узел с адресом 192.168.10.10 выполните команду:

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

machine set timezone

Команда используется для установки временной зоны (часового пояса).

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.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

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.

Примеры использования

Чтобы просмотреть список временных зон в Антарктике, выполните команду:

```
hostname# machine set timezone Antarc?  
Antarctica/Casey  
Antarctica/Davis  
...  
hostname# machine set timezone Antarc
```

Чтобы установить часовой пояс Москвы, выполните команду:

```
hostname# machine set timezone Europe/Moscow
```

machine show date

Команда предназначена для просмотра текущих даты и времени.

Синтаксис

```
machine show date
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> machine show date  
Thu Sep 27 19:11:56 MSK 2018  
hostname>
```

machine show dnssd log

Команда используется для отображения журналов СКЗИ, сохраненных на жестком диске ViPNet Coordinator KB.

Синтаксис

```
machine show dnssd log
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

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

machine show dnssd log usb

Команда используется для отображения журналов СКЗИ, сохраненных на USB-носителе.

Синтаксис

```
machine show dnssd log usb
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Для просмотра журналов СКЗИ, сохраненных на USB-носителе подключите USB-носитель к <Product_name>.

Для того чтобы ViPNet Coordinator KB отобразил файлы журнала *.dnsc, они должны быть сохранены в корне файловой системы USB-носителя.

Пример использования

```
hostname# machine show dnsc log usb
```

machine show hostname

Команда предназначена для просмотра имени ПАК.

Синтаксис

```
machine show hostname
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> machine show hostname  
hostname  
hostname>
```

machine show loghost

Команда предназначена для просмотра места хранения журнала событий.

Синтаксис

```
machine show loghost
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

По команде выводится одно из следующих значений:

- `null` — протоколирование выключено.
- `local` — журнал событий хранится локально на сетевом узле ViPNet Coordinator KB.
- IP-адрес удаленного сетевого узла, заданный с помощью команды `machine set loghost`.

machine show logs

Команда предназначена для просмотра журнала событий.

Синтаксис

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

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- Для завершения просмотра используется клавиша **Q**.
- Параметр `<время>` задается в формате `YYYY-MM-DD hh:mm:ss`
- В параметре `<демон>` можно указать один из демонов в составе ПО ViPNet Coordinator KB. Полный список демонов см. в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора», разделе «Список демонов 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 необходимо взять 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 `<демон>` или `string <строка>`.

Пример использования

Чтобы найти все записи журнала событий за все время для всех демонов, выполните команду:

```
hostname# machine show logs
```

Чтобы найти все записи журнала событий, начиная с 14:50 22 ноября 2018 года, и отобразить их в обратном порядке, выполните команду:

```
hostname# machine show logs reversed since 2018-11-22 14:50:00
```

Чтобы найти все записи журнала событий для демона `vmunix`, выполните команду:

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

Чтобы найти записи журнала событий за все время его ведения, для всех демонов и где есть строка `command 3001`, выполните команду:

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

machine show memory

Команда предназначена для просмотра информации об использовании оперативной памяти, файла подкачки и файловой системы.

Синтаксис

```
machine show memory
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> machine show memory
      total    used    free  shared  buffers  cached
Mem:   2007    522   1485      0      102    362
-/+ buffers/cache:
Swap:      0      0      0
```

```
Filesystem      Size  Used Avail Use% Mounted on
rootfs          1004M  3,3M  1001M   1% /
tmpfs           1004M   60M   944M   6% /mnt/root
...
hostname>
```

machine show session-timeout

Команда предназначена для просмотра текущего допустимого времени неактивности сессии.

Синтаксис

```
machine show session-timeout
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

machine show timezone

Команда предназначена для просмотра текущей временной зоны (часового пояса).

Синтаксис

```
machine show timezone
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

machine show uptime

Команда предназначена для просмотра времени работы ViPNet Coordinator KB после загрузки, а также среднего числа процессов в очереди за ближайшее время.

Синтаксис

```
machine show uptime
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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` (на стр. 41).

Команды группы mftp

Команды группы `mftp` предназначены для настройки параметров [транспортного модуля MFTP](#) (см. глоссарий, стр. 234) и каналов обмена ViPNet Coordinator KB с другими узлами сети ViPNet.

mftp config

Команда используется для редактирования конфигурационного файла демона `mftpd`.

Синтаксис

```
mftp config
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

- При вводе команды работают автозаполнение и подсказка, данные для подсказки берутся из списка команд ViPNet Coordinator KB.
- Перед редактированием конфигурационного файла требуется завершить работу демона `mftpd` (см. [mftp stop](#) на стр. 177). Перед выполнением команды проверяется, завершена ли работа демона `mftpd`. Если демон запущен, то выдается ошибка.
- При выполнении команды запускается текстовый редактор, и в него загружается файл `mftp.conf`.
- При сохранении файла происходит проверка его корректности, и в случае ошибки предлагается отказаться от изменений или продолжить редактирование. Если проверка прошла успешно, файл применяется для работы демона `mftpd`, а информации об изменении конфигурации сохраняется в журнал событий.

Пример использования

Чтобы включить режим немедленной передачи конвертов по каналу обмена с узлом 0x270e000a, выполните команду:

```
hostname# mftp config
```

В открывшемся файле в секции [channel] для узла 0x270e000a присвойте параметру call_flag значение yes:

```
[channel]
id = 0x270e000a
name = Client-1
off_flag = no
call_flag = yes
type = MFTP
...
```

mftp info

Команда предназначена для просмотра очереди исходящих транспортных конвертов.

Синтаксис

```
mftp info
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

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** (см. глоссарий, стр. 232);
 - Control request — управляющий запрос;
 - Control request answer — ответ на управляющий запрос;
 - Task receipt — **прикладная квитанция** (см. глоссарий, стр. 232);
 - Transport receipt — **транспортная квитанция** (см. глоссарий, стр. 234).
- 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

Команда предназначена для просмотра файла конфигурации транспортного модуля.

Синтаксис

```
mftp show config
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

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

Пример использования

```
hostname> mftp show config
[channel]
id = 0x15ea0011
name = Client-1
off_flag = no
call_flag = no
type = MFTP
...
hostname>
```

mftp start

Команда используется для запуска транспортного модуля MFTP.

Синтаксис

```
mftp start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname# mftp start
Loading MFTP daemon
No mftp running. Starting it
Daemonizing...
hostname#
```

mftp stop

Команда используется для завершения работы транспортного модуля MFTP.

Синтаксис

```
mftp stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

```
hostname#
```

mftp view

Команда используется для просмотра журнала конвертов транспортного модуля MFTP.

Синтаксис

```
mftp view
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим управления.

Особенности использования

- Если вы выполняете команду на одном из узлов кластера горячего резервирования, отображается только информация о конвертах транспортного модуля, 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 Dec 11 16:45:48 2018
-----
-----
| Envelope filename | Personal envelope name | Sender | Receiver | Date-Time
|   Event          |   Size   | Description |   Task   |
-----
| ~OJ) (#(A.RJ9    | ~OJ) (#(A.RJ9          | Admin   | Coordinator HW VA |
11.12.2018 16:45:48
|   Received      |   19090  |           | File exchange  |
-----
-----
hostname#
```

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

Команды группы `ups` предназначены для настройки взаимодействия ViPNet Coordinator KB с источником бесперебойного питания (UPS) (см. глоссарий, стр. 230).

`ups set driver`

Команда используется для выбора драйвера 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`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы выбрать драйвер UPS, выполните команду:

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

`ups set mode`

Команда используется для установки режима взаимодействия ViPNet Coordinator KB с UPS.

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 UPS и который непосредственно взаимодействует с UPS.
- `slave` — взаимодействие в режиме подчиненного компьютера. Подчиненный компьютер взаимодействует с UPS через главный компьютер.
- `<IP-адрес мастера>` — IP-адрес главного компьютера, находящегося в режиме `master`.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Перед выполнением команды требуется вручную завершить работу демонов пакета [NUT \(Network UPS Tools\)](#) (см. глоссарий, стр. 227) с помощью команды `ups stop` (на стр. 185).

Пример использования

Для установки режима главного компьютера выполните команду:

```
hostname# ups set mode master
```

ups set monitoring

Команда используется для включения или выключения мониторинга состояния UPS.

Синтаксис

```
ups set monitoring {on | off}
```

Параметры и ключевые слова

- `on` — включение мониторинга.
- `off` — выключение мониторинга.

Значения по умолчанию

По умолчанию мониторинг состояния UPS выключен (офф).

Режимы командного интерпретатора

Режим управления.

Особенности использования

- После включения мониторинга необходимо вручную запустить демоны пакета NUT с помощью команды `ups start` (на стр. 184).
- При выключении мониторинга будет автоматически завершена работа демонов пакета NUT.

Пример использования

Чтобы включить мониторинг состояния UPS, выполните команду:

```
hostname# ups set monitoring on
```

ups show config

Команда предназначена для просмотра текущих настроек взаимодействия ViPNet Coordinator KB с UPS.

Синтаксис

```
ups show config
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> ups show config
UPS service mode is Master. Driver: usbhid-ups
UPS service is RUNNING
hostname>
```

По команде отображается следующая информация:

- Включен или выключен мониторинг состояния UPS. Остальная информация выводится только в случае, если мониторинг включен.
- Режим взаимодействия ViPNet Coordinator KB с UPS (*master* или *slave*).
- Используемый драйвер UPS (только в режиме *master*).
- IP-адрес мастера (только в режиме *slave*).
- Состояние демонов пакета *NUT* (запущены или работа демонов завершена).

ups show status

Команда предназначена для просмотра текущего состояния UPS.

Синтаксис

```
ups show status [extended]
```

Параметры и ключевые слова

extended — просмотр всех параметров состояния UPS в формате утилиты *upsc*, входящей в состав пакета *NUT*. Эта возможность предназначена для квалифицированных системных администраторов, которые могут самостоятельно интерпретировать результат вывода утилиты *upsc*.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

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
hostname>
```

По команде отображается следующая информация:

- Производитель UPS.
- Модель UPS.
- 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 UPS посылает сигнал о необходимости выключения компьютера (задается производителем UPS).

ups start

Команда используется для запуска демонов пакета `NUT`, обеспечивающих взаимодействие `VIPNet Coordinator KB` с UPS.

Синтаксис

```
ups start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы запустить демоны пакета `NUT`, выполните команду:

```
hostname> ups start
```

ups stop

Команда используется для завершения работы демонов пакета `NUT`, обеспечивающих взаимодействие ViPNet Coordinator KB с UPS.

Синтаксис

```
ups stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

Чтобы завершить работу демонов пакета `NUT`, выполните команду:

```
hostname> ups stop
```

Команды группы vpn

Команды группы `vpn` предназначены для загрузки и выгрузки драйверов и служб ViPNet.

`vpn start`

Команда используется для загрузки всех драйверов и запуска всех демонов ViPNet Coordinator KB.

Синтаксис

```
vpn start
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Команда выполняется только в том случае, если перед этим была выполнена команда `vpn stop` или если демоны и драйверы не были запущены при загрузке ViPNet Coordinator KB (например, если вы не выбрали запуск сервисов VPN после разворачивания дистрибутива ключей). Если некоторые демоны были остановлены с помощью соответствующих команд, то команда `vpn start` не будет выполнена (отобразится сообщение `Failover daemon is already running (PID XXXX). Exit.`). Вместо нее используйте команды запуска демонов. Например, после выполнения команд `iplir stop` и `mftsp stop` для запуска демонов `iplir` и `mftsp` выполните команды `iplir start` и `mftsp start`.

Пример использования

Для загрузки драйверов и запуска демонов ViPNet Coordinator KB выполните команду:

```
hostname# vpn start
```

vpn stop

Команда используется для выгрузки драйверов и завершения работы демонов ViPNet Coordinator KB.

Синтаксис

```
vpn stop
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Нет.

Пример использования

Для выгрузки драйверов и завершения работы демонов ViPNet Coordinator KB выполните команду:

```
hostname# vpn stop
Shutting down failover daemon
Shutting down MFTP daemon
Shutting down Alg daemon
Shutting down IpLir
Unloading IpLir driver
```

Прочие команды

К прочим относятся команды, которые не входят ни в одну из групп команд, описанных выше.

debug off

Команда используется для выключения вывода сообщений о событиях.

Синтаксис

```
debug off [<источник> <важность>]
```

Параметры и ключевые слова

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

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим управления.

Особенности использования

Если в команде не указаны параметры, то будет выключен вывод всех сообщений.

Пример использования

Чтобы выключить вывод сообщений об ошибках демонов, выполните команду:

```
hostname# debug off daemon err
```

debug on

Команда используется для включения вывода сообщений о событиях.

Синтаксис

```
debug on [<источник> <важность>]
```

Параметры и ключевые слова

- `<источник>` — процесс, для которого должны выводиться сообщения. Например:
 - `kern` (ядро);
 - `user` (пользовательские программы);
 - `mail` (почтовая система);
 - `daemon` (демоны).
- `<важность>` — уровень серьезности выводимых сообщений. Например:
 - `err` (ошибка);
 - `info` (информационное сообщение);
 - `debug` (отладочное сообщение).

Значения по умолчанию

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

Режимы командного интерпретатора

Режим управления.

Особенности использования

Для демонов 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 демонов, выполните команду:

```
hostname# debug on daemon err
```

enable

Команда используется для перехода в режим управления.

Синтаксис

```
enable
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

Режим наблюдения.

Особенности использования

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

Пример использования

```
hostname> enable
Enter administrator password:
hostname#_
```

exit

Команда используется для выхода из текущего режима командного интерпретатора.

Синтаксис

```
exit
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

- В результате выполнения команды в режиме управления происходит переход в режим наблюдения.

- В результате выполнения команды в режиме наблюдения происходит завершение работы командного интерпретатора. При этом отображается приглашение ввести ПИН-код для запуска командного интерпретатора.

Пример использования

```
hostname# exit
hostname>
```

version features list

Команда предназначена для просмотра списка функциональных модулей, входящих в состав текущей версии ViPNet Coordinator KB.

Синтаксис

```
version features list
```

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

version

Команда предназначена для просмотра текущей версии ViPNet Coordinator KB и его компонентов.

Синтаксис

```
version [full]
```

Параметры и ключевые слова

`full` — просмотр текущей версии всех компонентов, а также других параметров (набор функционала для текущего исполнения, архитектура процессора).

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

```
hostname> version
Product: ViPNet L2
Platform: KB1000 Q6
License: KB1000
Software version: 4.1-160
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.

who

Команда предназначена для просмотра информации о запущенных сессиях командного интерпретатора (локальной и всех удаленных).

Синтаксис

`who`

Параметры и ключевые слова

Нет.

Значения по умолчанию

Нет.

Режимы командного интерпретатора

- Режим наблюдения.
- Режим управления.

Особенности использования

Нет.

Пример использования

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

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 наблюдения) или `admin` (Режим управления).
- `COMMENTS` — комментарий, содержащий информацию о консоли (обычно информация о местонахождении).

2

Справочник по конфигурационным файлам

Файл failover.ini	195
Файл iplir.conf	202
Файл iplir.conf- <интерфейс>	215
Файл mftp.conf	217

Файл failover.ini

Настройка параметров работы системы защиты от сбоев осуществляется путем редактирования файла конфигурации `failover.ini`. Для редактирования файла конфигурации используется команда `failover config edit`. Перед редактированием файла необходимо завершить работу демона `failoverd` командой `failover stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его с помощью команды `failover start`.

Файл `failover.ini` содержит секции с параметрами, описанные ниже.

Секция [channel]

Каждый сетевой интерфейс активного сервера, работоспособность которого должна контролироваться системой защиты от сбоев при работе в режиме [кластера горячего резервирования](#) (см. глоссарий, стр. 230), 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 демона `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.

- o `no` — эхо-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 демона failoverd и содержит следующие параметры:

- `debuglevel` — уровень детализации информации, выводимой в журнал. Возможные значения: от 1 до 5 (по умолчанию 3). Чем выше уровень детализации, тем более подробная информация выводится в журнал. Значение параметра `-1` выключает ведение журнала.
- 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 ОАО «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` (демоны).
 - `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 какого-либо демона или драйвера ViPNet Coordinator KB. Возможные значения:
 - `yes` (по умолчанию) — включить механизм регистрации в `watchdog`-драйвере и перезагружать систему, если какой-либо демон или драйвер не может восстановить свою работу;
 - `no` — выключить механизм регистрации в `watchdog`-драйвере и не перезагружать систему, если какой-либо демон или драйвер не может восстановить свою работу.

Нередактируемые параметры секции [misc]

- `activeconfig` — абсолютный путь к файлу конфигурации управляющего демона, который будет использоваться на активном узле кластера. Значение по умолчанию — `/etc/iplirpsw`.

- `passiveconfig` — абсолютный путь к файлу конфигурации управляющего демона, 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.
- `afterifconf` — имя скрипта, содержащего команды, которые выполняются непосредственно после конфигурирования всех интерфейсов при смене активного сервера.
- `beforeifconf` — имя скрипта, содержащего команды, которые выполняются перед конфигурированием всех интерфейсов при смене активного сервера.



Примечание. Параметры `afterifconfig` и `beforeifconfig` используются для организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов. Они не являются обязательными и могут отсутствовать в секции.

- `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](#) на стр. 217);
 - файлы, содержащие сетевые фильтры и правила трансляции (заданные пользователем и полученные из программы ViPNet Policy Manager);
 - файлы с настройками функции L2OverIP;
 - файлы `*.cfg` с контрольными суммами конфигурационных файлов;
 - файлы с настройками [маршрутизации](#) (см. глоссарий, стр. 231) 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 `journal` 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.
- `keys` — включение или выключение резервирования группы файлов **справочников и ключей** (см. глоссарий, стр. 233). Возможные значения: `yes` (по умолчанию) или `no`.



Внимание! Набор файлов, входящих в группы конфигурационных файлов (`config`), файлов справочников и ключей (`keys`) и файлов журналов (`journals`), определяется демоном `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 демонах `iplircfg` и `mftpd`, а также если параметры `config`, `keys` и `journal` установлены в значение `yes`. Установка параметра `config`, `keys` или `journal` в значение `no` означает выключение резервирования соответствующей группы. Не рекомендуется устанавливать параметры `config` и `keys` 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](#) (см. глоссарий, стр. 233) содержатся в файле `iplir.conf`. Для редактирования этого файла используется команда `iplir config`. Перед редактированием файла `iplir.conf` необходимо завершить работу управляющего демона командой `iplir stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его командой `iplir start`.

Файл `iplir.conf` содержит секции с параметрами, описанные ниже.

Секция `[id]`

Секция `[id]` используется для описания адресных настроек [защищенных сетевых узлов](#) (см. глоссарий, стр. 230), связанных с ViPNet Coordinator KB. Каждому узлу, с которым у ViPNet Coordinator KB есть связь, соответствует своя секция `[id]`. Первая секция `[id]` соответствует собственным настройкам ViPNet Coordinator KB (собственная секция).

Секция `[id]` содержит следующие параметры:

- `accessiplist` — определяет [IP-адреса доступа](#) (см. глоссарий, стр. 228) 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 управляющего демона.

- `<IP-адрес доступа>` — IP-адрес доступа к узлу.
- `<метрика>` — [метрика](#) (см. глоссарий, стр. 231) указанного адреса доступа. Метрика определяет задержку (в миллисекундах) отправки тестовых сообщений при выполнении процедуры определения адреса доступа узла. Опросы осуществляются периодически (см. параметры `server_pollinterval`, `checkconnection_interval` 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](#) (см. глоссарий, стр. 233), 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. Возможные значения:
 - `auto` — адрес задан ViPNet Coordinator KB.
 - `manual` — адрес задан администратором вручную (редактированием файла `iplir.conf`).
 - `addrdoc` — адрес взят из справочников, полученных из программы [ViPNet Центр управления сетью](#) (см. глоссарий, стр. 227).
- `blockforward` — включение или выключение блокирования транзитных пакетов, идущих через узел. Используется в собственной секции ViPNet Coordinator KB. Возможные значения: `off` — все транзитные пакеты на ViPNet Coordinator KB пропускаются, `on` — все транзитные пакеты на ViPNet Coordinator KB блокируются с кодом 70. По умолчанию данный параметр отсутствует, что эквивалентно значению `off`.
- `checkconnection_interval` — период автоматической отправки координатором сообщения другому связанному с ним координатору для оперативного определения недоступности этого координатора по текущему адресу доступа и попытки подключения к нему по альтернативному каналу доступа. Указывается в секундах, возможные значения: от 20 до 3600. Если данный параметр не указан в секции `[id]` координатора, то автоматическая проверка связи с ним не производится.
- `fixfirewall` — определяет режим фиксации настроек работы собственного узла через внешний межсетевой экран. Возможные значения:
 - `off` (по умолчанию) — внешний IP-адрес и порт доступа к ViPNet Coordinator KB определяются автоматически по информации от узлов внешней сети;
 - `on` — внешний IP-адрес и порт доступа к ViPNet Coordinator KB жестко заданы администратором в параметрах `firewallip` и `port` данной секции.
- `ip` — содержит [реальный IP-адрес](#) (см. глоссарий, стр. 232) и соответствующий ему [виртуальный IP-адрес](#) (см. глоссарий, стр. 229) узла. Причем 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. Причем в случае изменения порядка следования реальных IP-адресов, порядок следования виртуальных адресов не меняется.
- `port` — определяет порт назначения, на который следует посылать пакеты для узла, если этот узел находится за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр.

- `proxyid` — определяет режим работы узла, находящегося за межсетевым экраном. В каждой секции `[id]` может быть только один такой параметр. Возможные значения:
 - в собственной секции `[id]`:
 - `0xfffffffffe` — при работе в режиме «С динамической трансляцией адресов» (если в секции `[dynamic]` параметр `dynamic_proxy` установлен в `on` (см. [Секция \[dynamic\]](#) на стр. 208));
 - `0` — 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`.
 - 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](#) (см. глоссарий, стр. 233) 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` — содержит адреса незащищенных компьютеров, [туннелируемых ViPNet Coordinator KB \(указаны в собственной секции\)](#) или другими координаторами (см. глоссарий, стр. 234), в виде: `<ip1>-<ip2> to <ip3>-<ip4>`, где:
 - `<ip1>-<ip2>` — начальный и конечный реальные адреса диапазона туннелируемых узлов;
 - `<ip3>-<ip4>` — диапазон виртуальных адресов, которые соответствуют реальным адресам из диапазона `<ip1>-<ip2>`, и которые будут использоваться вместо реальных адресов туннелируемых узлов, если на узле, который к ним обращается, настроена видимость по виртуальным адресам. Например, 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` — при этом параметры `<ip1>` и `<ip2>` задаются администратором сети ViPNet в ПО 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
```

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

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

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

В одной секции `[id]` 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` — позволяет настроить тип видимости для всех узлов, туннелируемых координатором. Возможные значения:
 - o `real` — всегда обращаться к туннелируемым узлам по их реальным адресам;
 - o `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]`.

- `usetunnel` — используется в любой секции `[id]`, кроме собственной. 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` — позволяет настроить тип видимости узла. Возможные значения:
 - `auto` — автоматически определять тип видимости узла, в зависимости от текущего [адреса видимости узла](#) (см. глоссарий, стр. 228).
 - `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).

Нерадактируемые параметры секции `[id]`

- `accessip` — текущий [IP-адрес доступа к узлу](#) (см. глоссарий, стр. 228) 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 управляющий демон отличает одну секцию `[id]` от другой. Идентификатор присваивается сетевому узлу ViPNet при его создании в программе [ViPNet Центр управления сетью](#) (см. глоссарий, стр. 227). В каждой секции `[id]` может быть только один такой параметр.
- `firewallip` — определяет 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](#) (см. глоссарий, стр. 230) 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 программе ViPNet Центр управления сетью и предназначен для удобства настройки. Данный параметр записывается в файл конфигурации 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 `[adapter]`

Секции `[adapter]` описывают [статические сетевые интерфейсы компьютера](#) (см. глоссарий, стр. 233). Каждому интерфейсу соответствует своя секция `[adapter]`. Если статический интерфейс не описан секцией `[adapter]`, то все проходящие через него [IP-пакеты](#) (см. глоссарий, стр. 226) блокируются.

Если в файле `iplir.conf` нет ни одной секции `[adapter]`, то управляющий демон при запуске получает от системы список сетевых интерфейсов и автоматически создает соответствующие секции `[adapter]`.

В процессе работы управляющий демон 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, то он выключается и в драйвере ViPNet. После включения или изменения IP-адреса интерфейса эти изменения автоматически загружаются в драйвер ViPNet.

В секции `[adapter]` указываются следующие параметры:

- `allowtraffic` — разрешение или блокирование прохождения IP-трафика через интерфейс. Возможные значения:
 - `on` (по умолчанию) — IP-пакеты пропускаются или блокируются в соответствии с сетевыми фильтрами, заданными на узле.
 - `off` — IP-пакеты блокируются независимо от остальных настроек.

- `type` — тип интерфейса для драйвера ViPNet. Возможные значения: `internal` (внутренний) или `external` (внешний).

Тип интерфейса выбирается, исходя из следующего:

- 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](#) (см. глоссарий, стр. 229)), то интерфейсу, посредством которого ViPNet Coordinator KB будет связываться с узлом, выполняющим функции [межсетевого экрана](#) (см. глоссарий, стр. 231), следует назначить тип `external`, остальным интерфейсам ViPNet Coordinator KB — тип `internal`.

Нерадактируемые параметры секции [adapter]

- `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 управляющего демона и драйвера ViPNet все они будут представлять одно физическое устройство с базовым именем (`eth0`).

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](#) (см. глоссарий, стр. 233), 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.

Секция [misc]

Секция [misc] содержит различные дополнительные параметры:

- `client_pollinterval` — период опроса координатора ViPNet Coordinator KB **клиентами** (см. глоссарий, стр. 230), для которых этот координатор 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 конфигурационного файла (совпадает с версией ViPNet Coordinator KB, с помощью которой файл последний раз был сохранен).
- `ifcheck_timeout` — период опроса параметров сетевых интерфейсов, известных управляющему демону. Указывается в секундах, значение по умолчанию — 5.
- `iscaggregate` — включение или выключение накопления служебного трафика, обрабатываемого на координаторе. С помощью настройки 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** (см. глоссарий, стр. 226) при запуске управляющего демона;
 - `off` — выключать IP-форвардинг при запуске управляющего демона;
 - `system` — не изменять текущие настройки IP-форвардинга при запуске управляющего демона.



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). Значение 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. Значение по умолчанию — 0.

Уменьшать параметр MSS рекомендуется только, 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! Параметр `mssdecrease` не следует изменять без крайней необходимости.

- `server_pollinterval` — период опроса данным координатором других [координаторов](#) (см. глоссарий, стр. 231). 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. Значение параметра должно быть больше либо равно 1 секунде и меньше либо равно максимальному значению в зависимости от исполнения:
 - KB100 — 236 секунд;
 - KB1000 — 51 секунда;
 - KB2000 — 19 секунд;
 - KB5000 — 10 секунд.

Значение по умолчанию — 7.

Также от значения этого параметра зависит время, которое займет восстановление связи с ViPNet Coordinator KB после переключения узлов кластера.

- `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]` (см. [Секция \[id\]](#) на стр. 202).
- `tunnel_local_network` — параметр, который позволяет не туннелировать IP-адреса, входящие в локальную подсеть ViPNet Coordinator KB. Возможные значения:
 - `off` (по умолчанию) — обращаться к туннелируемым узлам, находящимся в локальной подсети, минуя туннелирующий координатор;
 - `on` — обращаться к туннелируемым узлам, находящимся в локальной подсети, через координатор, который туннелирует данные узлы. В этом случае доступ к туннелируемым узлам в локальной подсети может быть затруднен.
- `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 управляющего демона.

Секция `[debug]`

Секция `[debug]` определяет параметры ведения журнала устранения неполадок управляющего демона. Она содержит следующие параметры:

- `debuglevel` — уровень детализации информации, выводимой в журнал. Возможные значения: от 1 до 5 (по умолчанию 3). Чем выше уровень детализации, тем более подробная информация выводится в журнал. Значение параметра `-1` выключает ведение журнала.
- 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 ОАО «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` (демоны).

- o `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

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](#) (см. глоссарий, стр. 229) 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 файлов конфигурации. Кроме того, для узлов производится назначение виртуальных адресов в параметрах `ip` (см. [Секция \[id\]](#) на стр. 202).
- `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`).

Не редактируемые параметры секции [virtualip]

- `endvirtualip` — служебный параметр, в котором хранится следующий за последним назначенным [базовый виртуальный адрес](#) (см. глоссарий, стр. 228). 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] (см. [Секция \[id\]](#) на стр. 202) 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` — автоматическое определение видимости узлов;
 - `real` (по умолчанию) — доступ к узлам по их [реальным IP-адресам](#) (см. глоссарий, стр. 232);
 - `virtual` — доступ к узлам по их [виртуальным IP-адресам](#) (см. глоссарий, стр. 229).
- `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` (см. [Секция \[id\]](#) на стр. 202). 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 IPIir 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` — определяет версию используемого протокола IPIir. Может принимать следующие значения:
 - `il4x` — определяет использование версии 4.1 и 4.2 протокола IPIir. При указании этого значения параметр `cs` игнорируется. Данные версии протокола используются для совместимости с другими узлами сети ViPNet, не поддерживающими протокол IPIir версии 6.0.
 - `il60` — определяет использование версии 6.0 протокола IPIir.
- `cs` — определяет 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 стр. 213). 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 \[packet-settings\]](#) на стр. 213). Данный параметр не обязательный, если строки в секции нет, то 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 обязательный, если строки в секции нет, то 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 обязательный, если строки в секции нет, то 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`, управляющий демон 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 управляющего демона 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 управляющий демон не перезапускался. Поэтому после добавления секций `[adapter]` в файл `iplir.conf` вручную рекомендуется сначала запустить управляющий демон командой `iplir start`, затем завершить его работу командой `iplir stop`, после чего отредактировать нужный файл `iplir.conf`-<интерфейс> и снова запустить управляющий демон.

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 IP-пакетов до тех пор, пока не будет достигнут максимальный размер журнала, после чего самые ранние записи стираются и на их место записываются новые. Для уменьшения размера журнала, а также для удобства его просмотра одинаковые записи о пакетах, зарегистрированные в течение заданного времени, объединяются в одну запись, и затем при просмотре журнала можно узнать, сколько раз было зафиксировано событие, описываемое этой записью.

Секция `[db]` содержит следующие параметры:

- `maxsize` — максимальный размер журнала в мегабайтах (по умолчанию — 50 MBytes).

Реальный размер журнала из-за наличия в нем служебного заголовка получается примерно на 1 Кбайт больше. Каждый раз при запуске управляющего демона 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`.
- `registertcpserverport` — включение или выключение скрытия информации о порте клиента ViPNet при соединении 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 `registertcpserverport` установлен в значение `on`, порт клиента при TCP-соединении не регистрируется и не учитывается, что позволяет объединить события о попытках подключения к какому-либо порту на компьютере с определенного адреса в одну запись. Это часто бывает удобно.



Примечание. Если параметр `registertcpserverport` установлен в значение `on`, то значение клиентского порта, отображаемого в журнале пакетов, будет равно 0.

- `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 модуля MFTP](#) (см. глоссарий, стр. 234) содержатся в файле `mftp.conf`. Для редактирования этого файла используется команда `mftp config`. Перед редактированием файла необходимо завершить работу демона `mftpd` командой `mftp stop`, а после окончания редактирования, чтобы все изменения вступили в силу, — снова запустить его с помощью команды `mftp start`.

Файл `mftp.conf` содержит секции с параметрами, описанные ниже.

Секция [channel]

Секции `[channel]` содержат настройки каналов, по которым ViPNet Coordinator KB 4 может обмениваться данными с другими узлами. Каждому узлу, с которым у ViPNet Coordinator KB 4 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 модуля](#) (см. глоссарий, стр. 234).
- `call_flag` — признак немедленной передачи конвертов по каналам MFTP и SMTP. Возможные значения:
 - `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 в случае использования канала MFTP инициатором соединения не станет удаленный узел или в случае использования канала SMTP не будет вызван модуль MailTrans (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]` для каналов любого типа

- `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 управляющим демоном. Если значение этого параметра по каким-либо причинам не было получено от управляющего демона, то оно будет установлено в `0.0.0.0`. В этом случае его можно задать вручную, а затем перезапустить транспортный модуль. 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.

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.

Специфические параметры для канала SMTP

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

- `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.
- `reportaddress` — адрес электронной почты, на который будут отправляться исходящие конверты, в формате: `reportaddress = <имя пользователя>@<сервер>.<домен>`. Например: `reportaddress = user@example.com`



Примечание. В случае отсутствия параметра `maxsmtpsize` в данной секции используется значение, заданное для всех каналов SMTP в секции `[mailtrans]` (см. [Секция \[mailtrans\]](#) на стр. 220).

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 модулем 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 модуль 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 (см. [Специфические параметры для канала SMTP](#) на стр. 218). 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/smtout`.
- `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 модулем. В процессе работы транспортный модуль записывает в этот журнал информацию о полностью принятых, отправленных, удаленных и поврежденных конвертах.

Просмотр журнала конвертов осуществляется с помощью команды `mftp view`.

Секция `[journal]` содержит следующие параметры:

- `dump_interval` — период выгрузки информации из журнала конвертов в днях. В процессе работы транспортный модуль 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.
- `use_journal` — включение или выключение ведения журнала работы транспортного модуля. 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 секции `[journal]`

- `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.2018.09.23`.
- `last_dump` — время последней выгрузки информации из журнала конвертов.

Секция `[misc]`

Секция `[misc]` содержит различные параметры, определяющие работу транспортного модуля в целом:

- `connect_timeout` — интервал времени в секундах, в течение которого клиент будет пытаться установить соединение с удаленным узлом по каналу MFTP (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 (по умолчанию — 900).

- `max_listen_ports` — диапазон значений перебора портов для соединений по каналу MFTP с удаленным узлом в случае неудачи (по умолчанию — 3). Транспортный модуль циклично перебирает порты в диапазоне от `port` до `port+max_listen_ports-1`. Ожидая входящие соединения, транспортный модуль прослушивает все порты указанного диапазона.
- `num_attempts` — количество последовательных попыток соединения, после которых устанавливается тайм-аут, если соединиться так и не удалось (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 (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. Возможные значения:
 - `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 демон `mftpd` ожидает соединения по каналу MFTP от удаленных сетевых узлов (по умолчанию — 5000).
- `recv_buff_size` — размер буфера приема в байтах. Значение по умолчанию — 65500, минимально допустимое значение — 1024.
- `send_buff_size` — размер буфера передачи в байтах. Значение по умолчанию — 65500, минимально допустимое значение — 1024.



Примечание. Обычно значение 65500 параметров `send_buff_size` и `recv_buff_size` оптимально для обеспечения максимальной скорости приема и передачи конвертов транспортным модулем.

- `save_sent` — включение или выключение хранения имен отправленных прикладных конвертов. Возможные значения:
 - `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.
- `t1l_ct1` — время жизни конвертов, содержащих управляющие запросы, в исходящей очереди. Указывается в днях, значение по умолчанию — 10. Если по истечении времени, указанного в параметре `t1l_ct1`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.

- `t11_out` — время хранения конвертов в исходящей очереди в днях. Значение по умолчанию — 30. Если по истечении времени, указанного в параметре `t11_out`, конверт не удалось отправить, то он удаляется из очереди и помещается в корзину.
- `t11_trash` — время хранения конвертов в корзине в днях. Значение по умолчанию — 90. Если время хранения конверта в корзине превышает указанное в параметре `t11_trash`, то он удаляется.
- `wait_timeout` — время ожидания активности в установленном MFTP-соединении. Указывается в секундах, 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`.
- `remote_net_route` — включение или выключение использования прямой маршрутизации между сетями ViPNet. Возможные значения:
 - `yes` (по умолчанию) — в этом случае при настройке перенаправления конвертов с помощью параметра `transit` в секции `[channel]` шлюзовые координаторы не будут обрабатывать конверты, передаваемые между сетями ViPNet.
 - `no` — в этом случае все настройки прямой маршрутизации будут сброшены, и обрабатывать конверты будут шлюзовые координаторы. При последующем включении использования прямой маршрутизации потребуется повторная настройка обхода шлюзовых координаторов.

Секция `[debug]`

Секция `[debug]` определяет параметры ведения журнала устранения неполадок транспортного модуля и содержит следующие параметры:

- `debuglevel` — уровень детализации информации, выводимой в журнал. Возможные значения: от 1 до 5 (по умолчанию 3). Чем выше уровень детализации, тем более подробная информация выводится в журнал. Значение параметра `-1` выключает ведение журнала.
- 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 ОАО «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` (демоны).
 - `level` — уровень важности информации. Возможные значения: `err` (ошибка), `info` (информационное сообщение) или `debug` (отладочная информация).

Значение параметра `debuglogfile` по умолчанию — `syslog:daemon.debug`.

Секция [reserv]

Секция [reserv] содержит параметры настройки транспортного модуля на координаторе, работающем в составе кластера горячего резервирования:

- `cmd_port` — порт, на котором демон `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 файлах конфигурации 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. Возможные значения:
 - `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.
- `upgrade_replicate_timeout` — период времени в секундах, по истечению которого удаляется конверт с обновлением, который не удалось передать на пассивный сервер (по умолчанию — 300 секунд).

Секция [upgrade]

Данная секция содержит параметры, которые определяют поведение транспортного модуля при приеме конфигурационных файлов, справочников и ключей из программы ViPNet Центр управления сетью:

- `confsave` — тип конфигурации, автоматически создаваемой перед обновлением. Возможные значения:
 - `partial` (по умолчанию) — частичная конфигурация, включающая только конфигурационные файлы (без справочников и ключей).
 - `full` — полная конфигурация, включающая конфигурационные файлы, справочники и ключи.

- `off` — конфигурация не создается автоматически.
- `maxautosaves` — максимальное число автоматически сохраненных конфигураций. Возможные значения: от 1 до 10. Значение по умолчанию — 10. Перед автоматическим созданием очередной конфигурации проверяется число ранее сохраненных конфигураций. Если это число равно значению `maxautosaves`, то конфигурация, созданная раньше остальных, удаляется, после чего сохраняется текущая конфигурация.
- `upgrade_for_kc_path` — абсолютный путь к каталогу, в который внешние приложения помещают файлы `*.sok` с запросами на сертификаты (по умолчанию — `/opt/vipnet/ccc/for_kc`).
- `upgrade_ini` — имя конфигурационного файла для процесса обновления (по умолчанию — `/opt/vipnet/user/upgrade.conf`).

А

Глоссарий

DHCP-сервер

Сервер, автоматически администрирующий IP-адреса DHCP-клиентов и выполняющий соответствующую настройку для сети.

DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам компьютеров в интернет-домене. Например, ns.domain.net. Как правило, информация о домене хранится на двух DNS-серверах, называемых «Primary DNS» и «Secondary DNS» (дублирование делается для повышения отказоустойчивости системы).

Также DNS-сервер называют сервером доменных имен, сервером имен DNS.

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 смогут взаимодействовать друг с другом так, как будто они находятся в одном сегменте с прямой видимостью по MAC-адресам. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

NTP-сервер

Сервер точного времени, который необходим для синхронизации времени компьютеров, рабочих станций, серверов и прочих сетевых устройств. Этот сервер играет роль посредника между эталоном времени и сетью. Он получает время от эталона по специальному каналу (интерфейсу) и выдает его для любого узла сети, обеспечивая тем самым синхронизацию устройств.

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. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это 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 УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

VLAN

Виртуальная локальная компьютерная сеть, представляет собой группу узлов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному 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](#) (см. глоссарий, стр. 231). 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

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, то 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](#) (см. глоссарий, стр. 231) 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 узлы 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.

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, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

ДНСД (датчик несанкционированного доступа)

Электротехническое устройство, встраиваемое в устройство, несанкционированный доступ внутрь корпуса которого требуется контролировать. Обработка события несанкционированного доступа может обрабатываться независимо как самим датчиком, так промежуточным или самим контролируемым устройством с информированием администратора безопасности контролируемого устройства.

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 (UPS)

Автоматическое электронное устройство с аккумуляторной батареей, предназначенное для бесперебойного кратковременного снабжения электрической энергией компьютера и его компонентов 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 интерфейсам можно назначить следующие классы: `access`, `trunk`, `slave`.

По умолчанию сетевому интерфейсу назначен класс `access`. Если требуется, чтобы интерфейс Ethernet обрабатывал трафик из нескольких VLAN, ему необходимо назначить класс `trunk`.

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 сбоя, 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. Клиент должен быть зарегистрирован на координаторе. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключевой блокнот ДСДР

Ключевой блокнот ДСДР предназначен для средств криптографической защиты данных, не содержащих сведений, составляющих государственную тайну. Ключевой блокнот ДСДР содержит ключевую информацию, которая используется для шифрования конфиденциальной информации.

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, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или специальный программно-аппаратный комплекс. В рамках 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 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

Предназначена для задания приоритета маршрута передачи IP-трафика.

Область маршрутизации

Одна или несколько IP-сетей, в которых осуществляется обмен информацией по определенному протоколу, в частности, по протоколу [OSPF](#) (см. глоссарий, стр. 227).

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 осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса служит сетевая плата, в качестве виртуального — интерфейс для [VLAN](#) (см. глоссарий, стр. 228).

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

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 сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Статический сетевой интерфейс

[Сетевой интерфейс](#) (см. глоссарий, стр. 233), 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 конверта.

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через Интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей. При этом установка программного обеспечения ViPNet на эти узлы необязательна, то есть туннелируемые узлы могут быть как защищенными, так и открытыми.